FIGHTING FRAUD

How to Establish and Manage an Anti-Fraud Program

Dr. Gerald L. Kovacich

B H

Fighting Fraud

Other Books Authored or Co-Authored

Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program: May 1998, ISBN 0-7506-9896-9; by Dr. Gerald L. Kovacich; First Edition and July 2003, ISBN 0-7506-7656-6, Second Edition; published by Butterworth-Heinemann (Czech translation of First Edition also available).

I-Way Robbery: Crime on the Internet: May 1999, ISBN 0-7506-7029-0; co-authored by Dr. Gerald L. Kovacich and William C. Boni; published by Butterworth-Heinemann; Japanese translated version published by T. Aoyagi Office Ltd, Japan: February 2001, ISBN 4-89346-698-4.

High-Technology Crime Investigator's Handbook: Working in the Global Information Environment: First Edition, September 1999, ISBN 0-7506-7086-X; co-authored by Dr. Gerald L. Kovacich and William C. Boni; July 2003, and Second Edition; July 2006 ISBN 10: 0-7506-7929-8; ISBN 13: 9-780-7506-7929-9; co-authored with Dr. Andy Jones and published by Butterworth-Heinemann.

Netspionage: The Global Threat to Information: September 2000, ISBN 0-7506-7257-9; co-authored by Dr. Gerald L. Kovacich and William C. Boni; published by Butterworth-Heinemann.

Information Assurance: Surviving in the Information Environment: First Edition, September 2001, ISBN 1-85233-326-X; co-authored by Dr. Gerald L. Kovacich and Dr. Andrew J. C. Blyth; published by Springer-Verlag Ltd (London); Second Edition, ISBN 1-84628-266-7, published in March 2006.

Global Information Warfare: How Businesses, Governments, and Others Achieve Global Objectives and Attain Competitive Advantages: June 2002, ISBN 0-84931-114-4; co-authored by Dr. Andy Jones, Dr. Gerald L. Kovacich and Perry Luzwick; published by Auerbach Publishers/CRC Press.

The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program: April 2003, ISBN 0-7506-7487-3; co-authored by Dr. Gerald L. Kovacich and Edward P. Halibozek; published by Butterworth-Heinemann.

Mergers & Acquisitions Security: Corporate Restructuring and Security Management: April 2005, ISBN 0-7506-7805-4; co-authored by Dr. Gerald L. Kovacich and Edward P. Halibozek; published by Butterworth-Heinemann.

Security Metrics Management: How to Manage the Costs of an Assets Protection Program: December 2005, ISBN 0-7506-7899-2; co-authored by Dr. Gerald L. Kovacich and Edward P. Halibozek; published by Butterworth-Heinemann.

The Security Professional's Handbook on Terrorism: Establishing and Managing a Corporate Anti-Terrorism Program: To be released in September 2007, ISBN 0-7506-8257-4; co-authored with Edward P. Halibozek and Dr. Andy Jones; published by Butterworth Heinemann.

Fighting Fraud

How to Establish and Manage an Anti-Fraud Program

Dr. Gerald L. Kovacich

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Butterworth-Heinemann is an imprint of Elsevier

Elsevier Academic Press
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
525 B Street, Suite 1900, San Diego, California 92101-4495, USA
84 Theobald's Road, London WC1X 8RR, UK

This book is printed on acid-free paper.

Library of Congress Cataloging-in-Publication Data
Kovacich, Gerald L.
Fighting fraud : how to establish and manage an anti-fraud program / Gerald L. Kovacich.
p. cm.
Includes index.
ISBN 978-0-12-370868-7 (alk. paper)
1. Commercial crimes. 2. Commercial crimes — Investigation. 3. Fraud — Prevention. 4. Fraud investigation. I. Title.
HV6769.K68 2008
658.4′73 — dc22

2007013397

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN 13: 978-0-12-370868-7
ISBN 10: 0-12-370868-0

For all information on all Elsevier Academic Press publications visit our Web site at www.books.elsevier.com

Printed in the United States of America
08 09 10 11 12 13 10 9 8 7 6 5 4 3 2 1

This book is dedicated to all those fraud fighters who combat defrauders and the other miscreants who try to take something of value from others without their permission and without providing the owners with just compensation.

This book is especially dedicated to those whistleblowers who have the guts to stand up when a wrong has been committed!

This page intentionally left blank

Quotation*

[T]he modern economic world centers on the controlling corporate organization. . . . Executives of Enron, WorldCom, Tyco and others became the focus of widely publicized criticism, even outrage. Joining the language came the reference to corporate scandals. Avoided only was mention of the compelling opportunity for enrichment that had been accorded the managers of the modern corporate enterprise, and this in a world that approves of self-enrichment as the basic reward for economic merit . . .

. . . Great firms, particularly in energy and mass communications but not so confined, came to dominate the news. In all cases, the situation was the same, as was the result. Management was in full control. Ownership was irrelevant, some auditors were compliant. Stock options added participant wealth and slightly concealed take. . . .

The least expected contribution to the adverse and even criminal activity was the corrupt accounting . . . This provided cover for the devious actions that extended to outright theft. Individuals had long regarded accounting as both competent and honest. . . .

The corporate scandals and especially the associated publicity have led to discussion or appropriate regulation and some action — to positive steps to insure accounting honesty and some proposed remedies, as required, to counter management and lesser corporate fraud . . .

. . . Managers, not the owners of capital, are the effective power in the modern enterprise. . . .

. . . So, as a very practical matter, power passed to the mentally qualified, actively participating management, and it did so irrevocably. The belief that ownership has a final authority persisted, as it still does . . .

. . . The basic fact of the twenty-first century — a corporate system based on the unrestrained power of self-enrichment.

---

* From John K. Galbraith's book, *The Economics of Innocent Fraud: Truth for Our Time*. Houghton Mifflin, Boston. 2004.

This page intentionally left blank

Table of Contents

	Preface	xix
	Acknowledgments	xxiii
	Introduction and Premise	xxvii
	SECTION I: AN INTRODUCTION TO THE WONDERFUL WORLD OF FRAUD	1
1	The New-Old Global Business Environment	3
	Introduction	3
	Globalization of Business — Benefits to Nation-States	5
	Expansions of the Global Marketplace and their Areas of Operations	6
	Types of Corporations	7
	Corporate Owners and Locations	7
	Corporate Products	8
	The High-Technology Factor	9
	Nanotechnology	11
	High-Technology Related Frauds and Other Crimes	14
	Advent of the Superhighways	14
	The Impact of Superhighways on Frauds and Other Crimes	15
	A Short History of Crimes and Other Frauds Via the I-Way	17
	Superhighway Frauds and Other Crimes to I-Way Robberies	18
	I-Way Robbery — Its Prevalence	20
	There Is No I-Way Patrol to Stop I-Way Robbers	21
	Global Connectivity Via the I-Way = Global Exposure to Attacks by Fraud-Threat Agents and Other Miscreants	21
	Capabilities and Limitations of Law Enforcement	22
	Challenges to Security Professionals and Others	23
	Case Study 1	24

Case Study 2 25
Summary 26

2 Corporate Assets, Frauds and Other Terms — What Are They? 27
Introduction 27
Definition of General Fraud 28
Specific Fraud Definitions 31
Corporate Assets 32
Other Terms and Definitions 33
Case Study 34
Summary 35

3 Fraud-Related Laws 37
Introduction 37
Some U.S. Federal Fraud-Related Laws 38
Relevant Consumer Protection Laws for Fraud in the United States 40
A Few Examples of U.S. Federal Enforcement of Fraud-Related Laws, Approach and Actions 40
Mail Fraud Statutes (condensed and paraphrased) 41
Money Laundering 43
Financial Institution Fraud (Bank Fraud) 43
Civil Litigation 43
U.S. Treasury Collection 44
Securities Violations 44
Role of Phone Companies 44
European Fraud-Related Laws 45
EU Fight Against Frauds 45
ASIA and Fighting Fraud 47
Case Study 48
"Blowing the Whistle" on Defrauders can be Dangerous 50
Summary 50

4 Corporations Don't Commit Frauds, People Do 53
Introduction 53
Are Defrauders a Product of Their Environment, or Is It in Their Genes? 53
Some Criminology Theories 54
Fraud-Threat Agents 56

Human Errors — Accidents 56
Man-Made or Malicious Fraud Threats 57
Potential Fraud-Threat Agents 57
Capabilities 64
Motivation 65
Access 67
Catalysts 68
Inhibitors 69
Amplifiers 71
Fraud-Related Factors for Attacking Systems 74
Relationship of Threat Elements 74
Case Study 74
Summary 78

5 Fighting Fraud — Whose Job Is It Anyway? 79
Introduction 79
Role of Executive Management 80
Role of Corporate Management 82
Role of the Corporate Employees 83
Role of the Ethics Director 83
Role of the Auditor 84
Role of the Fraud Examiner 85
Role of the Chief Security Officer (CSO) 86
Why the Corporate Security Professional? 87
Case Study 88
Summary 88

6 Where There Is a Will There Is a Way — Fraud Schemes 89
Introduction 89
Types of Fraud Schemes 90
Financial 91
Credit Card Skimming 95
Mortgage Frauds 96
Computer and Telecommunications Frauds 97
ATM Frauds 101
Click Fraud 104
Clip-on Fraud 106
Securities Frauds 107
Employment Application Frauds 108

Identity Theft Scams 108
"Nigerian Scam" 109
Accounting Fraud Schemes 111
Bribery and Corruption 116
Conflicts of Interest 116
Purchasing — Four Basic Categories 116
Inventory 117
Investments and Fixed Assets 118
Payroll and Personal Expenses 119
Procurement/Contracts 120
Telemarketing Fraud 120
Advance Fee Scheme 121
Common Health Insurance Frauds 121
Letter of Credit Fraud 122
Prime Bank Notes 122
The Ponzi Scheme 123
Pyramid Scheme 123
Case Study 124
Summary 125

7 Fraud Cases and Commentary — Learning by Example 127
Introduction 127
Actual Fraud and Fraud-Related Cases 127
Phishers and Taxpayers 128
Fraud by Corporate Executives 129
Foreign Exchange Trading Fraud 131
Katrina Waste and Frauds 132
Organized Crime and Cybercrime 132
Securities Fraud in Cyberspace 133
Computer Hard Drives Lead to Frauds 133
Debt-Collecting Frauds 134
Government Contracting Fraud 135
Fraud-Threat Agents Can Be Anyone in Any Position 136
U.S. Securities and Exchange Commission (SEC) Fighting Fraud 137
Fraud in School Systems 138
Dead Soldiers and E-Mail Scams 139
Another Example of Insider Fraud 139
Executive Management and Accounting Fraud 140
Merchandise Receipt and Exchange Fraud 141

Click Frauds 142
Mortgage Fraud 142
Government Contractors and Fraud 143
Frauds and Microsoft Software 144
Y2K-Related Fraud 144
Data Storage Conducive to Fraud-Threat Agents 145
Another Example of Click Fraud 146
Pyramid Schemes Move on to the Internet 146
Prepaid Cellular Phone Fraud 147
Identifying International Corruption 148
Credit Card Information Theft and Frauds 149
Hackers, Crackers, Phishers, Oh My! 150
Urban Legends and Frauds 151
Medical Research Frauds 151
Corruption and the War in Iraq 152
Comments on Identity Thefts as a Vehicle to Fraud 153
Lobbyists and Corruption 153
Internet Scams are International 154
Faking a Medical Condition 154
Internet Fraud Sweep 155
ATM Fraud 156
Social Security Scam 156
Stamp Fraud 157
Banker and Identity Theft 158
Accounting Firm Fraud 158
Lawyers and Medical Rip-offs 160
Another Mention of the "Nigerian" Scams — Variations on a Theme 160
Case Study 161
Summary 161

SECTION II: ESTABLISHING AND MANAGING AN ANTI-FRAUD PROGRAM 163

8 The International Widget Corporation 165
Introduction 165
IWC Background Information 165
Key Elements for the CSO to Consider 168
Getting to Know IWC 169
IWC's Business Plans 170

Strategic Business Plan 170
Tactical Business Plan 171
IWC's Annual Business Plan 173
IWC and the History of Its CSO 173
Key Elements of IWC's Annual Business Plan 176
Anti-Fraud Program Planning 176
IWC's Departments of Primary Importance to the CSO 176
IWC Vision, Mission, and Quality Statements 178
Plans 180
Other IWC Plans and CSO Support 181
Case Study 181
Summary 182

9 Establishing an Anti-Fraud Program 183
Introduction 183
IWC's Anti-Fraud Program 185
Anti-Fraud Program Project Planning 189
IWC Anti-Fraud Program Project Planning and Management 192
Anti-Fraud Program Project Team 195
Anti-Fraud Drivers — The First Major Task in Anti-Fraud Program Development 195
IWC Anti-Fraud Program Requirements — Policies 196
Risk Assessment — The Second Major Task in Developing an Anti-Fraud Program 196
Basics of IWC's Risk Assessment Process 197
Threats 199
Natural Threats 200
Man-Made Threats 200
Vulnerabilities 201
Risks 202
Assets Protection Risk Assessments 202
Assets Protection Risk Analyses 204
Developing Anti-Fraud Defenses 204
Three Key Ingredients in an Anti-Fraud Program's Defenses 205
IWC's Anti-Fraud Policies 206
Anti-Fraud Requirements and Policy Directive 209
Anti-Fraud Procedures 210
The CSO and Security Department's Anti-Fraud Accountabilities 212

Off-Site Corporate Facilities 212
Recruiting Anti-Fraud Professionals 212
Case Study 213
Summary 214

10 Managing an Anti-Fraud Program 215
Introduction 215
CSO Leadership 216
Management versus Leadership 217
Meeting Customers' Expectations 218
IWC Internal Customers 219
IWC External Customers 219
IWC Executive Management Expectations of a CSO 220
Managing Risk 222
Security's Vision, Mission, and Quality Statements 223
Managing the IWC Anti-Fraud Program 223
Planning 223
Some Aspects to Incorporate into an Anti-Fraud Program Plan 225
Budgeting 227
Controlling 230
Quality, Process Improvement, and Assessment of Organization Performance 232
Process Management 232
Performance Management 233
Using Technology to Deliver Anti-Fraud Program Support and Services 234
Managing Quality and Management Oversight 235
What is Risk Management As It Relates to IWC's Anti-Fraud Program? 235
Managing and Reducing Risks to Corporate Assets 236
Program for Managing Anti-Fraud Defensive Risks 237
Responding to Fraud Incidents 240
Managing Fraud Threats 241
Case Study 242
Summary 244

11 Winning through Teaming 245
Introduction 245
Anti-Fraud Program Team Building 245

Executive Management as Team Members 246
Teaming with IWC Executive Management Through a Business Approach 247
Teaming with Corporate Peers 248
Teaming and Dealing with Office Politics 250
Teaming with Your Security Managers 252
Teaming with Your Security Staff 253
Teaming and Dealing with Satellite Offices in IWC Headquarters in the United States 257
Teaming and Dealing with Satellite Offices in Foreign Lands 257
Case Study 258
Summary 260

12 Anti-Fraud Functions 261
Introduction 261
Anti-Fraud Project Team Functional Tasks 261
Anti-Fraud Functions 262
Anti-Fraud Program's Non-Security Team Functions and Members 264
Case Study 265
Summary 266

13 Are We Winning the Battle? How Do We Know? Measure it! 267
Introduction 267
Measuring an Anti-Fraud Program's Costs, Benefits, Successes, and Failures 268
Common LOE Measurement Techniques for Each Function 269
Examples of Metrics by Function 270
Investigations and NCIS Metric Chares 271
Examples of Anti-Fraud Investigations Metrics 272
Process Measurements 277
Case Study 278
Summary 281

SECTION III: THE FRAUDULENT FUTURE 283

14 What Will the Fraudulent Future Hold for Corporations? 285
Introduction 285

Globalization of Business to Continue 288
Employees of the Future 288
The Future Global Corporation 289
Future of Fraud Attacks on Corporations 291
Future Anti-Fraud Protection Needs of Corporations 292
Case Study 293
Summary 293

15 The Impact of High Technology on Fraud 295
Introduction 295
High-Technology Frauds 295
High-Technology Anti-Fraud Defenses 298
Case Study 299
Summary 300

16 What the Security and Other Anti-Fraud Professionals Must Do Now to Personally Prepare to Combat Tomorrow's Frauds 301
Introduction 301
Becoming and Staying Proactive and Aggressive in Fighting Fraud 302
Getting a Fraud Education 302
Gaining Fraud-Related Certifications 303
Associations 304
Gaining Anti-Fraud Experience 305
To Conduct or not to Conduct Fraud Lectures and Write Fraud Articles 307
Case Study 307
Summary 308

17 Summary and Final Thoughts 309
Introduction 309
Summary 310
Final Thoughts 311
What Others Think About the Anti-Fraud Leadership Position in a Corporation 311
Toby J. F. Bishop, CFE, CPA, FCA, President and Chief Executive Office, Association of Certified Fraud Examiners World Headquarters 314
In Conclusion-My Thoughts 315

Some References 317
End of Line 318

About the Author 319

Index 321

Preface

I must tell you up front that the focus of this book is NOT on investigating frauds, corporations that are responsible in some form for perpetrating frauds, and the like, although some information in that regard is provided.

The emphasis in this book is on *Establishing and Managing an Anti-Fraud Program* for a corporation from an anti-fraud management and leadership viewpoint, with the emphasis on management and leadership.

Although I use the word "corporation" throughout, it also applies to government agencies, nonprofit groups, associations, privately held companies, and any entity that is concerned with the loss of its assets by fraudulent means.

Over the years, many books have been written about fraud in general and also about specific types of frauds. There have also been books written about specific fraud cases dealing with specific corporate frauds.

All of these books, however, for the most part seem to miss one basic fact: namely, the perpetration of a corporate fraud relates to attacking and stealing corporate assets of various kinds. Furthermore, the leadership role of protecting corporate assets has for decades fallen on the shoulders of the corporation's chief security officer (CSO), and it still does today.

That role will be discussed in more detail in the chapters of this book, but suffice it to say here that the corporate CSO has seemed to have abdicated that responsibility — leaving the protection of corporate assets from fraudulent attacks to others both inside and outside the corporation — to auditors and accountants.

This book was written in part to try to change that attitude and to provide justification to begin wresting that leadership responsibility from others and help make a case for justifying why fighting corporate fraud should be one of the primary duties and responsibilities of the CSO, who is indeed the leader for protecting all corporate assets.

This book also seeks to:

- Provide security professionals and others responsible for the protection of corporate assets (e.g., executive management) a roadmap for developing their own anti-fraud program.
- Help them to tailor the program to their own corporate environment.
- Help those who are interested in preventing fraud within their corporations by providing them with an awareness and a better understanding of the threats to corporations by these miscreants.
- Explain how the frauds are costing these corporations a competitive edge in the global marketplace.
- Provide guidance on how to:
  - Establish and manage a corporate anti-fraud program that is both proactive and defensive in nature.
  - Use an aggressive anti-fraud strategic approach under the leadership of the CSO.

This book will also be useful for those accountants, investigators, and auditors, as well as others who work for corporations in the areas of finance, contracts, supply, and the like, and who are interested in indicators of frauds and anti-fraud programs and in viewing the matter from other than an accountant's, investigator's, or auditor's point of view.

Hopefully, they will see that fighting corporate fraud is indeed the leadership responsibility of the CSO and push, pull, and otherwise support the CSO who wants to take on that leadership role.

I want to repeat that this book emphasizes *establishing and managing an anti-fraud program* and how to set up such a program for a corporation. As noted earlier, it is not about investigating incidents of fraud, describing fraud examination functions or incidents of fraud, and the like, except as they relate to the primary objective of establishing and managing an anti-fraud program.

The text consists of three sections and 17 chapters that will provide the reader with a practitioner's guide (a "how-to" book), augmented by some background information to put it all in perspective. The approach used should:

- Enable the reader to understand this global, fraud-threatening environment.
- Immediately put in place a useful anti-fraud program baseline under the leadership of the corporation's CSO.

The format used for this book follows the one I have used in several of my other successful books, primarily because according to many of my readers this format and approach provides basic information in an easy-to-read manner.

Because of similarities between protecting corporate assets from fraud and protecting corporate assets from various other threats agents, I have borrowed the format and some related information from some of my previous books published by Elsevier's Butterworth-Heinemann Publishers. This provides the reader the required information in one book instead of having to read through other books for the information, for example, *The Manager's Handbook for Corporate Security*.

The information provided in this book is the product of decades of experience in fighting fraud-threat agents and of information collected from multiple sources, private, public, governmental, and corporate. This information has been passed on through my professional colleagues as well as through the training and awareness courses offered by various U.S. federal government agencies and the courses and conferences provided by anti-fraud and security-related associations. If I failed to provide specific recognition within the heart of this book for the information they have provided over the years, I apologize in advance for this unintended oversight. After decades in this field, the sources and personal experiences tend to merge and blur.

I hope this book provides you with a basic foundation that will help you build an anti-fraud program and a total assets protection program. I would be very interested in hearing from you concerning your successes and failures in that regard. Also, I welcome all constructive criticism and suggestions on additional topics that you think should be addressed in any further editions of this book. Please send your questions and comments to me through my publisher: Elsevier's Butterworth-Heinemann.

Dr. Gerald L. Kovacich
Whidbey Island, Washington
U.S.A.

This page intentionally left blank

Acknowledgments

In taking on any book writing project, success will elude any writer who thinks he or she knows it all. Therefore, it was vitally important for me to be able to call on old friends and professionals to help me meet my specific objectives:

- To provide a book of useful information to help the security professionals and others who are involved in anti-fraud activities to gain information that can be quickly put to use.
- To assist in the protection of corporate assets from the global defrauders of today and tomorrow.

In that context, the following deserve special thanks:

- *Motomu Akashi*, mentor, great friend, and one of the best corporate security professionals ever to have protected a corporate asset, especially in the "Black World"!
- *William C. Boni*, Corporate Vice President and CISO, Motorola Corporation, one of our leading twenty-first-century security professionals.
- *Jerry Ervin*, good friend, former professional crime fighter, information systems security specialist, investigator, special agent, and security guru.
- *Don Evans*, InfoSec Manager, United Space Alliance, who is always there to lend a hand, provide advice to the security "rookies," and support a security conference anywhere, anytime.
- *Edward P. Halibozek*, Vice President of Security, Northrop Grumman Corporation, for his friendship, professional security advice, and his great work as a co-author.
- *Roscoe Hinton*, a very old friend and fellow fraud fighter, Special Agent (recently retired), who was my partner in fighting defrauders who targeted the U.S. government, especially in our investigations

and operations against the defrauders and other miscreants who tried to defraud the Department of Defense and the U.S. Air Force. I hope that we won more than we lost over the years! Thanks Roscoe for the advice and counsel.

- Dr. Andy Jones, Head of Security Technology Research, at the Security Research Centre for British Telecom, United Kingdom; distinguished professor, lecturer, consultant; co-author, good friend, and one of the best of what Britain has to offer to combat high-technology crimes and information systems assets protection.
- Jerry Swick, former senior telecommunications crime investigator, and retired Los Angeles Police Department Lieutenant and co-founder of their computer crime unit. A true crime fighting professional and a good friend.
- All those who work for the *Association of Certified Fraud Examiners* (ACFE) who daily lead the way in supporting the anti-fraud professionals, whether they be auditors, accountants, financial specialists, fraud examiners, security personnel, law enforcement personnel, investigators, corporate or government management — in fact, anyone who is interested in fighting fraud. Thanks especially for your many years of supporting my activities.
- The *American Society for Industrial Security* (ASIS), a security professional organization which has led the way in supporting security professionals. Thanks to them for their continued leadership and support in all they do.
- The *United States Air Force Office of Special Investigations* (AFOSI) for their years of leading the way in the DoD and the federal government in fighting fraud, supporting and providing some of the best anti-fraud training one can ever receive; as well as for being a great place to work as a special agent and fraud investigator.
- The *High Technology Crime Investigation Association* (HTCIA), which has become one of the primary leaders in investigating high-technology crimes, including telecommunications fraud, computer fraud, and various other forms of high technology-related frauds. Thanks to them, law enforcement and security professionals have been working closer together to fight high-technology crimes, including high-technology-related frauds.

Of course, thanks to my better half for over 30 years, Hsiao-yun Kovacich. I must always thank her for many years of support and giving me the "space" I need to research and write. Thanks also for her many hours of researching topics for my writings and for explaining the "thinking Asian mind"!

To the staff and project team of Butterworth-Heinemann — Mark Listewnik, Chris Nolin, Jennifer Rhuda Soucy, Pam Chester, and Kelly Weaver, the very best of professionals! Thanks again for providing great

support for another one of my book projects and for having the confidence in me to once again sign me to a book contract!

To those other professionals in the book publishing world of Elsevier's Butterworth-Heinemann, who helped make this book into a successful and professional product. Thanks for your help and professionalism: Melinda Ritchie, Marissa Hederson, and Alisa Andreola.

I also thank you, the readers, who have supported me over the years by attending my lectures and purchasing my books. I hope that my lectures and books have added to your body of knowledge and have helped you to be successful in leading the assets protection efforts of your company or government agency.

This page intentionally left blank

Introduction and Premise

This book is an introductory book on the general topic of fraud, with emphasis on fighting fraud through the *establishment and management of a formal anti-fraud program*.

The premise of this book, with which some may agree in whole, in part, or not at all, is based on the idea that today's approach to fighting fraud is not working and that a formal and aggressive anti-fraud program should be in place in all businesses and government agencies.

The leadership role of such a program falls under the duties and responsibilities of the chief security officer (CSO) of the corporation*. That person, or the person by another name, has leadership responsibility for protecting corporate assets from all threat agents whether they are thieves, defrauders, terrorists, or some other sort of miscreant.

It is logical, therefore, that the CSO lead the corporation's anti-fraud program efforts as a standalone program or probably best as an integral part and subset of an overall corporate assets protection program.

There are those who will disagree with this premise. That will be discussed in the last chapter of this book. As you read through this book, please form your own conclusions.

* As a reminder (this will be made more than once in this book): the word "corporation" is the catch-all term used in the book to describe any business whether it is a partnership, a corporation, charity, government agency, or the like. However, the anti-fraud program that is to be discussed and used as an example revolves around a corporation.

This page intentionally left blank

I

AN INTRODUCTION TO THE WONDERFUL WORLD OF FRAUD

Prior to discussing how to establish and manage a corporate anti-fraud program, it is important to set the stage for that discussion by looking at the environment where today's corporations — businesses — market and sell their products and buy their supplies.

This is important because as we go charging into the twenty-first century, we see that the business environment of the old twentieth century is yes, still there, kind of, sort of, but also rapidly changing in many ways. These changes make it almost impossible to conduct some types of corporate frauds and opens up new possibilities for perpetrating other types of frauds. Furthermore, in many ways, the defrauders of today have taken on a global profile and are no longer relegated to some local area in some small part of the world.

So, in Section I, we set the stage and hopefully provide some logic to help you understand why the corporate anti-fraud program discussed in Section II should be considered and structured (baselined) as proposed. This section is broken down into the following seven chapters:

Chapter 1 The New-Old Global Business Environment
Chapter 2 Corporate Assets, Frauds, and Other Terms — What Are They?
Chapter 3 Fraud-Related Laws
Chapter 4 Corporations Don't Commit Frauds, People Do
Chapter 5 Fighting Fraud — Whose Job Is It Anyway?
Chapter 6 Where There Is a Will There Is a Way — Fraud Schemes
Chapter 7 Fraud Cases and Commentary — Learning by Example

The logic of Section I is that you should first understand the global business environment. After all, that is where you, the leader or team member

of the corporate anti-fraud program, must work. Once the basic global business environment is understood, we move on to defining assets and frauds and their related laws. If you don't know what is meant by assets, what frauds are and their associated laws, you will have a difficult time defending corporate assets against attacks from fraud-threat agents. This basic understanding will also help you define a cost-effective process to establish and manage a successful anti-fraud program.

Once we get past the environment, laws, and definitions, it is important to discuss who commits fraud and who should lead the anti-fraud efforts for a business. As you will see, there are different opinions as to who should lead these efforts — there are "rice bowls" at stake anytime one tries to take duties and responsibilities along with their related budget away from another group. It is usually all about bureaucracy and power and not what is best for the corporation.

We will conclude Section I with an introduction to some basic fraud schemes and actual fraud cases that adversely impact corporations and, therefore, the profits and ability to successfully compete in the global marketplace. It is important to understand these threats to corporate assets and some of their modus operandi (MOs) because your anti-fraud program must be able to defend the assets against the fraud miscreants and their attacks.

Once you understand today's corporate and global fraud environment — your working environment — you will be in a better position to design, develop, implement, and manage your own anti-fraud program based not only on the global marketplace and high-technology environment, but also on the fraud-threat agents, their MOs, the specific culture and philosophy of your corporation, and its worldwide facilities.

1

The New-Old Global Business Environment

INTRODUCTION

For those who have responsibility for the protection of corporate assets, it means protecting the assets from all threats — natural and man-made. The emphasis of this book is on the protection of those assets (e.g., information, facilities, equipment, and employees) from fraudulent attacks.

In order to protect corporate assets from fraud, it is vitally important that the security professional and those in business management understand the global business environment in which the corporation will do business; they must also know where the corporate assets are located and how vulnerable they are to attacks by fraud-threat agents.

Some may argue that globalization is another word for internationalization, whereas others may contend that they are different. For our purposes, we will use the meaning stated below. It is best to leave matters relating to such definitions to academicians, whose world is the theoretical world more than the real world — at least the real world of global trade and international frauds.

> Globalization is the term used to describe the changes in societies and the world economy that result from dramatically increased international trade and cultural exchange. It describes the increase of trade and investing due to the falling of barriers and the interdependence of countries. In specifically economic contexts, the term refers almost exclusively to the effects of trade, particularly trade liberalization or "free trade". . . . More broadly, the term refers to the overall integration, and resulting increase in interdependence, among global actors (be they political, economic, or otherwise).[1]

[1] http://en.wikipedia.org/wiki/Globalization.

The "globalization" of business has been progressing for centuries. Ever since the first European explorers sought out new worlds, their purpose was to "Christianize the heathens" and trade with or steal from them. On the other side of the globe, Chinese and others were also exploring parts of the world and expanding their trading partners to those in the Middle East and Southeast Asia.

Economic globalization, the business of world trade and the "global marketplace," requires, and always has required, a mostly stable environment. Although in times of crisis and conflict, arms trading does indeed increase, that type of trade is very limited compared to other forms of trading — for example, those goods sought by the general consumers and other businesses. Trade on a global scale has been increasing for centuries, and it is expected to continue to increase, in some areas expanding exponentially and more rapidly than in the past.

As already suggested, in order for trade to flourish, businesses need a relatively stable environment; therefore, when wars break out in a region, as happened so often during the twentieth century, businesses (except for manufacturing and arms trading, of course) suffer. The recent global terrorist trends have adversely affected businesses, including tourism, in areas where the terrorists are the strongest, such as in the Middle East, followed predominantly by other Muslim nation-states or countries with major populations of Muslims, notably, Indonesia, the Philippines, and Malaysia.

You will find that no matter what threat you are protecting the corporate assets from, many of the same safeguards apply. For example, terrorists are currently being financially squeezed as the United States and other nations identify and stop the flow of funds to terrorists. This has led some terrorists to search for other sources of funding, including identity theft, credit card fraud, and other fraud-related schemes. So, it is not an exaggeration to say that your anti-fraud program may not only be protecting corporate assets but also fighting international terrorism.

Fraud-threat agents have in general much less effect on global trade and the marketplace than do terrorists. However, it has had a financial impact on affected corporations through, for example, pirated DVDs. Even the counterfeiting of goods has not slowed down trade with those nation-states such as China where it is prevalent. One finds that as nation-states improve the lives of their citizens and their economies, there is less need for counterfeiting (e.g., books, CDs, DVDs), and it tends to decline over time as in Taiwan.

Fraud-threat agents are those man-made threats that include people, their schemes, modus operandi, technology supported tools, and the like.

After World War II, trade resumed, increasing around the world, especially trade between the nation-states of Europe and the United States as a result of the Marshall Plan, which the United States implemented to help war-torn Europe rebuild. This rebuilding did not occur in China time because the communists seized control of China in 1949, and of course communism was diametrically opposed to democracy and to private ownership of businesses of the Western world. At the same time, noncommunist nation-states in the Far East, including Japan, South Korea, Thailand, and Taiwan, being capitalist-oriented regimes, began to become successful global trading partners with nation-states around the world. During that process, they regularly violated international agreements, in particular committing copyright violations, product dumping, and the like.

In the twenty-first century, we are witnessing improvements in nation-state relationships — Russia and China have normalized relationships with the United States and Europe, free trade zones have been formed, the European Union has been founded and is flourishing, and Eastern Europe has been liberated from communism, with the result that capitalism has been established in those nations.

In addition, vast and ongoing improvements in communications and in transportation (the ability to ship goods both more efficiently and more rapidly around the world) have led to increased and massive trade and with it dependencies on that global trade. These trade improvements have been brought about in part by ever-increasing improvements in technology, especially high technology driven by the microprocessor.

Current trends also show that an increasing number of nation-states are becoming democratic; the movement toward capitalism is accelerating, and global capitalism is expected to continue growing for the foreseeable future. This trend will drive more global trade, which terrorists do not want to occur, but fraud miscreants love it, for as nations modernize and open up their borders, it provides more opportunities for perpetrating fraud schemes.

Even China has loosened its hold on its people and businesses in recent years and is effectively competing as a global economic power. China is expected to successfully compete in the quest for dominance in the global marketplace in the years to come unless some drastic changes occur in the global trading environment, such as war between Taiwan and China that might include the United States.

GLOBALIZATION OF BUSINESS — BENEFITS TO NATION-STATES

Corporations continue to expand their markets, facilities, and areas of operation around the world, many of which are supported by the nation-states, which benefit from such trades in the following ways:

- Increased employment
- Rise in standard of living
- More tax money to the nation-states
- Ability of citizens to purchase cheaper goods
- Increased trade leverage in the global marketplace
- More global power through economic power

Opponents of globalization maintain that it contributes to the "exploitation of the poor." Others counter that globalization increases business development and expansion, providing employment for those who previously had little hope of finding jobs. Such arguments can be made on both sides of this issue, but one thing is almost certain: globalization will not stop.

EXPANSION OF THE GLOBAL MARKETPLACE AND THEIR AREAS OF OPERATIONS

The global marketplace has expanded over the years from Europe to the Americas and now to Asia. It is expected that future expansions must consider Africa. Although many of Africa's nation-states are presently rather unstable, with the help of more modern nation-states and their global corporations, their situation will eventually change. After all, businesses go around the world to find the cheapest resources, and as Asia becomes more and more modern with ever higher standards of living, Africa may offer the next cheap source of business resources, especially labor. The continent certainly offers some opportunities to become a center for some fraud attacks. One example that comes to mind is Nigeria, but to be fair, it appears to be trying to limit global fraud schemes.

If you look at the some of the attacks perpetrated by fraud-threat agents in Africa, you can see that the threats are already there and ready to wreak havoc on the corporations of the world that dare enter their "domain" and try to be successful. Africa may provide an "excellent test environment" where one can study

- The clash between democratic-minded people
- Corrupt dictators challenged by capitalism and democracy
- Increased adoption of high-technology devices
- Civil wars among the African states and the role fraud-threat agents play in those wars
- The impact of modern nation-states as they support their countries' businesses in the African nation-states
- The actions of miscreants to stop modernization except that which is under their control or to gain from it

> In 1999, Uganda became the first African nation to have more mobile than traditional phones. 30 other African nations followed by 2002. . . . the megacity of Lagos, Nigeria, cell phones were one of the three largest industries there, neck and neck with religion and nutritional supplements.[2]

Africa is a continent worth studying to get some idea of not only what future corporate business will contend with vis-à-vis fraud-threat agents and corrupt governments but also the techniques they may use there and spread to other continents, and vice versa.

Along with that expansion, the increased risks of today's fraud-related miscreants and their attack methodologies and schemes may be frequently encountered for the foreseeable future, and are even likely to increase over time.

What those risks are and how a security professional leading an anti-fraud program for a corporation should deal with them will vary and may depend on such things as

- Types of corporation
- Their locations worldwide
- Their ownership
- Products they produce and market
- Threats to those assets
- Vulnerabilities of the assets protection defenses
- Types of anti-fraud and asset protection controls in place

TYPES OF CORPORATIONS

The types of corporations do not appear to be primary factors when global miscreants use fraud schemes to attack a corporation's assets. In the future this may change, but for now at least the current trend will continue.

CORPORATE OWNERS AND LOCATIONS

The corporate owners are generally the stockholders who may live in various locations in the world. However, their ownership is generally

---

[2] From *Radical Evolution: The Promise and Peril of Enhancing our Minds, Our Bodies — and What it Means to Be Human*, by Joel Garreau, pg. 170. Doubleday and Company, NY. 2005.

believed to be equated to the nation-states where they have their corporate headquarters and other facilities, and not the location of the stockholders. Corporate ownership is so diverse that targeting a corporation owing to its ownership does not seem to be a plausible reason for fraud attacks against them.

Attacks against businesses may be based on their physical locations — local organized crime, local terrorists' cells needing funding, and other local fraud-threat agents. Some nation-states where their businesses are located may have weak laws, a dictatorial or possibly corrupt government, weak criminal justices systems, and so on. These all tend to provide a safer environment for global miscreants, which of course include global or local fraud-threat agents.

With today's high-technology dependencies and vulnerabilities along with our convenient and fast mobility of travel, all types of miscreants can easily move about the world plying their trade. Therefore, a corporation's location may play a role in most non–high-technology, non–Internet-related frauds.

CORPORATE PRODUCTS

The corporations' products may also be a factor in determining whether or not they will continue as targets of fraud-threat agents and other assorted miscreants in the future. Furthermore, it is important to remember that these miscreants may be domestic rather than international threat agents.

As we mentioned earlier, businesses — and global businesses maybe more so — require a stable environment in which to operate. The more chaos, the more difficult it is to successfully do business. However, as businesses expand around the world, many will take more risks and begin operating in foreign nation-states that may not have a stable government and indeed may be the home of one or more groups of miscreants. A prime example is Nigeria and its "have I got a deal for you money schemes." Chaotic internal conditions are ripe for exploitation by fraud-threat agents.

Businesses will take more risks as the global marketplace competition continues to heat up and as they continue to look for cheaper labor, less costly raw materials, and favorable operating conditions, most notably a low tax base. They need these advantages in order to compete and to offer products at lower prices based on lower operating costs. These favorable operating conditions may also be where the criminal justice system is the weakest and, therefore, ripe for exploitation by miscreants of all types, including fraud-threat agents.

It is useful to distinguish economic, political, and cultural aspects of globalization, although all three aspects are closely intertwined. The other key aspect of globalization is changes in technology, particularly in transport and communications, which it is claimed are creating a global village.[3]

As an anti-fraud professional responsible for the protection of corporate assets, you will continue to find this type of environment for the foreseeable future. How you will deal with those asset protection needs, defending them against fraud-threat agents' attacks, will offer you some of your greatest challenges.

THE HIGH-TECHNOLOGY FACTOR

The globalization of business is being supported and even driven by the continuing advancements in high technology (that technology based on the microprocessor). Thus, rapid and ever-expanding communications has also advanced the ability of fraud-threat agents to attack those they consider vulnerable to fraudulent schemes. Fraud-threat agents have been using the Internet, e-mails, cellular telephones, and the like to communicate with each other as well as to support their fraud schemes to attack their victims — their corporate targets. They have become quite sophisticated in their use of these high-technology devices and also to take advantage of their vulnerabilities.

As high technology becomes smaller, more powerful, and cheaper, fraud threat-agents will continue to take advantage of the current and future improvements in these devices.

As technology improved, transportation systems such as the sailing ships and ground transportation systems improved. For example, steam engines gave way to diesel and gasoline engines, which has had a positive impact on trade because such improvements increased their speed and size, thus allowing them to transport more products to market faster and more efficiently.

---

[3] Ibid.

The industrialization of nation-states led to expanded and increased trade throughout the world. The advent of modern transportation supported by high technology has allowed today's miscreants to operate far beyond their home territories. Today they operate around the world, and as transportation and communications improve, these fraud-threat agents will acquire additional speed and sophistication in their modus operandi and, therefore, increased ability to not only attack their targets but to do so more effectively, efficiently, and successfully.

A laptop in every pot: A *New York Times* article is provoking an online debate over whether cell phones or laptops are truly the best way to bring the Internet to the world's poor. In-house Microsoft (Research) blogger Robert Scoble agrees with his boss Bill Gates that cell phones are the best way to make Internet access universal: When he travels overseas, he sees everyone reading their phones, not using laptops. David Rothman says he hopes that MIT's cheap-laptop experiment wins out, because it's easier to read on larger screens.[4]

Because corporations depend on high technology, the most advanced high-technology nation-states have become more vulnerable to attacks, and successful attacks at that, than the Third World nation-states, which have little in the way of high-technology infrastructure and therefore, less reliance on it. This state of affairs is expected to continue into the foreseeable future.

At the same time, some previously unaffected nation-states — those not vulnerable to high-technology or other forms of attacks as they do not have that high technology-based infrastructure in place — are becoming more vulnerable to attacks of all sorts, including fraud-related attacks. For example, some nation-states have bypassed the installation of a telecommunications infrastructure based on the telephone landlines and have gone directly to cellular technology for their internal communications needs. Cellular phones are of course more vulnerable to fraud-threat agent attacks than landline telephones. Therefore, this dependency will cause fraud miscreants of the future to increasingly target the corporations and employees who make this infrastructure possible, as well as use that technology in those nation-states.

[4] http://money.cnn.com/2006/01/30/technology/browser0130/index.htm?cnn=yes.

> Intel: One billion transistors on tiny new chip: Company says it's on track to make fingernail-sized chips by the second half of 2007. . . . it had made the world's first microchip using tiny new manufacturing methods that promise to let the world's top chipmaker make more powerful, efficient processors. The fingernail-sized memory chip is etched with 1 billion transistors that are only 45 nanometers wide — about 1,000 times smaller than a red blood cell, said Mark Bohr, a leading Intel engineer. "It will pack about two times as many transistors per unit area and use less power. It will help future products and platforms deliver improved performance."[5]

NANOTECHNOLOGY

When thinking of protecting corporate assets from fraud-threat agents and their use of high-technology devices as their tools, a security professional must look into the future and see what other vulnerabilities to successful fraud attacks will emerge due to the changes in high technology. In addition, the security professional must also look to these future high technologies for tools to help them defend the corporate assets against fraud-threat agents, and protect them from other threat agents as well.

Some of the most intriguing new high technologies of the future will be based on nanotechnology. According to many government and private scientists, engineers, and business leaders, nanotechnology is the future, and in that future humans will be able to do wondrous things. What is nanotechnology?

> Nanotechnology is the understanding and control of matter at dimensions of roughly 1 to 100 nanometers, where unique phenomena enable novel applications. Encompassing nanoscale science, engineering, and technology, nanotechnology involves imaging, measuring, modeling, and manipulating matter at this length scale. . . . A nanometer is one-billionth of a meter; a sheet of paper is about 100,000 nanometers thick.[6]

According to the United States government[7]:

> The transition of nanotechnology research into manufactured products is limited today, but some products moved relatively quickly to the

---

[5] http://money.cnn.com/2006/01/25/technology/intel_chip.reut/index.htm.
[6] http://www.nano.gov/html/facts/whatIsNano.html.
[7] http://www.nano.gov/html/facts/home_facts.html.

> marketplace and already are having significant impact. For example, a new form of carbon, — the nanotube — was discovered by Sumio Iijima in 1991. In 1995, it was recognized that carbon nanotubes were excellent sources of field-emitted electrons. By 2000, the "jumbotron lamp," a nanotube-based light source that uses these field-emitted electrons to bombard a phosphor, was available as a commercial product. (Jumbotron lamps light many athletic stadiums today.) By contrast, the period of time between the modeling of the semiconducting property of germanium in 1931 and the first commercial product (the transistor radio) was 23 years.
>
> The discovery of another nanoscale carbon form, C60, the fullerene (also called the buckyball) brought the Nobel Prize in Chemistry in 1996 to Robert F. Curl Jr., Sir Harold W. Kroto, and Richard E. Smalley. It also started an avalanche of research into not only the novel characteristics of C60, but also other nanoscale materials.
>
> Nanoscale science was enabled by advances in microscopy, most notably the electron, scanning tunneling and atomic force microscopes, among others.

The United States and other modern nation-states, as well as global businesses, are racing to take advantage of what the future offers in products and services through the use of nanotechnology. One of the products that is being sought is nano-weapons.

> Public Law 108-153; 108th Congress; An Act: To authorize appropriations for nanoscience, nanoengineering, and nanotechnology research, and for other purposes. Be it enacted by the Senate and House of <<NOTE: 21st Century Nanotechnology Research and Development Act.>>. . . . The President shall implement a National Nanotechnology Program. Through appropriate agencies, councils, and the National Nanotechnology Coordination Office established in section 3, the Program shall —
>
> (1) establish the goals, priorities, and metrics for evaluation for Federal nanotechnology research, development, and other activities
> (2) invest in Federal research and development programs in nanotechnology and related sciences to achieve those goals; and
> (3) provide for interagency coordination of Federal nanotechnology research, development, and other activities undertaken pursuant to the Program.[8]

[8] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ153.108.

Nanotechnology is in just its initial stages of research and development but is rapidly growing. We have all heard of its potential uses to clear blocked arteries, repair human cells, and the like. However, as a security professional responsible for protecting corporate assets from fraud threat-agents, do you see any security issues? Of course there are the nanotechnology devices that may be embedded in an artificial fly or bee that can hover over a computer screen with an embedded video recorder or live video transmitter to capture the information shown on the computer screen, capture data flowing through computer networks or sitting in a room where sensitive discussions are taking place, and transmit that information live around the world through wireless systems.

Let's take that one step further and into the future: look at how the miscreants of the world can use such nanotechnology to destroy anything and anyone at the atomic level. Possible? Yes! Likely? If one has the knowledge and funding, it is quite possible that this may occur. Imagine buildings and people being "eaten away" by nanobots live on television. You can't see them and you can't stop them. Well, hopefully we can stop them but if security and assets protection follows today's trends into the future, the assets protection funding, especially related to defending the corporate assets against fraud-threat agents, is always after the fact and is never ready when needed.

> It appeared that nanotechnology was used to develop an artificial bug that penetrated the high security of the New World Trade Center in New York City and captured the personal information of the majority of the workers with the facility as well as the trade secrets of several corporations within the facility. A previously unknown group claimed credit for the attack and requested one billion dollars to destroy the information they had accumulated. — *Future Newspaper Headline?*

This may sound to you more like science fiction than future science facts. However, many previous science fiction stories have provided a realistic look at the future. We recommend that you research this future high technology and determine for yourself if it offers not only great benefits in the future but also great threats. In the hands of global fraud miscreants who care nothing of culture, societies, people, or their environment such as the world's great cities, the question is not will they use it? The question, rather, is when will they be able to use it? Do you think they really care about what would happen to a corporation, its suppliers, its customers, or its employees once the nano-weapons are unleashed?

Nanotechnology is rapidly approaching, and the question is: Will we be able to defeat these fraud-threat agents in the future to the point where

these miscreants will not be able to successfully use such technology against their targeted victims?

How can this technology be used to safeguard corporate assets from successful fraud attacks? For example, can it be used for product certification, and can it be built in to products where only non-pirated or non-counterfeited products will work with certain devices?

HIGH-TECHNOLOGY-RELATED FRAUDS AND OTHER CRIMES[9]

It is important to understand the history of crimes, miscreants' schemes, fraud-threat agents, and the like. The following provides some general insights into the impact of technologies of various types on the protection of corporate assets and the changing business environment threatened by these defrauders and other miscreants.

The global I-Way (Generally known as the Internet) has often been compared to a global highway for information. United States Vice President Gore in his December 1993 speech to the National Press Club commented that "today commerce rolls not just on asphalt highways but along information highways. . . . think of the national information infrastructure as a network of highways, much like the interstates of the 1950s. These are highways carrying information rather than people or goods."[10]

Many other public officials and industry leaders have also used this convenient metaphor. Although the comparison between the physical highways and the digital circuits for communication is not perfect, it nonetheless communicates a useful image. The "highway" metaphor can be especially helpful in better understanding the risks that are part of the I-Way environment.

Using the "information superhighway" metaphor should encourage security and law enforcement professionals to understand that much past experience is, in fact, relevant in this, the information period of the United States' history. The I-Way is intended to communicate in the broadest terms the extended state of connectivity and some of the vast new capabilities arising from the global telecommunications infrastructure.

ADVENT OF THE SUPERHIGHWAYS

In most major Westernized nations, the central governments invested heavily in the middle of the twentieth century to create modern high-speed

---

[9] Excerpts in part taken from the book, *I-Way Robbery: Crime on the Internet* (1999), co-authored with William Boni and printed here with permission from Butterworth-Heinemann (Elsevier).

[10] December 21, 1993. REMARKS BY THE FORMER VICE PRESIDENT, National Press Club Washington, DC.

physical highways. This was seen as a logical progression that would allow the national economies of the country to fully benefit from the potential offered by the invention of the automobile at the end of the nineteenth century. As fascinating as the early automobiles were, their ability to impact national commerce was severely constrained by the lack of paved road networks that would allow them to pass quickly between cities and regions. As recently as the 1930s, it may have required weeks for an auto to traverse the continent from New York to San Francisco, California.

Germany led the way in the 1930s with the *autobahn*; the United States followed with the interstate superhighways. In England they are known as the motorways, and in Italy they are called the *autostrada*. All represented huge capital investments that took decades to complete. In the United States alone, the freeways cost over tens of billions of dollars and took decades to complete. Why did national governments invest billions of taxes in such projects? Because these superhighways facilitated the flow of people, products, and, in time of war, troops and war materials between and among the regions of the nation.

One of the major consequences of these superhighway systems has been the beneficial spread of commerce to many cities. The advantages enjoyed by major metropolitan areas that were serviced by railroad lines, ocean or river ports, and major air terminals were now partially offset by the arterial superhighways of the nation. From mills, factories, fields, and warehouses, businesses created products and their contribution rolled away on trucks, cars, and scooters powered by the internal combustion engine and onto the superhighway system to distant locations. No longer did a business need limit itself to the expense of major transportation hubs.

In general, economists have argued that the superhighway systems contributed to the increased spread of industrial civilization and a generally higher standard of living for more people. Nation-states became a little more homogeneous as the physically mobile population relocated. People became much more mobile.

THE IMPACT OF SUPERHIGHWAYS ON FRAUDS AND OTHER CRIMES

One aspect of the automobile and superhighway system combination that was not anticipated by most citizens was how quickly criminals exploited the new possibilities offered by this combination of technologies. Perhaps the most striking examples can be drawn from the legendary criminals and gangs of the 1930s in the United States. Bank robbers like Bonnie and Clyde, "Ma" Barker, and others, especially Al Capone, exemplified the new breed of vicious criminal. Such criminals exploited submachine guns, combined with the mobility offered by the automobiles and superhighways, to pillage and plunder hapless banks and businesses.

Frequently, the criminals had better guns and cars than the police forces they confronted. Highly motivated by easy access to piles of money,

they tended to strike quickly against the poorly protected banks in the smaller towns in the country, machine guns blazing if the hapless local police force made any effort to intervene. Striking quickly, exploiting the element of surprise, they were often successful and typically escaped by automobile and superhighway.

When local police authorities became sufficiently alarmed in one area, the criminals exercised geographic flexibility and traveled down the superhighway to the next unsuspecting small town. The fact that many of these vicious criminals ended up dead did not deter others from committing similar criminal acts in similar ways. They, too, were opportunistically exploiting the environment of their time to engage in their trade. They were the direct heirs to Jesse James and the train bandits who ravaged the Old West in the United States during the post–Civil War era.

In less dramatic but still important fashion, the values, mores, and customs of the advanced nations were irrevocably changed by the combination of the automobile and the superhighway. Dishonor as a means of social control of behavior was weakened by the combination of increased mobility and the folk hero status the public ascribed to the criminals.

Though legal sanctions continued to apply to improper acts even during the advent of the automobile and superhighway, a person who was willing to move on down the superhighway to the next town could perhaps do things that their geographically constrained cousin would never consider. The stereotypical American "cowboy drifter" was now a role nearly anyone in any advanced country could play. If one committed petty theft, frauds, or other crimes locally, one had the option to escape community sanctions via the superhighway to another state and start over again. As with the bank robbers, defrauders and violent offenders found the easy escape by automobile offered continued opportunities to do their evil deeds whether a fraud, rape, murder, or other offense.

The deeds of these criminals were often widely reported through newspapers and radio broadcasts. This broadcasting of their exploits sometimes made them into "folk heroes." As part of this romantic exaggeration, they were portrayed as "Robin Hoods." Law enforcement was often portrayed as incompetent, lacking funding, knowledge, and jurisdiction to effectively pursue these criminals.

Throughout much of the United States' history, security and law enforcement responsibilities have primarily been a local affair. Training, scientific equipment, and technology such as radios or high-powered pursuit vehicles were nonexistent or in very short supply in the 1930s, and good detectives were as likely to break a case through physical or psychological coercion of suspects as through more professional police investigations. In such a world the high-powered weapons, mobility, and use of the superhighway by criminal gangs were often a winning combination.

In the late 1800s the Pinkerton Detective Agency was successful in obtaining contracts to safeguard railroads as a direct result of law

enforcement's geographic limitations during the 1870s. In a similar fashion, the gang wars in Chicago and elsewhere in the 1930s resulted in a little known United States federal government organization receiving a mandate to confront the crime problems of that time. The United States Federal Bureau of Investigation found itself tasked to be the lead agency to confront the wave of violence that local security and law enforcement professionals were unable or unwilling to confront. With some degree of success, federal law enforcement was able to prevail over the machine gun-toting robbers of the 1930s.

A SHORT HISTORY OF FRAUDS AND OTHER CRIMES VIA THE I-WAY

Let's look back at some examples of the "ages past." These examples are greatly simplified, but they support the idea that over the centuries the environment has changed, but criminals remain the same, committing crimes for the same reasons that they have always committed crimes.

During the Agricultural Age (up to about 1745 in the United States according to the Tofflers),[11] robbers stole money from banks, stores, and people, and escaped on foot or on horses. Particularly in the "colonies," criminals were limited to areas where they could walk or run to and/or away from apprehension. Using horses, they could make faster getaways! The only knowledge they required was how to ride a horse; where to go to get the money, goods, or other valuables they planned on stealing; and a plan for the crime.

If they could not afford a horse, they could always steal one. So the horse was one of the tools used to support committing the crime. This, coupled with their other basic tools of a good fraud scheme and a plan, meant they were ready to commit their frauds.

With the advent of the Industrial Age (about 1745 to 1956 in the United States according to the Tofflers) came the automobile, which greatly enhanced the robbers' ability to steal or defraud a person or business. Robbers still robbed and defrauders still committed frauds, but now they were able to expand their crime areas because through the automobile they could travel farther in less time. Also, they could get away faster and hide farther away from the crime scene.

So, the automobile did for the robbers, defrauders, and other miscreants in this age what the horse did for them in the earlier age: it expanded their crime areas; they also were able to get away farther and faster.

The advent of the superhighways exponentially increased the criminals' opportunities. No longer required to use dirt or country roads and

[11] The Tofflers discuss this topic in their numerous books. It is suggested that the reader do a "search" online for their books and read those that may help better understand our history.

two-lane highways, the automobile coupled with the superhighway greatly expanded their crime area. As before, criminals used this "new technology" and enhanced environment to help commit the same types of frauds they had always committed and for the same reasons. In this case, as in days past, they purchased their method of transportation — this time the car — or they stole one. They still needed a fraud scheme as their weapon and a plan.

SUPERHIGHWAY FRAUDS AND OTHER CRIMES TO I-WAY ROBBERIES

So why is all this history relevant to the security and law enforcement professional in dealing with the fraud and other crime challenges raised by the I-Way? Let's compare the environment of the 1930–1940s in the United States with the I-Way world of the 1990s:

1930–1940s

- Mobile criminals (automobiles + superhighways)
- Weakest targets selected for exploitation
- Employment of advanced technology (machine guns and commando tactics)
- Sequential attacks against targets of opportunity
- Local security and law enforcement poorly equipped for response
- Geographic limitations on investigations and response
- General decline in effectiveness of social controls due to mobility technology (superhighways and automobiles)
- U.S. federal government intervention via FBI (stop the bank robbers and bootleggers)

1990s–Present

- Mobile criminals (modems + I-Way)
- Weakest targets subject to exploitation
- Advanced technology (vulnerability scanners, information warfare tactics)
- Sequential attacks against targets of opportunity
- Local security and law enforcement poorly equipped for response
- Geographic limitations (national borders) on investigations and response
- General decline in effectiveness of social controls due to global mobility technology (microcomputers and I-Way)
- U.S. federal government intervention via FBI (stop the I-Way robbers, defrauders, and hackers)

When viewed in perspective, one can see that the I-Way defrauders and other miscreants of the Information Age have much in common with the

superhighway robbers of the Industrial Age. Based on these considerations, security and law enforcement professionals should therefore understand that little has really changed over the years. Therefore, the problems, issues, and approaches to dealing with them will be very similar. We must emphasize that what did not work before will not work now, and what worked before may or may not work in the present. Law enforcement and security professionals should learn from history and use the appropriate methods and techniques.

One overwhelming distinction is obvious. Whereas in the earlier era the U.S. federal government could respond to citizens' concerns about rampant lawlessness by empowering the FBI to enforce U.S. laws, that is not the case today.

The I-Way is global in scope and is growing fastest in nations and continents that are not likely to take direction from the United States and where the United States has no jurisdiction. How will security and law enforcement professionals of a nation influence the global response necessary to confront the more serious risks that the I-Way will create? In the absence of a global "I-Way Patrol," each individual nation's response is likely to fall short of effectively addressing the complete spectrum of criminal threats.

At a news conference held after an all-day meeting at FBI headquarters of the Justice Ministers of the G-8 countries (the largest industrialized countries in the world) in December 1997, former United States attorney general Janet Reno said, "Criminals no longer are restricted by national boundaries. . . . If we are to keep up with cybercrime, we must work together as never before."[12] The news release from this important meeting went on to list the following areas where these major nations have agreed to collaborate:

- Assign adequate number of properly trained and equipped law enforcement personnel to investigate high-tech crimes.
- Improve ways to track attacks on computer networks.
- When extradition is not possible, prosecute criminals in the country where they are found.
- Preserve key evidence on computer networks.
- Review the legal codes in each nation to ensure that appropriate crimes for computer wrongdoing are proscribed and that the language makes it easier to investigate the crimes.
- Establish close cooperation with the private sector to develop new ways of detecting and preventing computer crimes.
- Make increased efforts to use new communications technologies, such as video teleconferencing, to obtain testimony from witnesses in other nations.

[12] "Nations Band Together Against Cybercrime" Reuters 10 Dec 97.

These are essential steps, even if they are general in nature. However, the past track record of nations cooperating in such efforts has evidenced little past success. Therefore one should not be overly optimistic about the future based only on these actions. The global reach of the I-Way and the difficulties of obtaining jurisdiction over perpetrators represent one of the greatest challenges in dealing with I-Way robbers. To the extent that the collaboration of the G-8 nations ultimately extends to the other nations of the globe, perhaps under the broader auspices of the United Nations or other agencies, organizations can have increased confidence that even the most sophisticated I-Way robbers may ultimately face prosecution.

As law enforcement has adapted its methods and incorporated new technology to combat frauds, private organizations also have adopted various strategies to combat risks to their interests. It is likely that many organizations, confronted with increasing risks from the I-Way, will choose to respond as the railroad industry did in the 1880s in the United States.

At that time the railroads, frustrated by the largely ineffective nature of geographically limited law enforcement, engaged the Pinkerton Detective Agency to help protect corporate interests against the James gang and similar highly mobile criminal gangs. It is possible, indeed likely, that many large organizations will choose to engage the resources of private sector specialists (cyber-sleuths or digital detectives) to help them resolve I-way-enabled frauds directed against them. This may happen because the limited resources in the public sector are directed to larger or more serious crimes, or simply because public agencies will generally take longer to complete an investigation owing to the many competing priorities.

I-WAY ROBBERY — ITS PREVALENCE

Over the years, there have been dramatic increases in frauds and other crimes via the I-Way. Why the dramatic increase in such reports and apparent losses? Many factors have contributed to this trend, but in large part, these trends have developed because the I-Way makes every organization's system an on and off ramp, which puts computer systems at greater risk than ever before. With the rapid pace of growth in the I-Way, there are simply more computer systems that are more accessible than ever to more people in more places on the planet.

Because the I-Way connected computers and networks contain more valuable information and other valuable assets (including digital forms of money), they are thus more important to businesses and government agencies than ever before.

The same applies to the I-Way for the I-Way robbers, because the information that travels the I-Way and their ability to share methods, tools, and techniques is also one of their most important assets. Many tools and utilities are freely available to virtually anyone with a modem and I-Way access. There are perhaps thousands of public sites and an unknown

number of private bulletin boards and chat areas in which the most clandestine and capable I-Way robbers, defrauders, and other miscreants in the underground share tools, techniques, and methods of defeating security measures. With a vast array of tools to draw from, is it at all surprising that penetrations are becoming more common?

THERE IS NO I-WAY PATROL TO STOP I-WAY ROBBERS

It will come as no great surprise to security and law enforcement and professionals that criminals are willing to make the effort to transition their trade to the I-Way. Recall the classic comment by convicted bank robber Willy Sutton, who, when asked why he robbed banks, told his interviewer "Because that's where the money is!" Following that comment, *where* is the money in today's global economy? As almost every high school student now knows, it is in computers, wire transfer networks, and the global I-Way itself. It would be totally unrealistic to expect Willy's heirs to change their chosen profession merely because computers and networks are supplanting tangible cash in commerce.

Although computer fraud has existed for decades, some experts believe that computer technology today is roughly where automotive technology was in 1905 and that we have not yet seen the full extent of computer-related crime.[13] Jonathan Winer, deputy assistant secretary of state in the international narcotics and law enforcement arm of the State Department, has said: "We have created an information superhighway without speed limits and without traffic controls."[14] Many public and private sector representatives have expressed significant concern over the ability of criminals to use the I-Way to launder money and commit other crimes.[15]

GLOBAL CONNECTIVITY VIA THE I-WAY = GLOBAL EXPOSURE TO ATTACKS BY FRAUD-THREAT AGENTS AND OTHER MISCREANTS

It is vital that security and law enforcement professionals recognize how radically different this new environment is. As recently as the late 1980s, the most common form of nonemployee computer crime probably involved a teen-ager in the local telephone dialing area using a "war dialer"[16] to try to emulate the movie *War Games*.

In the 1980s, a company could protect itself against a wide range of risks with relatively inexpensive security technology. In today's era of

---

[13] Tuesday, September 15, 1998, 9:47 AM, NewsBits Reuters.
[14] Ibid.
[15] Ibid.
[16] Ibid.

global connectivity and access one should not assume that what was sufficient for simpler times will suffice for the present. Those organizations that choose to ignore their increasing vulnerability and trust haphazard security measures may well suffer serious losses. Potential I-Way robbers are not likely to ignore forever poorly protected on ramps that have valuable assets.

An I-Way robber is no more likely to ignore an easy network-firewall penetration any more than his distant relative in the 1930s would have passed an unlocked bank vault. Just as banks and businesses in the past had to harden their facilities, hire trustworthy guards, and install video surveillance cameras and alarms to safeguard their cash vaults, today's "digital data vaults" require enhanced protection. When organizations fail to invest adequately in protection, they run the risk of damage or loss of their key assets.

Any successful anti-fraud program must include controls to protect the corporate assets made accessible due to the I-Way and its corporations' on and off ramps, as well as internal corporate networks. It must also take into account the continuous changes in high technologies that often open corporations' assets to new fraud schemes.

CAPABILITIES AND LIMITATIONS OF LAW ENFORCEMENT

If tidal waves of criminal enterprise are about to overwhelm the I-Way and impact this new commercial medium, what can we expect from the "I-Way patrol"? Unless things change drastically, it would seem not much. First, every security and law enforcement professional must understand that, at present, no single, central organization has the responsibility and capability to patrol and protect the global I-Way; there is not (at least not yet) a global "I-Way patrol." The reasons are readily apparent considering the current state of planetary political organization.

The nation-state remains the primary organizing unit for most of the Earth's population, and it is unlikely any country would tolerate an international I-Way patrol with jurisdiction to seize and prosecute suspects or even proven perpetrators of activity that is criminal in another country. The uproar that arose in Mexico when U.S. government agents seized and prosecuted a physician affiliated with a drug cartel for his involvement with a U.S. Drug Enforcement agent's murder provides a real-world example of the consequences of unilateral transborder law enforcement. However, to put these matters in a little different perspective, imagine the uproar in the United States if a non-United States police force had authority to arrest U.S. citizens because they posted comments that were considered sacrilegious to another country's religious/spiritual leadership.

Rather than create a global I-Way patrol, it is more reasonable to expect updated extradition treaties as probably the best short-term answer

to the problems of obtaining jurisdiction over I-Way robbers. For example, note that Argentina initially declined to extradite to the United States a young man who admitted he hacked into a number of U.S. government systems via the I-Way, including NASA's systems. Although this was a criminal act under relevant United States statutes, he had not violated any laws of his homeland. Although he ultimately gave himself up to authorities and pled guilty to the charges, his surrender was done voluntarily.

The inconsistencies in legal language, statutes, and codes from country to country are just one of the major problems associated with policing the global I-way. In the absence of well-developed international agreements and treaties, and lacking any sort of I-Way patrol or even common policing standards, it is likely that organizations will be subject to criminal activities originating in another country. If this situation arises, there may be no local authority able or willing to pursue a criminal investigation against the I-Way robbers.

CHALLENGES TO SECURITY PROFESSIONALS AND OTHERS

The I-Way has brought with it many new challenges to the security professional. Just learning the vocabulary and technical terms arising from the I-Way is a significant issue. Some also look at the challenges from the I-Way robbers, fraudsters, spies, and terrorists as something completely new. Looking closer, we find little that is truly new from the I-Way robbers. Few of the basic techniques or objectives of these criminals have changed. What is actually new is the *environment* in which they operate.

It is now the Information Age, and all business and government agencies that operate today inhabit a technology-driven environment. It is the microprocessor-based, network-intensive environment alone that is new. Make no mistake: the "bad guys" and "girls" still have the same motives, opportunities, and rationalizations for committing their frauds and other crimes.

Today's generation of criminals is still committing crimes and frauds for precisely the same reasons that they and their predecessors have always committed crimes: it is how they choose to earn their livelihood. However, to be successful in the Information Age, they must now commit crimes in the contemporary business environment. With the rapid growth of the I-Way and I-Way Commerce (also known as Electronic Business in some parts of the world), I-Way robbers must operate with knowledge of the I-Way.

Criminals are attempting to do what they have always done: to steal, defraud, and subvert others for personal, corporate, national, and/or political gain. The methods they use are largely the same, and they only change when the I-Way environment requires them to change to achieve their objectives.

If we really think about it, do we have any reason to believe criminals, that is, defrauders, really are much different today than they were in the days of Jesse James? Even in a world featuring computers, coupled with the digital, virtual I-Way, and the increased use of I-Way commerce, "cyber defrauders" still have the same objectives: to take someone's money or other assets and to convert them for their personal benefit. However, no longer bounded by physical locations or very much by time, the I-Way now allows them to have global mobility and to escape in nanoseconds.

CASE STUDY 1

As the chief security officer for the XYZ Corporation, your boss told you that next year the corporation will be expanding its business, which includes the manufacturing of their widgets, into Nigeria. You are told that since you have primary responsibility for leading the corporation's assets protection efforts, you must tell executive management what needs to be done to protect the corporate assets en route to Nigeria and in-country at their new satellite location.

Executive management is concerned with protection of corporate assets and has heard many negative stories about the massive numbers of frauds being perpetrated out of Nigeria. So, they have a serious concern about establishing a facility there. However, they must do so inasmuch as the Nigerian government has offered favorable tax benefits as well as other incentives to build a factory there, and such a facility would help the corporation to achieve a more competitive position in the global marketplace.

So now what do you do? No, you don't leave the corporation, for you need the job and medical benefits, and it also pays well. The first step, of course, would be to contact those involved, probably a project team, who are responsible for successfully making this event happen. You should then become a member of that project team.

As a member of that project team, you should also consider the following:

- Develop and brief the team on an assets protection operational plan, which includes an anti-fraud aspect, equipment, and people, for moving the assets to Nigeria.
- Include the following subsets:
  - An operational security plan
  - A transportation plan
  - An executive protection plan
  - An employee protection plan
  - A budget plan
- Determine whether a new building will be constructed or whether a current building will be used instead. In either case, a facility physical

security plan to include physical security survey must be completed. Construction, supply, and logistics frauds are a major concern here.
- With employees traveling to Nigeria prior to the operation of the new facility, include a travel security plan that encompasses awareness of current and past fraud schemes against individuals.
- Conduct research on Nigeria, its culture, customs, society, and such.
- Learn to speak the local language as much as possible.
- Coordinate with your nation-state's government agencies, such as the U.S. Department of State and the U.S. Embassy in Nigeria, to determine the fraud-threat environment.
- Coordinate with the local authorities — local police, and government security personnel stationed in the area of the corporation's proposed facility; identify localized fraud schemes; profile defrauders and the like.
- Be actively involved in this project.

These are part of just a high-level outline as to what should be considered for implementation, to include the anti-fraud aspects. Can you identify other major tasks to ensure that a successful facility is established?

CASE STUDY 2

As the CSO of an international corporation, how would you go about determining the corporation's position in the global marketplace, its visibility to threat agents, and the vulnerability of the corporate assets to these fraud miscreants?

One approach would be to:

- Talk to the corporation's business office staff.
- Talk to the corporation's marketing and sales staff.
- Search the Internet for information on the corporation, its competitors, and its global visibility.
- Talk to the corporation's public relations staff.
- Talk to the corporate auditors.
- Review corporate security department's history of investigations and inquiries.
- Talk to the corporate ethics director.
- Search the Internet for fraud schemes and cases that may impact or apply to the corporation.

By taking these steps, you can begin to build a corporate profile and begin to answer the above question.

SUMMARY

Corporations are increasingly operating in a global marketplace and are therefore more susceptible to fraud-threat agent attacks anywhere in the world.

Corporations will continue to expand their global operations driven and supported by high technology. Although high technology is a crucial factor in lowering operating costs and increasing profits, it also makes corporate assets more vulnerable to all types of attacks. To date, many fraud-threat agents have used high technology as both tools and targets. The trend is expected to continue into the future.

Careful study of the information presented in this chapter and other publicly available data concerning a short history of globalization and frauds reveals several common themes:

- Globalization will continue.
- Computer/network-enabled frauds are a rapidly growing component of global fraud statistics.
- No one in business, government, or academe really knows the full extent or the complete nature of frauds that have already been committed or are happening at this moment.
- We can conclude that, although the I-Way and information access enabling technologies like the Web browser–server combinations are creating more complex environments, we should not expect that complexity alone will protect valuable resources against losses.

Criminals over the ages have proven themselves highly adaptable, and they already appear to be capable and willing to exploit globalization and technologies for their benefit.

As with the criminals, security professionals and law enforcement officers have all been challenged to adapt, learning in earlier ages to ride horses, drive automobiles, and now exploit the computers and networks to combat the latest generation of "digital desperados."

2

Corporate Assets, Frauds, and Other Terms — What Are They?

INTRODUCTION

To discuss how to fight frauds related to corporations and how to establish and manage an anti-fraud program for any business, for example, a corporation, it is important that we begin with a basic understanding of terminology. In this case, it is important to define the basic fraud-related terms. We will use those terms and definitions that are generally accepted throughout the security, auditing, and fraud examiner's professions,[1] and that means those terms that are legally defined. After all, those are about the only definitions that can be used in a court of law or any other legal proceeding.

Why is terminology so important? It is important because if you do not use legally defined terms and establish an anti-fraud program that includes investigations and inquiries into fraud allegations based on those terms, you may find that you cannot accomplish prosecution support or other forms of disciplinary action that are based on improper elements of proof. Remember: elements of proof for frauds are derived from the definitions of fraud terms.

[1] This is also important since many of the readers may be reading about frauds for the first time, and this will make it more convenient than having the reader rummage through books, articles and Internet sites to determine what is meant by what I've said, e.g. definitions.

In defining the general term *fraud* and providing samples of various forms of frauds, let's begin with a basic understanding of what a fraud is or what some forms of fraud actually are. It is also vitally important that you understand the "elements of proof" of the various types of frauds, for you must provide evidence that the identified fraud miscreant actually perpetrated a fraud and did not just make a mistake.

> In matters of fraud, proving "intent" is the key ingredient. Therefore, any anti-fraud program must provide controls and such that facilitate that proof.

Human errors often occur since we human beings are not perfect. It is often difficult to determine if someone just made a mistake or in fact intended to commit a fraudulent act. In all cases, proving "intent" is vital. By the way, one cannot perpetrate a fraud by mistake.

This "proof of intent" is vital in conducting:

- Fraud inquiries (where corporate policies or procedures have been violated but not civil or criminal laws)
- Investigations (where one or more civil, e.g., regulation, or criminal laws has been violated)

It is also vital when establishing your corporate anti-fraud program. Do you know why? Think about it. If you don't have policies, procedures, and processes in place that can help show that the employee violated some corporate or governmental laws or regulations and did so *knowingly*, it will be much more difficult, if not impossible, to show that the employee *intended* to defraud the corporation.

DEFINITION OF GENERAL FRAUD[2]

Fraud is generally defined as:

- A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.

---

[2] The definitions cited were reprinted from *Black's Law Dictionary*, Eighth Edition, Bryan A. Garner, Editor In Chief; published by West Publishing Company, St. Paul, MN; with permission of Thomas West.

- A misrepresentation made recklessly without belief in its truth to induce another person to act.
- A tort arising from a knowing misrepresentation, concealment of a material fact, or reckless misrepresentation made to induce another to act to his or her detriment.
- Unconscionable dealing; especially contract law, and the unfair use of the power arising out of the parties' relative positions and resulting in an unconscionable bargain.

Actual Fraud is defined as:

- A concealment or false representation through a statement or conduct that injures another who relies on it in acting.

It also comprises three elements:

- Fraud in fact
- Positive fraud
- Moral fraud

> In the case of an "actual fraud," you want to be able to prove these three elements and to have policies, procedures, and processes in place to provide controls that will show that it was in fact an actual fraud that an employee, supplier, customer, or others committed and it was their intent to do so.

It is also vitally important that the person committing the actual fraud did so

- Knowing what the corporation's policies, procedures, and processes were; and that the fraudster
- Knew that those policies, procedures, and processes were to be followed at all times, ideally by so attesting to this knowledge in writing — which is a key process in your anti-fraud program.

This consideration is important because in the U.S. judicial system today, it generally must be shown that the person perpetrating the fraud against the corporation, especially an employee or someone who has a business working relationship with the corporation, was aware of the policies, procedures, and processes that were violated and/or knew that such actions were against corporate policy, procedures, or civil or criminal laws.

In the United States, an investigator, fraud examiner, or security professional cannot rely on the expression "ignorance of the law is no excuse"

to help "make the case" against the defrauder. In fact, there are some indications that the alleged defrauder must also be told in advance when making them aware of anti-fraud policies and procedures to follow the consequences of his or her actions of not following the "rules". It is especially important in these days of "It's not my fault!" where personal responsibility seems to have taken an extended holiday.

Remember that unless you are a lawyer and feel confident in defining a fraud and how to go about identifying the elements of proof, you should coordinate with the corporate legal staff and get their input when such legal issues arise. It will not only save you time and possible embarrassment but will help ensure that your actions do not cause a lawsuit against the corporation, which may have not otherwise been contemplated by the "offended party."

It may also to help ensure that your employment is not terminated over such matters. Also remember that "anyone can sue anyone over anything." However, with the proper anti-fraud program elements in place, you have a better chance of ensuring that the fraud miscreant does not successfully win his or her lawsuit.

Even though the preceding and succeeding definitions apply to the United States and possibly some other countries, most modern countries have similar laws that basically require the same elements of proof. However, a global corporation must know the specific fraud-related statutes in each country and take these statutes into consideration when developing and managing an anti-fraud program for a global business.

> Fraud, in law, general term for any instance in which one party deceives or takes unfair advantage of another. Any means used by one person to deceive another may be defined as fraud. For example, if a person represents himself or herself as the agent of a business with which he or she is unconnected and causes another to make a contract to the other party's disadvantage or injury, the first party is guilty of fraud.
>
> Furthermore, if, in making a contract, a person obtains an unjust advantage because of the youth, defective mental capacity, or intoxicated condition of the other party to the contract, he or she is guilty of fraud.
>
> In a court of law, it is necessary to prove that a representation was made as a statement of fact; that it was untrue and known to be untrue; that it was made with intent to deceive and to induce the other party to act upon it; and that the other party relied on it and was induced to act or not to act, to his or her injury or damage.
>
> In equity, fraud includes any act, omission, or concealment involving a breach of legal or equitable duty or trust, which results in disadvantage or injury to another. An example of fraud in this sense is the act of an insolvent who contrives to give one creditor an advantage over

the others. Fraud can also be constructive, that is, deemed fraud by interpretation. The sole difference in the case of constructive fraud is that no dishonest intent need be adduced. It arises from a breach of duty, such as the breach of a fiduciary relationship in which a trust or confidence has been betrayed.[3]

SPECIFIC FRAUD DEFINITIONS

Each of the various types of frauds has its own definition that incorporates the general definition of fraud but also includes specifics related to various types of fraud. Following are some of the basic types of frauds that every security professional or fraud fighter should know:

- Civil Fraud: An intentional but not willful evasion of taxes. The distinction between an intentional (i.e., civil) and willful (i.e., criminal) fraud is not always clear, but civil fraud carries only a monetary, noncriminal penalty.
- Criminal Fraud: Fraud that has been made illegal by statute and that subjects the offender to criminal penalties such as fines and imprisonment.
- Fraud Feasor: A person who has committed fraud; also termed defrauder.
- Fraudulent Act: Conduct involving bad faith, dishonesty, a lack of integrity, or moral turpitude.

In addition and depending on your corporate environment (e.g., financial, manufacturing), you should also have a basic understanding and definitions of the following types of frauds[4]:

- Bank Fraud
- Bandkruptcy Fraud
- Constructive Fraud
- Extrinsic Fraud
- Fraud in Law
- Fraud in Inducement
- Fraud on the Community
- Fraud on the Court
- Fraud on the Market
- Fraud on the Patent Office
- Insurance Fraud
- Intrinsic Fraud
- Long-firm Fraud
- Mail Fraud
- Promissory Fraud
- Wire Fraud
- Fraudulen Alienation
- Fraudulent Banking
- Fraudulent Conveyance

[3] Microsoft Encarta Encyclopedia Standard 2004.
[4] These terms are from Black's Law Dictionary as noted earlier.

CORPORATE ASSETS

When discussing corporate fraud, we are talking about some fraud miscreant illegally gaining access to or fraudulently impacting a corporate asset or assets. Therefore, it is important to understand what an asset is and the various types of assets. After all, the objective of an anti-fraud program is to protect corporate assets from fraud.

In order to develop, establish, and maintain a viable anti-fraud program, you must know what assets are and the role your specific corporate assets play in your anti-fraud program, as well as their value to some *fraud feasor* or *defrauder*.

Yes, I am sure you have the general idea of what an asset is; however, it is important to know what an asset is in legal terms and also the various types of assets. After all, you don't want to develop an anti-fraud program based on what you think an asset is and discover your hard work is for naught when your corporation goes to court to get that asset back and ensure the perpetrators are held accountable. (This is a nice way of saying that they are found guilty and imprisoned or that a monetary punishment is exacted against them.)

With that in mind, the following definitions are provided concerning "assets":

- Asset
  - An item that is owned and has value
  - The entries on a balance sheet showing the items of property owned, including cash, inventory, equipment, real estate, accounts receivable, and goodwill
  - All the property of a person (especially a bankrupt or deceased person) available for paying debts or for distribution

If you want to show that someone defrauded the corporation of one or more of its assets, you must be able to show that the asset or assets were owned by the corporation and that the asset or assets had value.[5]

Please keep this consideration in mind when you develop and manage an anti-fraud program. If you cannot show that the corporation owned the asset and that it had some value to the corporation, then it may not meet the legal definition of an asset. Your anti-fraud program must ensure that

[5] The information provided here and throughout this book are based on my investigative and security experiences over 45 years. I am not a lawyer nor do I have a law degree. It is important that what you read be taken in that context. Each incident is somewhat different, and the corporate legal staff and/or prosecutor must be in the coordination loop to ensure all legal requirements such as the elements of proof are met.

there is documentation to show both. Some basic asset definitions are as follows:[6]

- Capital Asset: Long-term asset used in the operation of a business or used to produce goods or services, such as equipment, land, or an industrial plant (also termed fixed asset).
- Commercial Assets: The aggregate of available property, stock in trade, cash, and other assets belonging to a merchant.
- Intangible Asset: Any nonphysical asset or resource that can be amortized or converted to cash such as patents, goodwill, and computer programs, or a right to something, such as services paid for in advance.
- Real Asset: An asset in the form of land. Loosely, any tangible asset. Also termed hard asset.
- Tangible Asset: An asset that has a physical existence and is capable of being assigned a value.

Other asset terms you may need to know, again depending on your corporate products and environment, are as follows:[7]

- Accrued Asset
- Admitted Asset
- Appointive Asset
- Assets by Descent
- Asset in Hand
- Asset Under Management
- Current Asset
- Dead Asset
- Earning Asset
- Equitable Asset
- Frozen Asset
- Hidden Asset
- Illiquid Asset
- Individual Asset
- Legal Asset
- Mass Asset
- Net Quick Assets
- Net Asset
- Nominal Asset
- Nonadmitted Asset
- Nonprobate Asset
- Personal Asset
- Premarital Asset
- Quick Asset
- Wasting Asset
- Asset Acquisition
- Asset Allocation
- Asset-Coverage Test
- Asset-Depreciation Range

OTHER TERMS AND DEFINITIONS

Some other terms and definitions that will be used throughout this book and must be known in order to establish and manage a successful antifraud program for your business are as follows:[8]

---

[6] These definitions also taken from Black's Law Dictionary.

[7] Ibid.

[8] These are general definitions taken from various sources over the years.

- Policy: A course of action; a program of actions adopted by an individual, group, or government, or the set of principles on which they are based; shrewdness or prudence, especially in the pursuit of a particular course of action.
- Procedures: The established methods for doing something.
- Processes: A series of actions taken toward a particular aim; treatment or preparation of something in a series of steps or actions.
- Plans: Schemes for achieving objectives; a method of doing something that is worked out usually in some detail before it is begun and that may be written down in some form or possibly retained in memory.
- Projects: Tasks or schemes that require a large amount of time, effort, and planning to complete; an organized unit of work.
- Formal Project Plan: A formal project that is documented in writing and includes the combination of tasks to be accomplished to meet a specific objective or objectives, has a beginning and an ending date, and will take more than 30 days to complete. It may or may not have specific resources identified and allocated to it. It is monitored by management on a periodic basis.
- Informal Project Plan: A plan that may or may not meet the criteria of a Formal Project Plan with the exception that it will not take more than 30 days to complete and will not be formally monitored by management.

Some of these definitions may or not apply to your particular working environment. However, they are presented here to assist you in developing and managing your anti-fraud program. Specifically, they provide a baseline on which you can build such a program by incorporating into it the various types of assets that apply to your working environment. It also ensures that your anti-fraud and assets protection policies, procedures, processes, plans, and projects provide for any needed successful disciplinary action, civil lawsuits, or criminal prosecutions.

CASE STUDY

As the leader for your corporation's anti-fraud program, you are asked to provide material to be used as part of a total assets protection awareness briefing to be given to new employees of the corporation as part of their orientation into the corporation's working environment.

These monthly new-hire briefings will be given by a staff member of the Human Resources Department who is not familiar, in detail, with the anti-fraud program. The time spent on the anti-fraud topic will be limited to three slides or about five minutes.

What informational slides would you provide for that briefing?

At the International Widget Corporation (IWC), the anti-fraud program leader provided the following slides:

1. A summary chart of IWC's anti-fraud program
2. A summary chart of the definition of what IWC considers a fraud and employees' reporting requirements
3. A summary chart citing policy references and the names and contact numbers for yourself and others who could provide additional information on the IWC anti-fraud program.

What information would you provide the awareness briefing person in your three slides?

SUMMARY

In order to build a successful anti-fraud program as part of or separate from a corporate assets protection program, one must know what a fraud is and the various types of frauds. It is also important to know what an asset is and the various types of assets that you must consider in building your anti-fraud program for your particular corporation and its working environment.

You must define the elements of proof required to "prove" that a fraud has occurred against your corporation, and you must be able to support any wanted disciplinary action, civil lawsuits, and/or criminal prosecution. After all, if your anti-fraud program does not provide the necessary policies, procedures, processes, plans, and projects, you may lose corporate assets and not be able to successfully do anything about it.

This page intentionally left blank

3

Fraud-Related Laws

INTRODUCTION

When fighting fraud where the corporation is the "victim," it is important to keep in mind the laws that may apply. After all, when you are defending the corporation against fraudulent attacks, you also want to be in a position to support corporate disciplinary action of employees and to support the civil or criminal prosecution of the fraud miscreants, whether they are employees or outsiders.

It is vitally important that your corporate anti-fraud program have in place those policies, procedures, and processes leading to controls that not only help mitigate fraud-threat agent attacks but also provide for the elements of proof required to prove that a fraud has occurred. In addition, your program should provide reasonable controls that would assist in identifying the fraud-threat agent.

> The element of fraud which tends to stymie successful prosecution is the obligation to investigate. It falls on potential investors or customers to fully investigate a proposal before any money exchanges hands. Failure to take appropriate measures at the time of the proposal can seriously weaken a fraud case in court later. The accused can claim that the alleged victim had every opportunity to discover the potential for fraud and failed to investigate the matter thoroughly. Once a party enters into a legally binding contract, remorse over the terms of the deal is not the same as fraud.[1]

If you, in coordination with the corporate legal staff, cannot identify a law that has been violated, it may not be a fraud in legal terms but may possibly be just a violation of corporate policy. If it is a violation of corporate

[1] http://www.wisegeek.com/what-is-fraud.htm.

policy, disciplinary action may be justified against corporate employees, but obviously the corporation would not be in a position to discipline non-corporate employees. The corporation may, however, be in a position to take some civil action against the attackers (e.g., suppliers, customers). For example, the violation may be one related to a breach of contract only.

FRAUD COULD INFLATE COST OF TERRORIST ATTACKS Officials are gearing for a possible wave of insurance fraud that will inflate the financial cost of the recent terrorist attacks, warns the Coalition Against Insurance Fraud, a Washington-based watchdog. "Disasters inevitably attract scam artists who try to exploit emergency conditions for profit. The only question is how much insurance fraud will occur, and how much it will cost policyholders," said Dennis Jay, the coalition's executive director. Most scams will involve phony or inflated claims. But crooks also could peddle fake, overpriced or unneeded "terrorism" or "travel" coverage to jittery consumers, Jay said. Insurers likely will pay most basic attack-related claims upfront, then revisit the suspicious claims when the emergency subsides, Jay said. Anti-fraud agencies and insurers in the New York region already are setting up coordinated anti-fraud operations to root out scams as early as possible. Investigators have uncovered several suspicious claims, but still are probing whether they're true scams. Personal and commercial lines are vulnerable to fraud. It may take weeks, however, before officials can estimate the seriousness of the fraud problem. Suspicious commercial claims that are large and complex could take longer to detect, Jay noted. . . . Only a small fraction of claims will be phony, but even a tiny portion of the huge overall claim volume could mean millions of stolen dollars, Jay said. Officials are preparing for insurance scams such as these: Fake death, Business interruption, Commercial property, Workers compensation, Personal property, Padded repairs, Phony auto claims, Backdating of policies. and Phony, overpriced or unneeded insurance.[2]

SOME U.S. FEDERAL FRAUD-RELATED LAWS[3]

The following are some of the primary federal anti-fraud laws in the United States:[4]

---

[2] http://www.insurancefraud.org/releases_2001.htm#060701.

[3] It is important to note that these are not all of the possible laws on which a corporation may support prosecution against attackers but just a sampling. As always when it comes to legal matters, close coordination must be maintained with the corporate legal staff and reliance on them for guidance. However, such laws should be considered when establishing and managing your corporation's anti-fraud program.

[4] http://www.access.gpo.gov/uscode/title18/parti_chapter47_.html.

- Sec. 1001. Statements or entries generally
- Sec. 1002. Possession of false papers to defraud United States
- Sec. 1003. Demands against the United States
- Sec. 1004. Certification of checks
- Sec. 1005. Bank entries, reports, and transactions
- Sec. 1006. Federal credit institution entries, reports, and transactions
- Sec. 1007. Federal Deposit Insurance Corporation transactions
- Sec. 1008, 1009. Repealed
- Sec. 1010. Department of Housing and Urban Development and Federal Housing Administration transactions
- Sec. 1011. Federal land bank mortgage transactions
- Sec. 1012. Department of Housing and Urban Development transactions
- Sec. 1013. Farm loan bonds and credit bank debentures
- Sec. 1014. Loan and credit applications generally; renewals and discounts; crop insurance
- Sec. 1015. Naturalization, citizenship or alien registry
- Sec. 1016. Acknowledgment of appearance or oath
- Sec. 1017. Government seals wrongfully used and instruments wrongfully sealed
- Sec. 1018. Official certificates or writings
- Sec. 1019. Certificates by consular officers
- Sec. 1020. Highway projects
- Sec. 1021. Title records
- Sec. 1022. Delivery of certificate, voucher, receipt for military or naval property
- Sec. 1023. Insufficient delivery of money or property for military or naval service
- Sec. 1024. Purchase or receipt of military, naval, or veterans' facilities property
- Sec. 1025. False pretenses on high seas and other waters
- Sec. 1026. Compromise, adjustment, or cancellation of farm indebtedness
- Sec. 1027. False statements and concealment of facts in relation to documents required by the Employee Retirement Income Security Act of 1974
- Sec. 1028. Fraud and related activity in connection with identification documents and information
- Sec. 1029. Fraud and related activity in connection with access devices
- Sec. 1030. Fraud and related activity in connection with computers
- Sec. 1031. Major fraud against the United States
- Sec. 1032. Concealment of assets from conservator, receiver, or liquidating agent of financial institution
- Sec. 1033. Crimes by or affecting persons engaged in the business of insurance whose activities affect interstate commerce

- Sec. 1034. Civil penalties and injunctions for violations of section 1033
- Sec. 1035. False statements relating to health-care matters
- Sec. 1036. Entry by false pretenses to any real property, vessel, or aircraft of the United States or secure area of any airport

RELEVANT CONSUMER PROTECTION LAWS FOR FRAUD IN THE UNITED STATES

Consumer protection laws are designed to protect all consumers, the gullible as well as the shrewd. The fact that a false statement may be obviously false to those who are trained and experienced does not change its character or take away its power to deceive others less experienced. Our consumer protection laws were enacted for the protection of the people, many who are trusting and naive about the wolves of the business world that come dressed in lambs' clothing.[5]

A FEW EXAMPLES OF U.S. FEDERAL ENFORCEMENT OF FRAUD-RELATED LAWS, APPROACH AND ACTIONS

The U.S. Department of Justice conducts both criminal and civil litigation in combating telemarketing fraud. United States Attorneys' Offices throughout the country, as well as the Fraud Section of the Criminal Division of the DOJ, have successfully prosecuted many criminal cases against fraudulent telemarketers. The Office of Consumer Litigation of the Civil Division of the department, which conducts both civil and criminal litigation in consumer-related cases, has also prosecuted telemarketing fraud cases.

Under federal law, state attorneys general have been given broad power by the U.S. Congress to combat telemarketing fraud. For example, a state attorney general can file lawsuits in federal court and shut down fraudulent telemarketers through national injunctions so as to prevent companies from moving on under a different name after being banned in one state.

Federal mail and wire fraud charges, which had a five-year maximum penalty, now carry an additional five years for telemarketing fraud or an additional ten years if ten or more senior citizens are targeted.

In a typical telemarketing fraud indictment that a federal grand jury would return, the Department of Justice includes charges under criminal statutes such as wire fraud (18 U.S.C., sec. 1343), mail fraud (18 U.S.C.,

[5] http://www.crimes-of-persuasion.com/Laws/US/criminal_laws.htm.

sect. 1341), and conspiracy to engage in wire and mail fraud (18 U.S.C., sect. 371). Each of these statutes carries a maximum term of imprisonment of five years.

The court holds that to sustain a conviction for wire fraud, a fraudulent telemarketer need not personally call victims to incur criminal liability for a "co-schemer's" use of telephones to cheat them.

Mail and wire frauds have a unique characteristic in that each is complete when the mail or wire has been used. Just the existence of the scheme plus the use of the mail or an interstate wire to further the scheme will suffice. Each completed call is therefore a separate, completed fraud offense, even if the money was not sent in.

MAIL FRAUD STATUTES (CONDENSED AND PARAPHRASED)

Title 18, United States Code, Section 1301. Importing or transporting lottery tickets

Whoever brings into the United States a ticket, gift enterprise, or similar scheme for sale or interstate transfer, or offers prizes dependent on chance, or any advertisement of such a scheme, shall be fined under this title or imprisoned not more than two years, or both.

Section 1302. Mailing lottery tickets or related matter

Whoever knowingly deposits in the mail, or sends or delivers by mail:

Any letter or such concerning any lottery, gift enterprise, or similar scheme offering prizes dependent in whole or in part upon lot or chance or any payment for the purchase of any ticket or part thereof shall be fined or imprisoned not more than two years, or both; and for any subsequent offense shall be imprisoned not more than five years.

Section 1303. Postmaster or employee as lottery agent

Any employee of the Postal Service who knowingly delivers any letter advertising any lottery, gift enterprise, or similar scheme shall be fined under this title or imprisoned not more than one year, or both.

Section 2326. Senior Citizens Against Marketing Scams Act

In addition, under a statute enacted in 1994 as part of the Senior Citizens Against Marketing Scams Act (18 U.S.C., sect. 2326), federal courts can

impose an additional term of up to five years' imprisonment where the mail, wire, or bank fraud offense was committed in connection with the conduct of telemarketing.

They can impose an additional term of imprisonment of up to ten years' imprisonment if the offense targeted persons 55 and older or victimized ten or more persons 55 and older. A similar enhancement can be added to the bank fraud sentence.

Convicted individuals must also be ordered to pay full restitution to their victims.

Title 39, United States Code, Section 3005. False Representations; Lotteries

(a) Upon evidence that any person is engaged in conducting a scheme or device for obtaining money through the mail by means of false representations, or is engaged in conducting a lottery, gift enterprise, or scheme for the distribution of money, the Postal Service may issue an order that:

(1) directs the postmaster of the post office at which mail arrives to return such mail to the sender appropriately marked as in violation of this section;
(2) forbids the payment by a postmaster to the person of any money order or postal note and provides for the return to the remitter; and
(3) requires the person or representative to cease and desist from engaging in any such scheme, device, lottery, or gift enterprise.

Section 1341. Frauds and Swindles

Whoever, having devised or intending to devise any scheme to defraud, or to sell any counterfeit or spurious security, sends by the Postal Service, or by any private or commercial interstate carrier, or receives any such thing, shall be fined or imprisoned not more than five years, or both.

If the violation affects a financial institution, such person shall be fined not more than $1 million or imprisoned not more than 30 years, or both.

Section 1342. Fictitious Name or Address

Whoever, for the purpose of promoting, or carrying on any such scheme or any other unlawful business, uses a fake name or address shall be fined or imprisoned not more than five years, or both.

Section 1345. Injunctions Against Fraud

The attorney general may commence a civil action in any federal court to rejoin such violation.

MONEY LAUNDERING

Because the owners and operators of telemarketing schemes often use the proceeds to further the scheme — for example, to pay the costs of their telemarketing business activities, such as payment of salaries and rent and purchases of "leads" and "gimmie gifts" — the Department has increasingly included charges under the federal money-laundering statutes (18 U.S.C., sects. 1956 and 1957).

Each of these latter statutes carries a maximum term of imprisonment of 20 years and 10 years, respectively, and provides the department with a basis to obtain criminal forfeiture of the telemarketers' property. In some cases they will even, as appropriate, use RICO (Racketeer Influenced and Corrupt Organization) charges.

FINANCIAL INSTITUTION FRAUD (BANK FRAUD)

In cases where fraudulent telemarketers have misled banks when they applied for merchant accounts to process victims' credit card charges, the department has also charged the telemarketers with financial institution fraud (18 U.S.C., sect. 1344). That statute carries a maximum term of imprisonment of 30 years.

CIVIL LITIGATION

Telemarketers sometimes engage in unfair practices that may not rise to the level of criminal violations but nevertheless harm consumers. In such cases, the Office of Consumer Litigation frequently initiates civil litigation at the request of the Federal Trade Commission (FTC).

These cases seek enforcement of FTC rules that govern the conduct of telemarketers, such as the Telemarketing Sales Rule, or rules that directly apply to telemarketers or the Franchise Rule, and rules that regulate the practices of anyone, including telemarketers, selling franchise opportunities.

These enforcement actions serve several purposes. First, they obtain court orders that prohibit misrepresentations and require the telemarketer

to comply with the pertinent FTC rule. This frequently results in firms going out of business. Firms that remain in business tend to provide more complete and accurate information to potential customers. Second, these actions may obtain civil penalties or consumer redress from violators, forms of monetary deterrence that can also benefit victims.

Third, the individuals who are subject to orders in these cases risk charges of civil or criminal contempt of court if they violate the court orders. The Office of Consumer Litigation and the FTC, through "Operation Scofflaw," have sought and obtained terms of imprisonment against individuals who violate such orders.

U.S. TREASURY COLLECTION

In many cases involving fraud, the FTC receives judgments against the defendants so that they will attempt to collect on these with the goal of returning money to the victims. Collection is often difficult, however, because the defendants do not have identifiable assets subject to seizure. So, the FTC recently began working with the U.S. Treasury for assistance in collecting these judgments.

The Treasury's Financial Management Services Division is able to use its collection expertise to aggressively collect amounts owed by fraudulent telemarketers.

In cases where Treasury is unable to collect after diligent effort, it will report to the Internal Revenue Service that the uncollected debt should be treated as income to the defendant, subject to taxation.

SECURITIES VIOLATIONS

By successfully advocating in the General Assembly for a change making securities violations felonies, attorney generals can initiate a policy of criminally prosecuting securities violators rather than handling them administratively.

ROLE OF PHONE COMPANIES

A federal law requires phone companies to discontinue or refuse services to businesses that use their lines to transmit gambling information. The law has been used primarily to stop bookmaking operations but has shut down lottery operations as well.

EUROPEAN FRAUD-RELATED LAWS

The European Union (EU) and individual European nations are also concerned with fighting frauds. They define fraud as: "Deliberate deception used for unfair or illegal advantage."[6]

In Europe, Interpol, Europol, and the EU share information in order to help prevent, investigate, and prosecute frauds. The EU has established the OLAF (or Office Européen de Lutte Anti-Fraude) or "European Anti-Fraud Office" with fighting fraud that includes "protecting the interests of the European Union, to fighting fraud, corruption and any other irregular activity, including misconduct within the European Institutions, in an accountable, transparent and cost-effective manner." In so doing, OLAF reports to the European Parliament.

OLAF fulfills its mission by conducting, in full independence, internal and external investigations. It also organizes close and regular cooperation between the competent authorities of the member states in order to coordinate their activities. OLAF supplies member states with the necessary support and technical know-how to help them in their anti-fraud activities. It contributes to the design of the anti-fraud strategy of the European Union and takes the necessary initiatives to strengthen the relevant legislation.

> The objective of the OLAF is to protect the interests of the European Union, to fight fraud, corruption, and any other irregular activity, including misconduct within the European's institutions. In pursuing this mission in an accountable, transparent and cost-effective manner . . .[7]

EU FIGHT AGAINST FRAUDS

The EU's OLAF is set up:

- To provide an independent investigative service.
- To "Carry out all the powers of investigation conferred on the Commission by Community legislation and the agreements in force with third countries, with a view to reinforcing the fight against fraud, corruption and any other illegal activity affecting the financial interests of the European Community."

---

[6] See http://europa.eu.int/comm/justice_home/glossary/glossary_f_en.htm and the subsequent footnotes relative to EU's anti-fraud program, from which this section is liberally quoted.

[7] Ibid.

- "To consolidate this independence, the Office is subject to regular control of its investigative function by a Supervisory Committee, made up of five outside persons independent of the Community Institutions, who are highly qualified in the areas of competence of the Office. At the request of the Director-General or on its own initiative, the Supervisory Committee will deliver opinions to the Director-General concerning the activities of the Office, without however interfering with the conduct of investigations in progress."
- "In close cooperation between the Commission services and the member states, the Committee also issues guidelines for national authorities and reference documents on Fraud and other irregularities. It elaborates the Annual Report of the Commission, as provided under Article 280 of the EC Treaty, an overview of Community and national action and initiatives, including an image of case reporting and of the trends of fraud and other irregularities throughout the EU."
- "OLAF, in cooperation with its national partners (investigation services, police, legal and administrative authorities, etc.) does its best to counter the criminals and the fraudsters, who did not wait for the opening of the borders to organize their illicit activities at international level. OLAF is to some extent the engine of the 'Europe of legality' against the 'international nature of criminality; harmful to Community interests."
- "To this end, OLAF can carry out administrative investigations inside the institutions (see EC Decisions 1999/394 and 1999/396), the bodies and organs of the Community, in the event of fraud harmful to the budget of the EU. It is also responsible for detecting the serious facts, linked with the performance of professional activities."
- "OLAF comprises some 280 agents, including the nonstatutory personnel; the total number of staff should rise to 330 persons towards the end of 2002. The investigators of OLAF, like all the other officials and Community servants, work in the exclusive interest of the Communities. They have to discharge their functions and do their work while keeping only in mind the interests of the Communities, without taking instructions from any government, authority, organisation or person independent of the institution. To achieve these specific tasks, the majority of the personnel of OLAF have however a solid professional experience gained in the national investigation, police and judicial services, in the area of investigations concerning complex fraud cases, in the analysis and evaluation of information, or in activities of support or development of policies in the area of the fight against fraud."
- "OLAF is therefore neither a 'secret service,' nor a police force. It is rather the legal instrument for administrative investigation with which the European Union has been equipped by the

Commission, to guarantee better protection of Community interests and compliance with the law against attacks from organized crime and fraudsters."[8]

ASIA AND FIGHTING FRAUD

Asian nation-states are also concerned with the crimes perpetrated by both internal and international miscreants. Although their emphasis seems to be more on combating illegal drugs, trafficking in women and children, money laundering, and terrorism, they are also concerned with fighting fraud.

One of the primary bodies for fighting such criminal activities is the Association of Southeast Asian Nations (ASEAN). At the inaugural meeting of the association hosted by the Philippine government in December 1997, it issued a declaration establishing a framework for cooperation among the ASEAN members in combatting "transnational crime."

The Declaration provided the following initiatives for regional cooperation on tackling transnational crime:[9]

1. Hold discussions with a view to signing mutual legal assistance agreements, bilateral treaties, memorandum of understanding or other arrangements among member countries.
2. Consider the establishment of an ASEAN Centre on Combating Transnational Crime (ACTC), which will coordinate regional efforts against transnational crime through intelligence sharing, harmonization of policies and coordination of operations.
3. Convene a high-level ad-hoc Experts Group within one year to accomplish the following with the assistance of the ASEAN Secretariat:
   a. ASEAN Plan of Action on Transnational Crime
   b. Institutional Framework for ASEAN Cooperation on Transnational Crime
   c. Feasibility study on the establishment of ACTC
4. Encourage member countries to consider assigning Police Attaches and/or Police Liaison Officers in each other's capital in order to facilitate cooperation for tackling transnational crime.
5. Encourage networking of the relevant national agencies or organizations in member countries dealing with transnational crime to further enhance information exchange and dissemination.
6. Expand the scope of member countries' efforts against transnational crime such as terrorism, illicit drug trafficking, arms smuggling,

---

[8] http://europa.eu.int/comm/dgs/olaf/mission/mission/index_en.html.

[9] http://www. aseansec.org/5640.htm

money laundering, and traffic in person and piracy, and to request the ASEAN secretary general to include these areas in the work program of the ASEAN Secretariat.

7. Explore ways by which the member countries can work closer with relevant agencies and organizations in Dialogue Partner countries, other countries, and international organizations, including the United Nations and its specialized agencies, Colombo Plan Bureau, Interpol, and such other agencies, to combat transnational crime.
8. Cooperate and coordinate more closely with other ASEAN bodies such as the ASEAN law ministers and attorneys general, the ASEAN chiefs of National Police, the ASEAN finance ministers, the directors-general of Immigration and the directors-general of Customs in the investigations, prosecution, and rehabilitation of perpetrators of such crimes.

CASE STUDY

As in all wars, the war in Iraq offers many challenges, and one of them is the potential for fraud. The following case[10] is but one example showing that when it comes to matters of fraud, the waters are often very murky:

> The Virginia courtroom, just outside of Washington, D.C., was set to try what should have been a simple matter of whether or not Custer Battles, an upstart security company, based in McLean, Virginia, had defrauded its customers by as much as $50 million. By the end of the hearing last week, a perplexed judge was asked to decide whether the United States government controlled Iraq's oil revenues that were used to pay the company.
>
> "The funds that were used were Iraqi funds, not U.S. funds," said veteran Washington lawyer John Boese. . . . The fact that CPA was in temporary possession of the money and distributed it does not form a basis for a false claim.
>
> . . . , the attorney for the plaintiffs claimed . . . that the U.S. largely controlled the Coalition Provisional Authority (CPA) that was running Iraq at the time and was clearly understood to be "a government entity" by the U.S. Congress when approving the $87 billion funding package in November 2003 for reconstruction and military spending in

[10] See article, "Iraq Contractor Claims Immunity from Fraud Laws; Seized Oil Assets Paid for Offshore Overbilling" by David Phinney, Special to CorpWatch, December 23, 2004.

> Iraq. . . . Custer Battles[11] has been accused of illegally inflating costs on plum contracts in 2003 to protect the Baghdad International Airport as well as for a massive program that replaced Iraq's currency.
>
> . . . the lawsuit under the False Claims Act, reinvigorated by Congress in 1986, which is considered a key weapon in fighting contract fraud. It allows federal courts to award financial incentives to people in the private sector to step forward and assist the government in recovering the money, if they have evidence of wrongdoing."

As the chief security officer (CSO) for such a company:

- How would you react to the above?
- Would you try to get involved?
- If so, in what manner would you try to get involved? For example, would you offer investigative assistance to the company's legal staff?
- How would you feel working for such a company?

As the CSO, what things must you consider? An example of some things to think about are as follows:

It seems that in today's corporate world, it is not unusual to be working for a company that has been accused of perpetrating a fraud. Normally, your anti-fraud program should address such types of frauds; however, in the "real world" it generally will not.

One reason that you will have a difficult time selling such a program or a particular part of such a program is that corporate frauds are often committed at the highest levels of a corporation, and any attempt to conduct an inquiry to prove or disprove rumors of fraud or specific allegations will cause a quick end to your professional career in that company. Remember that these are the same executives who must approve your corporate anti-fraud program.

If you have a basis for believing that such frauds are being perpetrated within your corporation, you can become a "whistleblower." If so, no matter if you are right or wrong, your career at that corporation will be in jeopardy as corporate executives will find some way to get rid of you — "reorganization" is sometimes used to "squeeze" someone out of the corporation.

Although it is not right to take this punitive action, it unfortunately happens more often than one may realize. Furthermore, any chances of your joining another corporation will be minimal because of the stigma attached to your name. Consequently, your chances of obtaining a similar job may be in jeopardy.

---

[11] This case is an example of the complications of fraud matters, and in no way are we implying the guilt or innocence of the contractor.

It is a sad commentary on today's corporate world that ethics and honesty are good as long as you don't "rock the boat." The following is an example of what may happen when you become a whistleblower:

"BLOWING THE WHISTLE" ON DEFRAUDERS CAN BE DANGEROUS

> **Los Alamos whistleblower beaten outside bar:** A Los Alamos lab whistle-blower scheduled to testify before Congress was badly beaten in an attack outside a Santa Fe bar. . . . in a hospital recovering from a fractured jaw and other injuries, . . . wife and his lawyer believe the attack was designed to keep him quiet . . . assailants told her husband during the attack early Sunday that "if you know what's good for you, you'll keep your mouth shut.". . . . has a pending lawsuit against the University of California alleging whistleblower retaliation.
>
> He had been scheduled to testify before the House Energy and Commerce Committee later this month about alleged financial irregularities at the nuclear weapons lab. . . . the 52-year-old lab employee got a telephone call late Saturday night — after he was already in bed — wanting to meet with him at a Santa Fe bar about 45 minutes from their home. . . .
>
> husband told her the man never showed up, but as he was leaving the topless bar's parking lot, a group of men pulled him from his car and beat him. . . . sued the university in March, alleging that after they uncovered management failures, university and lab managers tried to make their jobs miserable so they would quit. . . . had been voicing complaints about lab management for years. He testified in a 1997 deposition that the chief of the lab's audit division "didn't want to see certain things put in reports," including "unallowable costs" and "embarrassment to the university."[12]

This is an example of how dangerous such activities can be. Whistleblowers are vital, but they may pay a heavy price.

SUMMARY

Nations-states around the world are concerned with fraudulent activities within and directed toward their corporations. Many nation-states have banded together to form associations, such as EU and ASEAN, to combat international crimes, including frauds. Generally, the most developed nation-states have more comprehensive laws, one reason being the fact that they are the most targeted.

---

[12] http://www.cnn.com/2005/US/06/07/whistleblower.beaten.ap/index.html

It is important to be familiar with the associations, treaties, and laws relative to fraudulent matters in every nation-state where your corporation has offices. Furthermore, your corporate anti-fraud program should consider such laws and design a corporate anti-fraud program that will help prove or disprove allegations against the applicable laws of the nation-states where the corporate facilities are located.

This page intentionally left blank

4

Corporations Don't Commit Frauds; People Do

INTRODUCTION

According to John Galbraith, "the word capitalism has been replaced by the term 'the Market System'. . . . Those who most enjoy their work . . . are all but universally the best paid. . . . Low wage scales are for those in repetitive, tedious, painful toil. Those who least need compensation for their effort, could best survive without it, are paid the most. The wages, or more precisely the salaries, bonuses, and stock options, are the most munificent at the top, where work is a pleasure."[1]

If you agree with Galbraith, and let's assume for the sake of discussion that you do, then consider this: It should only be "those on the bottom" who should consider perpetrating frauds since they who are least likely to enjoy their work and are paid the least, while at the same time they are trying to enhance their lifestyle.

Some may see perpetrating a fraud or other type of crime as the only way out of their current predicament. They are also the ones who may generally have the least amount of education and the least amount of experience in a job or profession that can help propel them to the "good life". But other reasons may also be involved; these will be discussed throughout this chapter.

ARE DEFRAUDERS A PRODUCT OF THEIR ENVIRONMENT, OR IS IT IN THEIR GENES?

If you agree with Galbraith's comments, then why is it that history, especially the recent history of U.S corporations and their executive

[1] From John K. Galbraith's book, *The Economics of Innocent Fraud: Truth for Our Time*. Houghton Mifflin, Boston. 2004.

management, has shown that apparently many frauds are committed at the higher levels of corporate management? Is it:

- Just plain ole human nature at work?
- All about power?
- About seeing how much money you can amass?
- Based on how a person was raised, or is it more in the genes derived from the defrauder's ancestors?
- All of the above?
- None of the above?

Criminologists from all over the world have made a lifetime study of the reasons humans commit frauds and other crimes. The debate goes on and will probably continue much as the chicken and the egg "controversy" is forever. There are those who say it is based on your "inherited DNA," but then they can't explain it when the child of alcoholic, drug using, or criminal parents turns into a model citizen. There are those who believe that an individual's criminal behavior is based on his or her environment; again, however, they are unable to explain why some people raised in crime-ridden housing projects become model citizens.

Is it, as some believe, that we are reincarnated in each life to learn and experience new things and by doing so, over many thousands of lifetimes, eventually enter Nirvana or become "one with the Universe"? If that is the case, then we have no choice as to our fate in each lifetime.

Obviously, at least in this lifetime, we won't know. However, some theories have been floated that may help us understand the criminal mind and thereby put us in a better position to thwart their fraud attacks.

SOME CRIMINOLOGY THEORIES

Throughout history, many theories have been proposed as to why people commit crimes. It is important for the security professional to have a basic understanding of these theories as a baseline for protecting corporate assets from fraud-threat agents and other criminals. This of course then holds true for protecting the assets from defrauders through a comprehensive corporate anti-fraud program. "Know your enemy" is a good adage to remember and one that is quite often not thought about or not contemplated enough by the corporations' anti-fraud professionals.

Do people commit crimes because (1) it is their fate, (2) it is God's will, (3) they are a product of their environment, or (4) they inherited bad genes? Or (5) is society to blame?

Is there a method for identifying potential defrauders and other criminals by their physical features (e.g., thin fingers and bushy eyebrows)? Don't laugh. Since at least medieval times, such ideas have been advanced. And you know what? We still don't really know why some people commit frauds and other crimes while those in similar circumstances do not. However, there have been, and still are today, theories on why people commit frauds and other crimes.

Some of the theories of crime, punishments, and why people commit crimes can be summarized as follows:

- Spiritual:[2] People commit crime due to some "other worldly powers." These people believe that they were inflicted with natural disasters as punishments for their past deeds.
- Naturalism:
  - Criminal actions are free-will choices.
  - Criminal actions are caused by factors beyond the person's control.
  - Criminal actions are so designated by criminal law where certain actions and/or people are designated as criminal. In other words, the law defines the criminal act and therefore defines as a criminal anyone who violates that act.
- Realism: Nation-states have the power derived from God to govern their people and to punish them for wrongdoing.
- Classical/Neo-Classical/Idealism: Cesare Beccaria wrote in 1764 that reforms were needed to make the criminal justice system more rational and logical in lieu of what he perceived to be the personal justice meted out by judges and the harshness of the punishments.
- Utilitarianism: The actions of human beings are motivated by self-interest; morality should be judged based on the usefulness to society. Criminals should be reformed through hard labor.
- Positivism: Criminals have specific characteristics that are different from those of others; a thief may be identified by bushy eyebrows, large lips, sharp vision, mobile eyes, long and slender fingers.[3]
- Existentialism: Human beings are free to make their own choices and are not bound by heredity, social conditions, morality, or the like.
- Analytical: There are two forms of society according to Emile Durkheim:
  - A society with a high degree of homogeneity based on a more primitive, mechanical form of society and a low division of labor; laws keep humans from deviating from society's norms

---

[2] These theories and others can be found in *Theoretical Criminology*, Third Edition, by George B. Vold and Thomas J. Bernard, published by Oxford University Press, 1986, New York; and *History of Criminology: A Philosophical Perspective* by David A. Jones, published by Greenwood Press, 1986, New York.

[3] Ibid, Page 82, Jones

- A society with a greater homogeneity of values and a higher division of labor. Durkheim also argued that
  - Some percentage of crime in a society is natural; without which society would be unhealthy
  - "No living being can be happy or even exist unless his needs are sufficiently proportioned to his means."[4]

These and related theories consider crime causations based on poverty, economic inequality, social controls, learned behavior, ecology of crimes, and the like.

As a security professional, remember that you are defending the corporate assets against defrauders. It would behoove you to learn more about the theories of criminology and consider such theories when developing your corporate anti-fraud program. After all, you are defending the corporate assets, and the defenses should incorporate controls that mitigate the attacks of fraud-threat agents. Therefore, knowing something about their makeup helps provide fraud-threat agent profiles.

FRAUD-THREAT AGENTS

Let's look at the fraud-threat agents, their profiles, motivations, inhibitors, capabilities, amplifiers, and catalysts. First, however, let's take a moment to discuss human errors or accidents vis-à-vis fraud.

HUMAN ERRORS — ACCIDENTS

Being human, we naturally will make mistakes. So, does human error fall under the category of natural threats and are we humans to be considered "natural threat agents," or do we fall under the category of "man-made" threats?

There is no law or rule that says that you must treat it as one, the other, both or neither. However, human error is a threat to corporate assets. For example, by downloading a program, joke, or photo from some Web site to your corporate computer in your office, you may also download and initiate some form of malicious code such as a worm or a virus. Such malicious codes attack valuable corporate assets and may cost the corporation in terms of cleanup costs, public image, lost revenue, and the like. You didn't mean to do it. It was an accident.

Yes, corporate assets must be protected from such incidents. However, when it comes to fraud and fraud-threat agents' attacks against corporate assets, one thing should be perfectly clear: *It is not possible to accidentally, unintentionally, or mistakenly perpetrate a fraud!*

---

[4] Durkheim, *Suicide*. Translated into English in 1952. Extracts at http://www.mdx.ac.uk/www/study/xdur.htm.

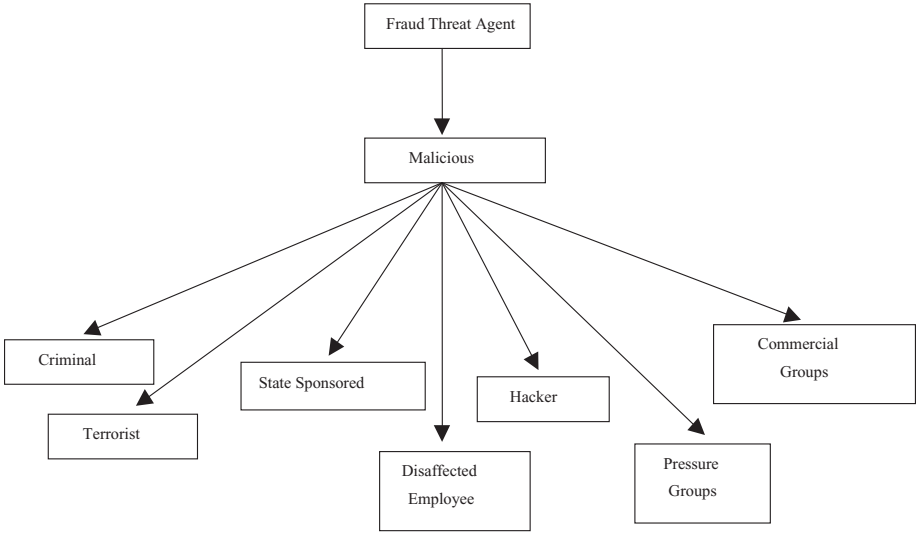


Figure 4-1. Various types of malicious fraud-threat agents.

So, when someone is identified as having attempted or successfully perpetrated a fraud, and says it was a mistake or an accident, give the person no credence. The only mistake he or she may have made was perpetrating the act in the first place and subsequently getting caught.

MAN-MADE OR MALICIOUS FRAUD THREATS

Man-made or malicious fraud threats take many forms, with new types of fraud threats being identified all too often.[5] However, these fraud threats can all be categorized into general groupings.[6] (See Figure 4-1.)

In order for a malicious fraud threat to exist (is there any other kind than malicious?), there must be an agent who will implement the threat, and that agent must have the motivation, capability, and opportunity to do so.

POTENTIAL FRAUD-THREAT AGENTS

A malicious threat agent can be generated from any number of groups. This is not meant to be an exhaustive list of potential sources or groupings of

[5] The information in this section is based on the work of Dr. Andy Jones, my previous co-author, colleague, and friend and modified here to specifically address the fraud threat agents.

[6] Ibid.

malicious threat agents, for these will change over time as technology, society, education, national and international politics, culture, and a host of other factors change and have an effect.

Malicious Threat Agent — State Sponsored

State-sponsored malicious fraud threats may take any form, such as attacks against financial systems in order to modify public perception or cause instability in the country and cause or prevent the country from taking other actions. Characteristically, this group will be risk averse and will be conservative in its actions, making great efforts to evade identification.

Most information on nation-states is readily available from open sources. The limiting factor in this information is that it may be dated. To be effective, a fraudulent attack sponsored by a nation-state must have:

- The technology to mount the attack against financial institutions
- The telecommunications, Internet, and power supplies to allow the attack to take place and to sustain it
- Sufficient personnel resources with an adequate level of education and skill to mount and maintain the attack

Each country will have specific cultural drivers. These drivers will impact why and how fraudulent attacks are conducted. The impact of each type of attack will vary, and the likelihood of each must be considered separately.

Malicious Threat Agent — Terrorists

Terrorist activity may be linked to criminal activity, and as malicious fraud-threat agents, terrorists may operate as individuals or in groups. Terrorism requires funding to be effective, and given that terrorists operate outside of normal national and international laws, they will commonly resort to criminal activity to generate funds that will support their activities in addition to any direct terrorist related actions.

Qualitative information on terrorist organizations is not, for the main part, readily available from open sources. Although generic information from external sources will be available, accurate and in-depth information is not normally available in a form that can be verified except where it is released or disseminated from national resources that will probably be hostile to the "terrorist" organization. Therefore, security professionals will have a difficult time preparing for fraudulent attacks by terrorists. However, they undoubtedly will employ the same basic attack techniques as any other defrauders will use. After all, their goal is basically financial: to

support their terrorist activities that will cause economic chaos in nation-states they consider their enemies.

For a terrorist-sponsored attack to be effective, as noted earlier, it may also be necessary to have the technology available to mount the attack, as well as the telecommunications, Internet connectivity, and power supply that will allow the attack to take place. If one of the required outcomes of the attack requires that it be sustained, then a sufficient depth of personnel resources with an adequate level of education and skill must also be available. Each terrorist group will have specific drivers, which may be religious, cultural, ethnic, political, or any number of others.

A good generic resource for information on terrorism and terrorist groups can be found at *The Juris*,[7] a publication that provides a large number of links to give specific information on particular groups and to resources that provide general information on terrorism.

Terrorist groups are affected by a wide range of factors that will influence their motivation and ability and the likelihood that they will be able to successfully carry out a fraud attack. The sources of this information will be varied, but the most likely sources will be those that concentrate on the terrorist organizations or the media, which are likely to have up-to-date information.

Malicious Threat Agent — Pressure Group

Pressure groups will tend to have a specific focus or cause that they support and maintain. Recent history has shown that such groups, whether they are secular or religious, have learned that they can achieve results by exerting influence on peripheral targets rather than on a direct attack on the primary target. In order to hurt their targeted corporation, they may also resort to attempts to hurt the corporation financially.

Qualitative information on pressure groups is not, for the main part, readily available in the public domain from open sources. Although generic information from external sources will be available, accurate and in-depth information is not normally available in a verifiable form inasmuch as these are not accountable organizations.

To launch an effective attack, the pressure group must have the requisite technology. It is assumed that the group would have the telecommunications, Internet connectivity, and power supply sufficient for the attack to take place. If the required outcome of the attack is that it is sustained, then the pressure group must also have sufficient personnel resources with an adequate level of skill. Each pressure group will have specific drivers, which may be religious, cultural, ethnic, political, or any number of others.

---

[7] See www.law.duq.edu/pdf/juris

Because of the range of organizations included in this group and because they have varying degrees of legitimacy and history, identifying specific sources of information for the various aspects of the pressure group cannot easily be done. For detailed information on a specific pressure group, it is necessary to examine the information sources specifically related to that group. The details available on a pressure group will be variable over a period of time as it becomes more or less active.

Pressure groups are affected by a wide range of factors that will influence their motivation and ability and the likelihood of carrying out an attack. The objective of a threat agent sponsored by a pressure group may be to cause a corporation to declare bankruptcy and otherwise hurt its public image and thus its stock prices. The impact of each type of fraud attack will vary, and the likelihood of each must be considered separately in light of the organization's aims and target.

Malicious Threat Agent — Commercial Group

A threat agent that acts on behalf of a commercial group will tend to have one of a small number of objectives, including damaging the interests of competitors to influence small nation-states. This group will generally be risk averse and conservative in its actions and will go to great lengths to evade identification. For a fraud attack sponsored by a commercial group to be effective, it is necessary that the group have the requisite resources.

If the required outcome of the attack requires that it be sustained, the group must also have sufficient personnel resources with an adequate level of skill. Each commercial group will have specific drivers, but these will be predominantly financial or competitive gain.

Qualitative information on the capability of a commercial organization to carry out an attack is not generally available in the public domain from open sources. Although very specific and detailed information will be available on many aspects relating to the commercial concern, specific information with regard to its capability to pose a fraud threat will only be generated from analysis of the organization or from information on past activity as it becomes available. To avoid identification, the commercial group may outsource such fraud attacks to "mercenaries."

A successful attack that is sponsored by a commercial organization requires that the group have the needed technology, notably, the telecommunications, Internet connectivity, and power supply.

If the required outcome of the attack is that it be sustained, then the organization must also have sufficient personnel resources with an adequate level of skill. The driver for a commercial organization to mount an attack will be the desire to gain a commercial advantage in the marketplace, for example, by reducing the competitor's ability to operate efficiently in the marketplace.

A wide range of factors will affect the commercial group's motivation and ability and the likelihood of carrying out an attack. The impact of each type of fraud attack will vary, and the likelihood of each must be considered separately in light of the organization's perceived aims and target.

Malicious Threat Agent — Criminal

Criminal activity poses a fraud threat to corporations and is the type of fraud threat most often discussed. These criminals attack in order to

- Gain access to a computer network in order to defraud someone of resources (money or property).
- Prevent the detection or investigation of other criminal activity.
- Gain information that will enable them to commit other frauds.
- Gain access to personal information that will enable them to commit other fraud crimes, such as identity theft.

Because the descriptor "criminal" covers an enormous range of activities extending from financial gain to murder, drug smuggling, trafficking, and sex offenses, it is not possible to present any generic characteristics. However, our main concern is their classification as a fraud-threat agent.

For the purposes of the present work, the threat agent, whether a defrauder or a group of defrauders, will generally have one of a small number of objectives. This group, like the others already discussed, will generally be risk averse and conservative in its actions and will make every effort to evade identification.

This defrauder group, like the others discussed, requires the necessary resources to mount an effective attack. Having resources is not normally an issue for these criminals because they tend to be "cash rich" and do not have to account for their funds. If the attack outcome needs to be sustained, they must also have sufficient personnel resources with an adequate level of skill. Each defrauder or defrauder group will have specific drivers, mostly financial or competitive gain.

Any form of usable information on a criminal organization's ability to carry out an attack is not generally in the public domain from open sources. Law enforcement and national intelligence agencies invest a vast effort to gather this type of information and usually have only limited success, though some inference can be made over a period of time as the effects of the group's actions become apparent.

This defrauder or defrauder group may also require the technology and level of skill needed to mount an effective attack. It is assumed that the telecommunications, Internet connectivity, and power supply are available to allow the attack to take place.

If the required outcome of the attack is that it be sustained, then the organization must also have sufficient depth of personnel resources with an adequate level of skill. The driver for a defrauder or defrauder group will be financial gain or influence. This may not be apparent from the form of an attack.

It is difficult to deal separately with each factor that may contribute to a defrauder or defrauder group's capability to pose a threat; however, considerable information is available from which the individual elements that are required can be extracted. Defrauders or defrauder groups are affected by a wide range of factors that will influence their motivation and ability and the likelihood of carrying out an attack.

A fraud-threat agent may be sponsored by a criminal group such as an organized crime group. The impact of each type of fraud attack will vary, and the likelihood of each must be considered separately in light of the criminal group's perceived aims and target.

Malicious Threat Agent — Hacker

The hackers' normal objectives are to demonstrate to their peers that they have a level of skill that will gain them status or cause visible damage to a system simply "because they can." Other reasons may include their desire to gain access to a system in order to utilize its resources, either for the processing capability or to cover other activities. Inasmuch as the basis of this group is technical capability rather than a specific motive or pressure, the type of attack that may be mounted will not be based on the impact to the system owner but rather on the real or perceived benefit to the perpetrator.

For the hacker's fraud attack to be effective, the hacker needs the requisite resources. This is not normally an issue for a hacker group because they have support from their peers. If the required outcome of the attack requires that it be sustained, the hackers must also have sufficient personnel resources with an adequate level of skill. Each hacker group will have specific drivers, but these will be predominantly for self aggrandizement or revenge. All the same, one cannot discount the fact that some hackers are used to commit fraudulent acts.

Any form of usable information on the hacker group's ability to carry out a fraud attack will, if it is available, be in the public domain from open sources. Law enforcement and national intelligence agencies make only limited attempts to gather information on these groups, and owing to the groups' transient nature, they have had only limited success. Some inference can be gathered over a period of time as the effects of the hacker group's actions become apparent.

To be effective in their fraud attack, the hacker group needs the appropriate level of skill, and it is assumed that the group will have the telecom-

munications, Internet connectivity, suitable technology, and power supply sufficient to allow the attack to take place.

If the required outcome of the attack is that it be sustained, then the group must also have sufficient depth of adequately skilled personnel. The drivers for a hacker group to mount an information attack will vary, with the main drivers ranging from curiosity to financial gain to revenge.

It is difficult to deal separately with each factor that may contribute to the capability of a hacker or hacker group to pose a threat; however, considerable information can be extracted from the individual elements. Hacker groups are affected by a wide range of factors that will influence their motivation and ability and the likelihood of carrying out a fraud attack.

The impact of each type of fraud attack will vary, and the likelihood of each must be considered separately in light of the hacker organization's perceived aims and target.

Malicious Threat Agent — Disaffected Staff

A disaffected staff member will be seeking to cause damage to the image or structure of the organization or to extract value in the form of funds or property of some value. Indicators of potential disaffected staff can be isolated, and a number of identified case histories can be used to identify significant common factors from these case histories.

Any form of usable information on the capability of a disaffected staff member to carry out a fraud attack will be in the public domain from open sources, providing it has been made available by the employing organization. Information that is held by law enforcement and national intelligence agencies is not likely to be made available in reasonable time because it will potentially be required for prosecution.

To carry out a fraud attack, a disaffected staff member needs to possess the appropriate level of skill. The drivers for the disaffected employee to mount an information attack will be varied, with the main ones ranging from financial gain to revenge using fraudulent attack techniques.

Malicious Threat Agent — Subversive Organizations

A staff member who belongs to a subversive organization will probably not be known to the organization by which they are employed. Membership in a subversive organization will become an issue when the fraud-related aims and objectives of the employing organization are in conflict with those of the subversive organization or when the subversive

organization can further its own fraudulent aims using the information, facilities, infrastructure, or influence provided by the employing organization.

Indicators of this type of threat agent will be difficult or impossible to identify because the motivation of the perpetrator will not be clear and it will be difficult to determine his or her membership in the organization. It is clear that some organizations will be more prone to this type of fraud-threat agent than others — for example, large and high-profile international corporations, which are the types of organizations that can leverage significant influence and favor.

Any form of usable information on the effect of subversive or secretive organizations on a corporation with regard to their ability to carry out a fraud attack will not likely be in the public domain unless it has already been made available. Information that is held by law enforcement and national intelligence agencies is not likely to be made available because it will have been gathered either as part of an investigation for subsequent criminal prosecution or as intelligence for reasons of national security.

For a fraud attack undertaken by a subversive within an organization to be effective, it is necessary that such subversives possess the appropriate level of skill. The drivers for a subverted staff member to mount a fraud attack will vary, with the main ones being the desire to gain influence and financial rewards to help support their organization.

In these cases, it may not be the individual or group that poses the most significant element of threat, but instead the organization is the target of their attention. The most likely reason for this fraud-threat agent to mount an attack on an organization would be to gain funds and/or financially harm the corporation.

CAPABILITIES

An organization or an individual's capability to mount a fraud attack and to sustain it at an effective level will vary with the complexity, resources, and sophistication of both the attacking force and the target. It may be sufficient for fraud attackers to mount an attack at any level in order to achieve their objective, but a high level of sophistication may be needed over a long period for the attack to have a significant effect.

To be effective, a malicious fraud-threat agent must have the capability to conduct and sustain an attack. The constituent elements of "capabilities" are detailed in Figure 4-2.

To be able to carry out an attack, a malicious threat agent must have the necessary means, skills, and methods. In some cases, these agents must also have a sustainable depth of capability in order to achieve their aims.

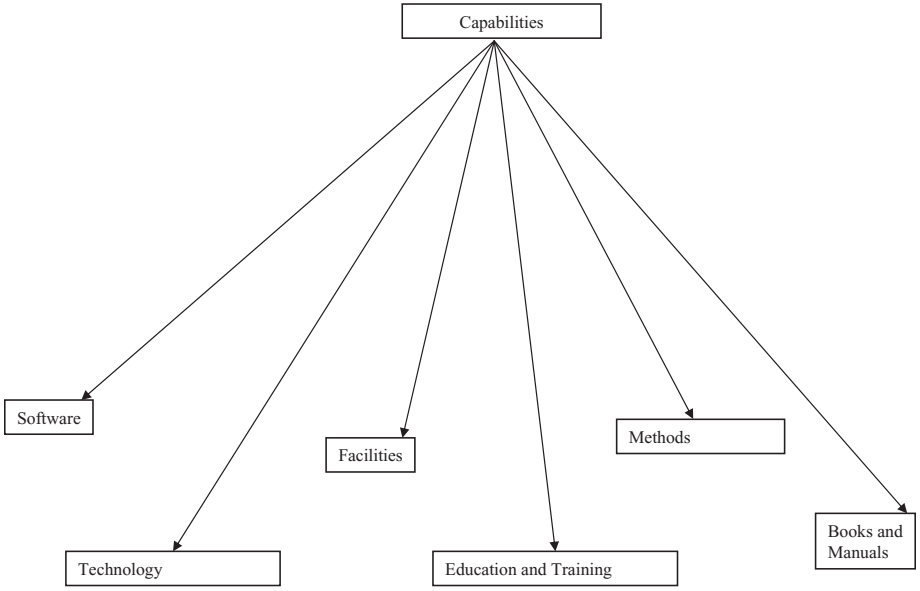


Figure 4-2. Components of malicious fraud attack capabilities.

MOTIVATION

The motivation to carry out a malicious attack may arise from any number of situations. Some commonly accepted motivational drivers are political, secular, personal gain, religion, revenge, power, terrorism, curiosity, and the like.

The motivation of the fraud-threat agent is a subjective area influenced by a wide range of factors dependent on the originating threat agent. The preceding motivational factors are not intended to be a comprehensive list, but rather to indicate the range of potential drivers. In some cases, a number of these drivers will act together to influence the threat agent (see Figure 4-3).

Fraud-Threat Agent Motivators

The factors and influences that motivate a threat agent are diverse and may operate either singly or in unison. Although a range of groupings of threat agent motivators can be easily generated, the reason that each of the factors would come into effect and the degree to which they would influence the threat agent are subject to many varying influences.

The primary groupings of threat agent motivators are detailed in the following listing, together with a general description, but no further

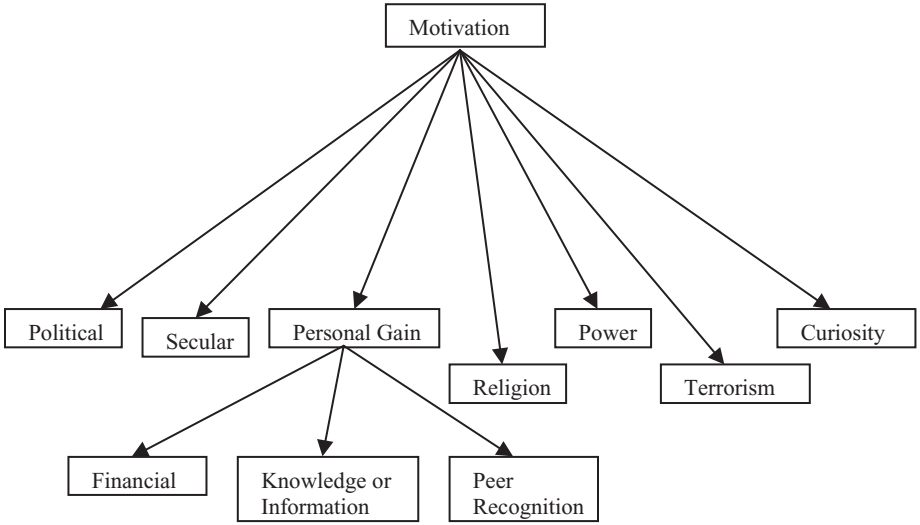


Figure 4-3. Components of the fraud-threat agent motivation factors.

analysis of this subject area will be undertaken here. The main motivational factors are:

- Political. Where the motivation is for the advancement of a political cause, it may be because the threat agent wishes to further the cause of the political organization or their own position within the political grouping. The outcome may be an attack on a political party's Web site or the denial of service of a resource, particularly during the period running up to an election.
- Secular. If the threat agent's motivation is to support his or her secular beliefs, it is possible that the agent's level of action is quite high. A person who is supporting his or her own secular beliefs will be likely to pursue an attack to a final conclusion.
- Personal Gain. A number of aspects have been grouped together under this general descriptor, as individuals are motivated by different rewards and gains.Three types of gain have been identified. The first is financial gain, through which the threat agent will gain money, goods, or services upon carrying out the attack. This may be direct gain through using stolen credit card numbers, or it may be indirect gain through being paid to carry out the attack. The second type of gain is the acquisition of knowledge or information. In this area the benefit that the threat agent may seek is in the information itself or the knowledge that is gained in obtaining access to the information. The third type of personal gain is in the form of recognition by the threat agents' peers. As a result, the threat agent may gain status

among his or her peers or get access to additional information or resources as a result of having demonstrated certain abilities.

- Religion. This is one of the more regularly observed motivational factors. Religious conflicts are among the most common, and as a result it is expected to be a major motivational factor for a threat agent. Attacks on these types of targets are common, given the number of conflicts that are occurring at any point in time, as well as the profile of the varied religions and an attacker's ability to identify not only the religious artifacts but also the assets of the adherents of that religion (in a number of cases, it is possible to tell an individual's religion from his or her name).
- Power. If an individual seeks to gain power or to demonstrate already attained power, he or she may choose to demonstrate his or her capability through an attack on an information system.
- Terrorism. A relatively new phenomenon, cyberterrorism has not yet been conclusively observed. Conversely, the terrorists' use of information systems is well proven.
- Curiosity. Curiosity is a strong and difficult factor in quantifying motive. Because it is normally unfocused and will only be directed at the target in question while the curiosity lasts, it is difficult to predict or to determine when the threat agent will have sated his or her curiosity.

The elements that provide the motivation for an individual or a group to carry out an attack will be highly variable and subjective. What constitutes motivation to one individual or group may not affect another similar group in the same way. The following elements are general indicators only. (No attempt has been made to quantify or value the effect of the preceding factors on the threat agent as this is outside the scope of the project.)

ACCESS

In order for threat agents to carry out a fraud attack on corporate assets, they must have access to those assets, either directly or indirectly. By indirectly, we mean that the defrauder causes someone to take some action that will support the defrauder's attack. Furthermore, in today's high-technology and microprocessor-driven world, such attacks can likely be accomplished through electronic access (via other networks).

A defrauder may, for example, use "social engineering" techniques — that is, try to talk someone into doing what the defrauder wants them to do or provide the defrauder with the information needed to assist in perpetrating the fraud. Using such methods as posing as someone else, gaining information through normal discussions with the person having

that information, and getting that person to talk about their jobs, company, and so on, the defrauder can often successfully receive the information needed.

> Without direct or indirect access to corporate assets, a fraudulent attack cannot be successful.

CATALYSTS

A catalyst is required to cause a fraud-threat agent to select the target and the time at which the attack will be initiated. The catalyst could be something that affects either the target or the threat agent.

The causal factor in a fraud-threat agent's decision on whether and when to carry out an attack on corporate assets may be as a result of an event, such as publicity for a organization with which the agent has a disagreement, or perhaps the start of an armed conflict between the agent's country and an opponent. Another factor may be the defrauder's circumstances, and any change (perhaps in location, social grouping, employment, or financial status) may affect the defrauder's ability or desire to carry out an attack.

An attack may also be triggered by the advent of a new technology, which makes what was previously not achievable a possibility (see Figure 4-4).

The catalyst may be either real or perceived. Examples of catalysts are a change in the employee's employment status or a negative change in the employee's financial condition (see this chapter's case study for a more detailed example).

The main groupings of threat catalysts have been identified as:

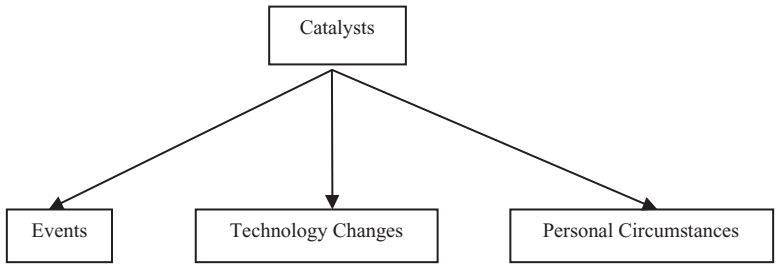


Figure 4-4. Components of the fraud-threat agent catalysts.

- Events. An event may be related to the attacker or to the target, either directly or indirectly. An event that influences the threat agent might be a personal experience or exposure to news that triggers predetermined actions. An event that affects the target might be a research and development success that might change the value of the company and damage a competitor who may want to "get even."
- Technology Changes. A change in technology occurs at approximately nine-month intervals, and as a result, new uses for technology become apparent, and shortcomings in the technologies in use become understood in the wider community. This constant technology churn can be the catalyst for fraud-threat agents to carry out an attack as they see an opportunity developing.
- Personal Circumstances. The fraud-threat agent's personal circumstances may change as a result of exposure to information that affects his or her values or beliefs. Alternatively, the change might come as a result of the actions of others, such as the agent's being fired from his or her job, thereby opening the time needed to conduct a fraud attack, and having the motivation of revenge against the former employer. Another alternative may be an elevation in position or peer regard and a desire to demonstrate one's skills.

INHIBITORS

A number of factors (effectors) will inhibit a fraud-threat agent from mounting an attack either on a specific target and/or at a specific time. Again, these factors may affect either the target or the threat agent. An example may be the perception that the targeted corporate assets are well protected and that any attempt to attack them will be quickly detected.

A range of factors will both inhibit and assist a fraud-threat agent in perpetrating a successful attack. These factors have been labeled as inhibitors and amplifiers. The inhibitors are identified in Figure 4-5.

An inhibitor will either prevent a fraud-threat agent from carrying out a successful attack or minimize the impact of a successful attack or reduce a threat agent's inclination to initiate an attack. These inhibitors constitute the heart of any anti-fraud program and are often called anti-fraud defenses; in some cases they are called controls. These inhibitors include:

- Fear of Capture. If threat agents have the perception that, if they initiate an attack, they are likely to be identified and captured, this perception will act as a deterrent and will inhibit the perpetrator.
- Fear of Failure. If the threat agents believe that they are likely to fail in their attempt to conduct an attack, this belief may deter them from trying. This effect will be further enhanced if they are sensitive to the

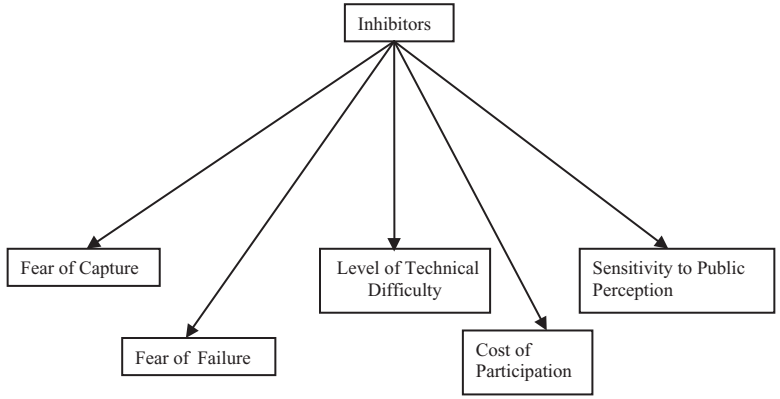


Figure 4-5. Components of fraud-threat agent attack inhibitors.

opinions of others and believe that the failure will become known to them.

- Level of Technical Difficulty. If the defenses of a target that has been identified by a fraud-threat agent are shown to be difficult to overcome, then this will, in most cases, reduce the likelihood of the threat agent attacking the system as the threat agent will search for a less challenging target. In some cases, this situation may be inverted as the threat agents will attack the most difficult of targets to prove or demonstrate their skills and abilities.
- Cost of Participation. If the cost of undertaking the attack is too high, the fraud-threat agent will be deterred from initiating the attack. The cost may be in terms of finances or of the appropriate equipment or of time or information.
- Sensitivity to Public Perception. If the target that the threat agent has selected is one that would gain the threat agent disfavor in the eyes of the public, this may act as a deterrent. An example would be an attack on the military resources of your own country during a conflict or an attack on a respected charity. The threat agent's sensitivity to public feelings may inhibit the action.

A threat inhibitor will be any factor that decreases the likelihood of either a fraud attack taking place or an attack being successful. The factors may be either real or imagined. Examples of inhibitors may be publicity relating to individuals being prosecuted or investigated for attempting to break into a corporate network or a change in the state of the security of a system in order to perpetrate a fraud.

Threat inhibitors will, in a manner similar to threat amplifiers, be a mixture of transient and longer term influences. As a result, the sources of information on these threat inhibitors will be varied. The added dimension relating to these influencing factors is that some are real and others are perceived.

Other Issues That May Inhibit Fraud Threats

- Law Enforcement Activity. If the laws within the target country or the country from which the fraud-threat agent is operating are strong and relevant and have been tested in the courts and shown to be effective, and if the law enforcement community is seen to be aggressive in its application of the law, these, too, will act as an inhibiting factor.
- Target Vulnerability. If the targeted assets that the fraud-threat agent has identified are perceived to be in a well-protected state or if the assets are thought to be protected by a variety of devices, the fraud-threat agent will likely be deterred from undertaking the attack.
- Target Profile. If the target is less attractive to the threat agent than those in similar organizations, the likelihood of an attack may be lessened.
- Peer Perception. If the consensus of opinion of the fraud-threat agent's peers is that the target would be "poor" for reasons of ease of access, resulting in no peer acknowledgment for a successful attack, or because the business of the target receives the peer's support, then the likelihood of an attack will decrease.

AMPLIFIERS

A number of factors will encourage a fraud-threat agent to mount an attack against a particular target. Again, these factors may affect either the target or the fraud-threat agent. An example may be the perception that the targeted corporate assets are not well protected and that an attempt to attack it will not be detected.

The types of effectors that will amplify or increase the possibility of a successful attack are varied but will include factors such as peer pressure. In this amplifier, fraud-threat agents may also have a desire to be well regarded by their peers. Their desire is to gain the recognition and respect of their fellow miscreants and peers through the demonstration of their skills, and this will strengthen their resolve to carry out the attack.

The fraud-threat agent's level of education and skill will improve his or her confidence and increase the likelihood of success. The amount of access to the information that the fraud threat agent needs in order to

mount a fraud attack will increase the possibility of a successful attack. (See Figure 4-6.)

A threat amplifier is any factor that increases the likelihood that an attack will either take place or will be successful. The factors may be either real or imagined. Examples of amplifiers may be discussion among defrauders of the discovery of a new method for penetrating the security of a particular corporate target.

Threat amplifiers may be a mixture of transient and longer term amplifiers; as a result, the sources of information on these will be varied. There is an added dimension with these influencing factors in that some are real and some are perceived.

Of the factors that were identified, the following were considered to be the most significant:

- Peer Pressure. Threat agents may be more likely to carry out an attack if they feel that to do so will enhance their prestige or status within their peer group. Particularly within system-hacking circles, elevated status and regard by other hackers will gain the individual access to information and resources that they did not have before and will also achieve one of their aspirations of increased status within the community.
- Fame. In all social groupings, a proportion of the defrauders will seek to be recognized for the actions they have undertaken. These actions may have been good or bad, but the attacker's desire to be recognized for his or her skill and daring will be quite high.
- Access to Information. If an individual or a group believes that they will gain access to useful information, either as a direct result of carrying out a fraud attack or as an indirect reward for it, they will, in

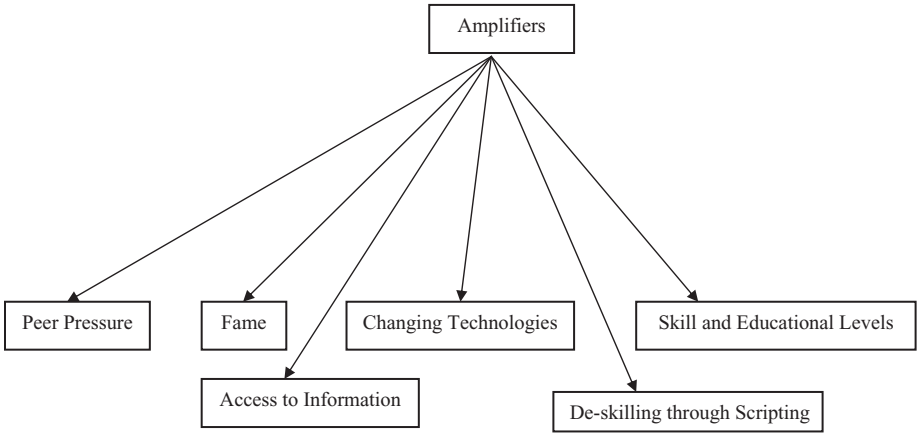


Figure 4-6. Components of the amplifiers.

some cases, be more inclined to carry out the attack. This access to information may be the primary motivation for the attack or a secondary benefit.

- Changing Technology. As technology develops, a recurrent theme that has also developed is the release of a new technology, its acceptance into common use, discovery of weaknesses in the technology, and finally exploitation of the weaknesses for illicit purposes.
- De-Skilling Through Scripting. As new techniques to subvert the security of systems are understood, the more skilled attackers, most particularly those from the hacking community, will write scripts that will automate the attack. As these techniques become available to the less skilled users who could not carry out the attack without the automated tools, the number of people who could conduct an attack is increased. Such attacks may be the basis for perpetrating frauds.
- Skill and Education Levels. As the general level of education with regard to technology increases and the use of technology becomes almost ubiquitous and as the skill level with regard to the use of new technologies increases, so the number of people who have an understanding of the technology and ways to carry out fraud-related attacks will rise.

Other Issues That Will Amplify Fraud Threats

- Law Enforcement Activity. If the laws within the target country or the country in which the fraud-threat agent is operating are perceived to be weak or not relevant to the types of activity that the attackers are using; or if the laws that are being used have not been tested in the courts or have been tested and been shown to be ineffective; or if the law enforcement community is seen to be reluctant in its application of the law — any of these alternative scenarios will act as an amplifying factor.
- Target Vulnerability. If the targeted assets identified by the fraud-threat agent are perceived to be in a poorly protected state or if they have vulnerabilities that come into effect through no fault of the security professionals or corporate management, the likelihood that the fraud-threat agent will undertake the attack will be amplified.
- Target Profile. If the target profile is more attractive to the threat agent than those of similar organizations, this will amplify the likelihood of an attack.
- Public Perception. If the public is largely opposed to the organization that the target represents (e.g., large oil corporations that are perceived to be gouging their customers through artificially high prices), then the likelihood of a threat agent carrying out an attack will be increased.

FRAUD-RELATED FACTORS FOR ATTACKING SYSTEMS

In today's high-technology environment, one must have a working knowledge of computer systems and include the use of these systems in any defense against fraud-threat agent attacks because certainly the fraud-threat agents will use such tools if they can help perpetrate a successful fraud attack on corporate assets.

In order for a fraud-threat agent to mount a successful attack on a system, at least two system-related factors must be present:

1. In order to have an effect, there must be an exploitable vulnerability in the system for the threat agent to utilize. For a vulnerability to be exploitable, it must be known, or there must be an expectation that it will be known, to the threat agent, and the threat agent must have sufficient access to the system to affect the attack. The vulnerability may exist in the hardware, the operating system software, or the applications software.
2. The target system must be important enough to the defrauder that the loss of it or a degradation in its availability, confidentiality, or integrity would support the defrauder's successful attack to defraud the corporation or other entity.

RELATIONSHIP OF THREAT ELEMENTS

The potential for a fraud-threat agent to pose an actual fraud threat through such things as an information infrastructure will be influenced by a number of factors. For the threat agent to pose a real threat to an information infrastructure, the agent must posses a capability and must also be able to gain either physical or electronic access.

The potential impact of such a threat agent will be influenced by its level of capability. The threat agent will be influenced by factors that will inhibit his or her ability to form a threat and will be strengthened by other factors. In addition, some type of catalyst will cause the agents to act, depending on their motivation. The components of "threat" that apply to a malicious threat and their interrelationships are detailed in Figure 4-7.

CASE STUDY

In this chapter, it was pointed out that motivation and opportunities play a major role in fraud-threat agent attacks or the potential for their attacks. The topic of threat agents can be discussed and written about for volumes; however, the preceding provides the corporation's chief security officer (CSO) or other security professionals with at least an overview of the topic.

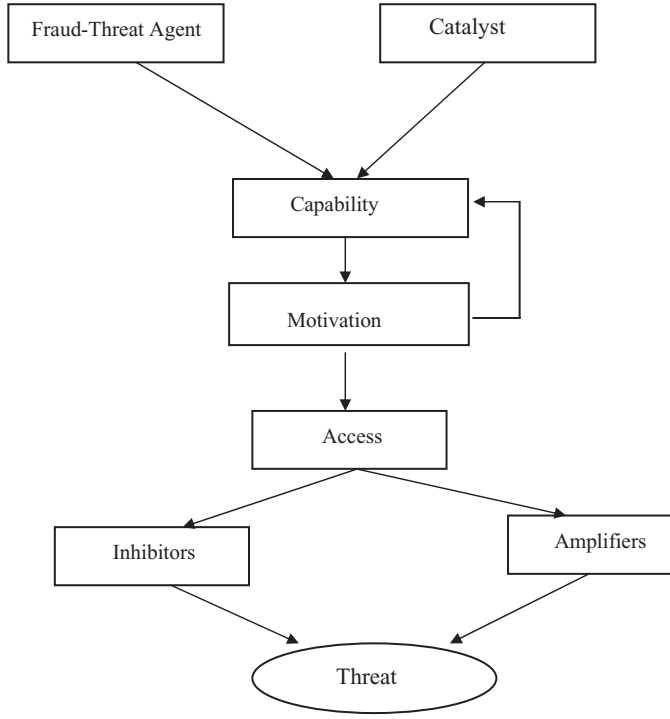


Figure 4-7. Threat components and their relationships.

As a CSO, what do you think you need to understand about fraud-threat agents? The following information may help you answer that question:

In order for a CSO to be able to mount an adequate, cost-effective defense of company assets, the CSO must understand all the types of fraud threats against the company. Furthermore, he or she must also understand the mind of these defrauders. One must understand as much as possible how these miscreants think and why they think, act, and react as they do.

Remember that first and foremost it is the human factor that is involved in all these threats and it is the human miscreants that the CSO, other security professional, or others charged with defending the corporate assets against fraud-threat agent attacks must understand. This point cannot be overemphasized, especially since it is precisely the human factor and how the miscreants think that are usually lacking in the CSO's quest to build a successful assets protection program and specifically an anti-fraud program as a standalone corporate program or as a subset of the corporate assets protection program.

The security professional, though "required" to be knowledgeable in international politics, business, marketing, finance, management, leadership, auditing, high technology, social science, psychology, and the like, must also have a good working knowledge of criminology.

Being a corporate security professional and especially a CSO is a very challenging job, and to be successful, one must have much more than just a background and experience in fighting fraud attacks and attackers. In fact, that is one of the major problems with many security professionals. Their backgrounds are usually planted firmly in basic assets protection, with the priority being given to physical security, when in fact the primary threats are rooted more in the human factors associated with the threat agents such as the defrauders.

> Understanding the human factors is at least as important, if not more important, than understanding when and how to install alarms, physical access controls, and the like.

The security professional must first of all understand the fraud threats and then use a holistic and systematic approach to finding the solution to mitigating the threats. Some threats may be completely eliminated, some may be mitigated to provide for the least amount of risks, while others may be such that the security professional can only hope and pray that the company's assets will not be threatened by the defrauders. However, it seems that there are always some of "them" around.

According to the Association of Certified Fraud Examiners and members of the criminology profession, three requirements are present when considering the human threat agent. They are the same regardless of the type of attack to be launched.

- Motive: If one is not motivated to attack a system, that person will not attack; therefore, that person is not a threat.
- Rationalization: One must be able to rationalize the attack. For example, many devoutly religious people have committed one or more crimes. If they were that religious, how could they commit such a crime when they also believe that they would go to hell and suffer eternal damnation for such crimes? They must rationalize in their minds that what they were to do was not in violation of God's law or God would forgive them. If they could not rationalize or justify it to themselves, they would not commit the crime. The rationalization need not be logical or make any sense to anyone else, but the attacker must believe it.

- Opportunity: The final part of this triad is opportunity. Those who are motivated and can rationalize an attack, but know there is no opportunity to commit or successfully commit that attack or no opportunity to commit that crime without getting caught, will not commit the crime.

When discussing this triad, it is important to remember that as human beings we will all probably commit a fraudulent act under the "right" circumstances. An internal employee of the company may be a model employee; however, if the employee's circumstances changed for the worse, elements of the triad would come into play and an employee once not considered a threat would become a threat. For example:

> You have a family with kids growing up and getting ready for college; you have a mortgage, car payments, and the normal other bills; you worked for a company for about 25 years; and you are about 54 years old. You were called into the boss's office one Friday and told the company was downsizing and was terminating your employment. However, because the company was terminating over 500 people, the federal law required that you be given 60 days notice. You knew that you would have difficulty finding another job, especially at your age, and besides that your skills were somewhat outdated, not in great demand. You didn't know how you would make it. You knew that the college money for the kids would have to be used to survive. You also knew that you'd have to sell one car as you couldn't afford two. You were also concerned about other finances. In other words, in about 60 days, you knew that your entire world would be turned upside down and you didn't know how you would survive. Gloomy enough for you? It happens every day. Sometimes by the thousands!
>
> For most people, that would be enough to start thinking somewhat negatively about the place where they work and the managers, company president, et al. However, to really push you over the edge, let's say the next morning you get up for work and read in the business section of the paper that the company you work for was having greater sales than ever and had record profits. You read on to learn that because of that, the company president was getting a $2.5 million bonus and the executive managers were getting $1 million each for saving the company so much money over the years and for increasing sales and profits.
>
> You are now motivated to get what you can from that company in the next 60 days. You deserve it. You gave them your "blood, sweat and tears" for 25 years, and they are where they are today partly because of you. And what did they give you? The boot! So now you have the motive and the rationalization. Some people use violence (e.g., the post office worker kills the manager who yelled at him). Others use fraud, theft, and whatever opportunity gives them; while yet others steal and

sell sensitive company information and destroy or modify company information and systems.

The triad "bar" is higher for some than for others. However, it is now a matter of survival, a basic and extremely strong human trait. You and your family must survive. You are not about to have your house repossessed, as well as your car, and be one of the homeless out there. Add to that a little revenge, frustration, and hostility at not being able to find another job as day 60 approaches.

Yes, we all have our limits. As a security professional, keep the triad in mind as you build the corporate anti-fraud program. It is important to know the culture and atmosphere of a company, and as the CSO, you must be tuned into the changes caused by downsizing, restructuring, mergers, and the like, for they often create additional fraud-threat agents.

As a CSO for a major international corporation, what policies, procedures, plans, processes, and/or projects would you put in place to mitigate the fraud threats based on the preceding scenario?

SUMMARY

Today's security professionals are faced with many threats, and one of the biggest and fastest growing of these threats is the fraud-threat agents. Once these agents were either internal or in some way associated with the corporation (e.g., supplier); because of such interfaces as the Internet and other businesses' networks, as well as the new global market environment where the corporation is now connected, the threats of frauds and thus the number of fraud-threat agents has grown. It appears that internal fraud threats may be equally matched by the external threats — or even exceed the internal threats.

Today's security professional must understand these internal and external (e.g., global) fraud threats to the company's assets. These fraud threats are categorized as malicious fraud-threat agents.

5

Fighting Fraud — Whose Job Is It Anyway?

INTRODUCTION

Many corporations' managers, employees, stockholders, and government oversight agencies (e.g. the U.S. Securities and Exchange Commission) continue to struggle with the unprofessional, unethical, and/or downright criminal conduct perpetrated by miscreants from inside and outside corporations. These activities include the fraudulent escapades of corporations' executive management, lower-level management, other employees, suppliers, customers, and anyone else who can see a selfish, though illegal, gain for themselves at the expense of the corporation or others.

The ever-increasing frauds perpetrated by people on corporations, internally and externally, will continue as the "What's in it for me? I deserve it! You owe me!" attitudes prevail. A combination of greed, lack of ethics, integrity, and honesty; as well as short-sighted executives, and also a lack of coherent, holistic, and proactive corporate anti-fraud programs, are some of the root causes of the fraud problems facing corporations today.

> It is not necessary to change. Survival is not mandatory. — *W. Edwards Deming*.[1]

The ferreting out of frauds within a corporation has been and generally remains the responsibility of various departments within a corporation. These may include security staff investigators, outside CPA firms, internal auditors, external auditors, the corporate ethics director, and

[1] http://en.thinkexist.com/quotes/w._edwards_deming/2.html.

basically anyone else corporate management deems to be the "logical" place to saddle a department with this responsibility. They are often scattered responsibilities throughout a corporation with either little or no delegated cohesive, consolidated leadership responsibility, nor a comprehensive, holistic anti-fraud program.

ROLE OF EXECUTIVE MANAGEMENT

The owners of a corporation or other entity expect management to be responsible for all that goes on within that corporation, including safeguarding the interests (e.g., assets) of that corporation. After all, that is why they were hired and why they get the "big bucks!"

Sadly, some of the most outrageous frauds perpetrated in the last decade, at least within the United States (although these corporations have offices, influence, and impact around the world), have been done by executive management.

> It is the responsibility of all levels of management, as well as all employees, suppliers, and others who have access to corporate assets to protect those assets from fraud.

Executive management, has taken advantage of their positions and have perpetrated frauds that have had major financial impact on their corporations, employees, and stockholders. There is no excuse for such behavior, which is done for purely selfish reasons. One would think that their millions of dollars in salary, stock options, bonuses, "golden parachutes," and other perks would leave them content. However, as we have seen, this is not the case.

Executives are sometimes able to perform such devious and fraudulent acts in collusion with others such as outside accounting, CPA, or auditing firms, which assist in rationalizing or twisting some financial or accounting procedures in favor of the corporation and executive management in order to hold on to their lucrative corporate contracts worth often millions of dollars.

The major questions that should be answered by executives — some of whom may perpetrate frauds — relative to an anti-fraud program include the following.

- Will corporate executive management approve and support a corporate anti-fraud program?
- If not, why not? Are they afraid of getting caught with their hands in the corporate assets cookie jar?

- If they will support a corporate anti-fraud program (e.g., budget), will they allow it to be sufficiently proactive and have sufficient controls in place to identify indicators of frauds by corporate executives?
- Will executive management support oversight of their activities to include looking for fraud indicators related to their actions?
- Will they support a strong corporate ethics program?
- Will they support a strong "whistleblower" policy that encourages the reporting of fraud indicators, anonymously without management trying to identify the whistleblower and easing them out of the corporation?

These are just a few of the key questions that will determine the quality and success of a corporate anti-fraud program. If executive management does not support a proactive anti-fraud program, you may wonder why. Some executives rationalize that they already have that in place by having an ethics program, auditors, outside CPA firm oversight, SEC oversight, or other such positions.

They may even maintain that by establishing a corporate anti-fraud program, they are implying or saying to the world that they need one because frauds permeate the corporation. They also say that such a formal program would be a "public relations disaster" as they would then have to explain that they are just trying to help safeguard the owners' assets and that they are not aware of any frauds within the corporation. In some respects they may be correct in what they say. However, are such excuses adequate and logical to explain away a formal corporate anti-fraud program?

Other complications that arise are due to the laws, rules, regulations, and policies that are so complex, such as those relating to accounting procedures, tax procedures, and the like, that they are often subject to interpretation that may be stretched past their logical limits. Thus, they become indicators of frauds, but it is difficult to prove intent and not just one interpretation of what is required.

So, what should executive management do? Approaching this issue from a corporate assets protection viewpoint, giving the interests of the corporate owners the highest priority, a corporation's executive management should support such a program both in spirit and with budget. Without the approval and budgetary resources support, as well as other types of executive management support, such a program is doomed to failure.

> Executive management generally will not directly say no to an anti-fraud program but will instead rationalize that such a formal program is not needed. Executives will base that decision on their use of internal and external auditors, a corporate ethics specialist, external CPA firm, SEC oversight, and the like as being their anti-fraud program.

Would a corporate anti-fraud program identify fraud indicators relative to the actions of executive management? If the program was an ideal program, possibly maybe, maybe not. That is probably not the answer you would want to hear, but it is a realistic one.

> No matter what happens in a corporation, ultimately the protection of assets, although they may be delegated for day-to-day responsibility to the CSO, rests with the executive management and cannot be delegated away to others.

ROLE OF CORPORATE MANAGEMENT

Other corporate managers will of course take their direction from executive management. In any anti-fraud program or even a general assets protection program, corporate managers have the responsibility for supporting the protection of corporate assets from frauds and other crimes, as well as protecting those assets so that they are controlled and used only as stated in corporate policies.

Corporate managers are also responsible for ensuring that all corporate employees, customers, suppliers, associates, subcontractors, and any others who have access to corporate assets do so in accordance with corporate policies. Hopefully, that will include those policies supported by procedures, plans, processes, and projects of a corporate anti-fraud program.

Currently, some management of corporations lack corporate loyalty, for they want to know what is in it for them. Based on this and other short-term views by corporate managers, is it any wonder why corporate employees feel no loyalty to the corporations? This feeling is compounded by the many corporate layoffs of employees that take place as the easy way to save corporate assets, primarily money. Those who survive the cuts see that many in management positions get ridiculously huge bonuses for saving the corporation money through layoffs.

> The Twenty-first Century Management Motto: I am as loyal as you pay me. Someone pays me more, I will be more loyal to them. So, what's in it for me?

One vice president of a large international corporation told his management staff that they should look for savings in all areas of their

department and that included laying off employees and finding ways to merge departments, even if by doing so the managers eliminated their own positions. They were told that they should do so for the good of the corporation!

Wouldn't that be a wonderful thing to do — for the good of the corporation? Can you imagine going home and telling your spouse that the kids will not be going to college, or your mortgage will not be paid in the future as you just eliminated your own job for the good of the corporation?

Do you think that the vice president will do that too? Actually, it may be possible as long as the "golden parachute" is attached to his or her back. Such attitudes by corporate managers make many employees ill at ease and cause them to begin making contingency fraud plans (e.g., "If I am going to be laid off, I am going to get even before I leave").

ROLE OF THE CORPORATE EMPLOYEES

The role of all corporate employees is to safeguard the corporate assets under their control and to do so in accordance with management direction and corporate policies, which hopefully include those requirements as stated in a corporate anti-fraud program.

That would include reporting violations of such policies as when fraud indicators are identified. Such responsibility must be told to the employees and is generally done so through security awareness and training programs that include anti-fraud briefings and possibly e-mail anti-fraud messages, pamphlets, posters, and the like.

ROLE OF THE ETHICS DIRECTOR

Over the years, may corporations, especially in the United States, have seen the need to establish a position, staff, and/or department of ethics. This need has arisen as individuals have become more, well, unethical.

The workforce that was once loyal to the corporation has gradually found that their loyalty is not reciprocated by the corporation. In fact, many in corporate management quietly discourage long-term employees from remaining as they are paid more due to their corporate longevity. Moreover, as they get older, they may require more time off for medical treatment and the corporate medical benefits will increase, making the long term employee an expensive corporate asset.

Add to that the need to "cut corners" to save money in a very competitive global environment and the decline in general morality, for example, "Why shouldn't I get my share? The means may be fraudulent but the gains are what counts."

An ethics specialist is therefore mandated in many corporations. How much they actually accomplish will be a factor of their budget, management support, and executive management direction for zero tolerance of unethical behavior — at all levels within the corporation.

Based on their primary duties and responsibilities, should they lead a corporate anti-fraud program? The answer is maybe, depending on the structure and culture of the corporation. It is my belief that they are part of the anti-fraud program team but not its leader unless that leader is also the corporation's chief security officer (CSO).

ROLE OF THE AUDITOR

Corporate internal auditors (those who are employees of the corporation and are paid directly by the corporation) are hired to internally audit corporate departments for compliance with corporate and government policies, laws, regulations, and the like.

Although some may argue that there may be a few exceptions out there in the corporate world, auditors basically look for compliance and if it looks good on paper, they are usually satisfied if one plus one equals two.

> Remember that "corporate fraud" means the frauds perpetrated against a corporation or other business-related entity by individuals within and/or external to a corporation. It does not mean frauds perpetrated exclusively by "corporations." Fraud is a "people business."

The accountants and/or auditors (who often have an accountancy background and experience) can provide a good supporting role in combating corporate fraud. However, although they have been receiving some training and gaining some experience in dealing with frauds over the years, they approach it from an auditor's viewpoint and not as part of leading an assets protection program that includes a proactive anti-fraud program.

No offense is intended to auditors or others, for they are just doing what they have been trained to do in the manner in which they were trained. Frauds are perpetrated by people, and therefore, one's anti-fraud training, education, and experience should focus in part on understanding people in general, as well as defrauders and their motivations. This aspect is not emphasized to auditors in their auditing and accounting education.

In addition, most people do not like confrontation, nor do they like dealing with hostile people. Even security and law enforcement

professionals do not like hostile encounters. However, the training and experiences of security and law enforcement professionals place them in a better position to successfully deal with people in confrontational situations.

Should the manager of the audit department also be the leader of a corporate anti-fraud program? The answer is no, for several reasons, including those stated earlier. For example, this would include compliance with the corporate anti-fraud program, as well as the audit staff writing the anti-fraud program and its policies, and perhaps also many of its processes, procedures, and such.

This would represent a conflict of interests inasmuch as they themselves approve what they have written and implemented; they also serve as the auditors to determine whether what they did was the correct thing to do and supports compliance with other corporate policies, government oversight laws, regulations, and so on.

> Today's auditors have been filling the vacuum left by the security specialists who have not taken responsibility for total assets protection, for example, protecting corporate assets from defrauders. Consequently, auditors are even becoming involved in fraud-related investigations and establishing anti-fraud programs!

ROLE OF THE FRAUD EXAMINER

A fraud examiner (certified fraud examiner) is a rather recent "profession," and for many it is an additional duty or responsibility. It is the focus of the Association of Certified Fraud Examiners (ACFE).[2] ACFE has a certification program that certifies individuals as fraud examiners if they pass an extensive examination and have a certain amount of experience.

A CFE may have the background of a federal, state, local, international, or foreign law enforcement professional, such as a detective, private investigator, accountant, auditor, or professional security personnel. The basic criterion is that the CFEs are in some way involved in fighting fraud.

Although CFEs do play a vital role in combating frauds, they generally have another and primary responsibility — auditor for a corporation. Therefore, they fall into those categories discussed earlier and are not in a position of authority or have primary leadership responsibility for protecting corporate assets, unless they are also the chief security officer (CSO) for a corporation.

---

[2] See http://www.acfe.com.

The authority for assets protection falls on the corporation's CSO, with all its accompanying duties and responsibilities. Assets protection leadership has been delegated to the CSO by corporate management.

ROLE OF THE CHIEF SECURITY OFFICER (CSO)

The corporation's CSO and staff of security professionals have for the most part shirked their professional anti-fraud responsibilities, much as they have evaded their duties and responsibilities with regard to information systems security (InfoSec). As with the InfoSec assets protection needs, corporate security professionals must take a lead role in combating corporate frauds — those that occur to or within their corporation. Until corporate security professionals begin to lead the corporation's anti-fraud efforts, the fraud problems of corporations will continue to fester and more often than not will continue to cost the corporations their profits and their poor public relations images — as it has in the InfoSec sector.

After all, what are we talking about here? We are talking about protecting the corporate assets from the fraud-threat agents. Security professionals are in a position to defend the corporation against this threat to the corporate assets, just as they are with defending the corporate assets (i.e., people, physical holdings, and information) from thieves, terrorists, and the many other threat agents.

The role of the corporate security professional is to lead a protective assets protection program whether it is formal or informal. The program is more than just a checklist of duties to be performed and responsibilities to be met. It is a commitment to the management and employees of a corporation to provide a safe and secure work environment.

A safe and secure work environment reduces the chances of disruptions to the business. Disruptions (which can be in many forms), breaches of security, and loss of information or physical assets can degrade the quality of the work environment and negatively impact the profitability of the corporation. The CSO has the lead in this protective role. Security professionals in the security department provide their skills and effort in support.

Because the security professionals are involved with all departments within a corporation, they should have some of the best overall knowledge as to the state of the corporation as it relates to employee morale, corporate projects, and problems within various departments. They also know basically what is going on throughout the corporation. If the security staff is out and about the corporation as they should be, they will probably have a better understanding of the state of the corporation than anyone else in the corporation, including the CEO. Therefore, they are in a better position to view poor assets protection processes, which leave assets vul-

nerable to frauds by those employees they see who are, for example, disgruntled.

The CEO hears what managers tell the CEO, and the security staff sees and hears what those doing the hands-on jobs are saying about their work. Therefore, the security staff can provide an overall idea of the state of security within the corporation and its vulnerabilities to frauds. However, they may also be able to provide nonsecurity help to various departments. For example, if someone is dealing with a problem and trying to figure out how to solve it, a member of the security staff may know of others within the corporation who had that problem and how to solve it. That problem solving may also be able to better secure assets from frauds, or at least the employee may "owe" the security professional a favor and repay that favor in some way, for example, identify fraud threats or vulnerabilities in anti-fraud defenses.

WHY THE CORPORATE SECURITY PROFESSIONAL?

Global markets, uniqueness of product, diversity of the workforce, customers, and a rapidly changing technological environment make the anti fraud task incorporated into an anti-fraud program more complex. Understanding how a business works is necessary, but not sufficient, for providing an appropriate level of anti-fraud protection. It takes more than just an understanding of the business to develop and implement a successful anti-fraud program; it also takes an understanding of fundamental security principles, people (human nature), and fraud schemes.

These are the basic reasons security professionals should manage the task of providing an anti-fraud program for a corporation. Do you want an auto mechanic to do brain surgery on your daughter? No, of course not. So, executive management should not take the anti-fraud program role lightly.

Investigators approach fraud from, naturally, an investigative viewpoint — solve the crime. Fraud examiners specialize in fraud-related matters; however, few come from outside the audit or investigative professions. Furthermore, within a corporation they are usually investigators (they react to fraud allegations) or auditors (they look for compliance). All serve in a reactive role. They are normally not in a leadership position responsible for protecting corporate assets — defending the assets against frauds; a proactive (offensive) as well as a defensive posture is needed. While some CSOs may also be a certified as fraud examiners, that is only a side benefit. Regardless, the duties and responsibilities of a CSO clearly call for the CSO to lead the corporate assets protection efforts, and anti-fraud program is part of that effort.

CASE STUDY

As the CSO for a global corporation, what department manager do you believe has the *leadership* responsibility for protecting corporate assets from fraud-threat agents? It is the auditors, security staff, ethics director, human resources specialist, or another department manager?

The case is made in this chapter for making that responsibility part of the CSO's duties and responsibilities, inasmuch as the CSO has leadership responsibilities for assets protection and that means from any threats, including fraud-threat agents.

SUMMARY

The responsibility for establishing and managing a specific corporate anti-fraud program is generally nonexistent, although many professionals within a corporation have a "piece of the anti-fraud action." These include the security staff, security investigators, ethics specialists, accountants, auditors, general management, legal staff, human resources personnel, executive management, and employees.

The duties and responsibilities for leading the corporate assets protection effort fall on the shoulders of the corporation's CSO and security staff. It is therefore logical that they be responsible for establishing and managing — and leading — the corporation's anti-fraud program.

This leadership role would include responsibility for establishing an anti-fraud program and establishing and leading a corporate anti-fraud team, which would include all those team members responsible for some part of the tasks related to fighting fraud such as ethics director, management, auditors, human resources specialists, and legal specialists.

6

Where There Is a Will There Is a Way — Fraud Schemes

INTRODUCTION

In discussing fraud schemes, we are also covering their history because these schemes have already been tried — usually more than once and often successfully. By understanding fraud schemes of the past, we can learn from them and develop an anti-fraud program that will identify controls and provide better defenses to protect corporate assets.

When developing a corporate anti-fraud program, we must also project these same schemes into the future and look at future technology, business changes, and environmental changes to determine whether such fraud schemes will be eliminated through the installation of improved technologies or other changes, or actually make the corporate assets even more vulnerable to these fraud schemes.

We must also "think outside the box" by incorporating future technology advances, looking into the minds of future defrauders, and brainstorming fraud schemes of the future that are not even possible today — or at least not tried as far as we know. The schemes of future fraud-threat agents must then also be considered in the establishment and management of a corporate anti-fraud program.

> A proactive corporate anti-fraud program would be a welcome change from today's mostly reactive approach!

For once, the security professionals and others should try to prepare now to meet the future fraud-threat agents so that their defenses will already be in place when these defrauders attempt to attack corporate assets. Now that would be a welcome change!

TYPES OF FRAUD SCHEMES

Defrauders in the past have used many types of fraud schemes. The following are just a few of those that have been identified. Obviously, the many types of fraud schemes that have been perpetrated, even in just the twentieth and twenty-first centuries, are too numerous to be provided here.

The objective of identifying some fraud schemes here is to give you an idea of what challenges lay ahead of you in fighting fraud and to provide at least some glimmer of the types of fraud schemes your corporate anti-fraud program must consider if you are to successfully defend the corporate assets against fraud attacks.

You may not agree with the categories identified, and you should remember that the list is not all inclusive. However, no matter what your corporation's products and/or services are, your corporation will more than likely be in the position of a victim to some fraud-threat agents' schemes. For example, even though your corporation may not be in the financial field, it will have financial transactions and a financial department. It may produce widgets, but it will also in all probability use the Internet and other telecommunications to conduct business.

When developing your corporate anti-fraud program, you should research the corporation's overall organizational structure and then identify the fraud schemes that may be used against each of the corporation's functions and departments. For example, employment fraud would be a primary concern for the Human Resources Department, which must be wary of employee applicants who provide false education and experience information and perhaps even impersonate another person.

> CNN.com on April 27, 2007 asked the following: "Have you ever lied on a resumé?" The answer was "Yes 15% and No 85%". This means that a percentage of your employment applicants may not be trustworthy.

Some may categorize the fraud schemes presented in one way or another. However, such schemes often overlap, which may make it more difficult to categorize them in one category only. For example, should you categorize an ATM fraud scheme as one under banking, financial, computer, telecommunications, or technology fraud schemes?

How you establish a set of fraud scheme categories should be based on what seems the most logical method to you as the developer of a corporate anti-fraud program. Suffice it to say that fraud schemes should be categorized and that all relevant information for each fraud scheme should be placed in a database as part of a corporate anti-fraud program. Further-

more, subsets should be established using a logical dataset naming convention so that the fraud schemes can be sorted in a variety of ways.

> Wells Fargo will never send unsolicited e-mail that requires our customers to provide personal or account information. Any unsolicited request for Wells Fargo account information you receive through e-mails, Web sites, or pop-up windows should be considered fraudulent and reported immediately. (Wells Fargo Online)

The rest of this chapter is devoted to identifying and discussing various fraud schemes that may be applicable to your corporation. A word of caution is needed here. No matter what your corporation does as far as products and/or services, you should not discount a fraud scheme because you do not think it applies to your corporation. Some examples are cited to support this view.

FINANCIAL

Under this category you should consider such matters as those related to your corporation's finance department. Also under this category one can add "Banking" and categorize all fraud schemes related to banking.

Note: Some of the schemes presented may be considered legitimate — for example, requests for information and requests for actions; however, they may also be used for fraud attacks.

Through use of the Internet as a fraud-threat agent tool, one can send out blanket e-mails such as the following:

- Dear JPMorgan Chase & Co. Member, We recently reviewed your account and suspect that your JPMorgan Chase & Co. account may have been accessed by an unauthorized third party. Protecting the security of your account is our primary concern. Therefore, as a preventive measure, we have temporarily limited access to sensitive account features. To restore your account access, we need you to confirm your identity. To do so we need you to follow the link below (link deleted by author) and proceed to confirm your information: Thank you for your patience in verifying your account information. Sincerely, JPMorgan Chase & Co. Customer Service
- We regret to inform you that the primary e-mail for your e-bay account was changed on April 10, 2005. If you did not authorize this change, please contact us using the link below: **click here and reenter your account information. Please do not reply to this e-mail. This mailbox**

is not monitored, and you will not receive a response. For assistance, log in to your e-bay account and click the Help link located in the top right corner of any e-bay page. Regards, Safeharbor Department e-Bay, Inc, The e-Bay team. This is an automatic message. Please do not reply.

- Unauthorized access to your PayPal account! We recently noticed more attempts to log in to your PayPal account from a foreign IP address. If you accessed your account while traveling, the unusual log in attempts may have been initiated by you. However, if you are the rightful holder of the account, please visit Paypal as soon as possible to verify your identity: You can also verify your account by logging into your PayPal account at (deleted by author). If you choose to ignore our request, you leave us no choice but to temporarily suspend your account. We ask that you allow at least 72 hours for the case to be investigated, and we strongly recommend that you verify your account in that time. Thank you for using PayPal! PayPal Email ID PP315
- Dear Bank of the West customer, We recently noticed one or more attempts to log in your Bank of the West account from a foreign IP address, and we have reasons to believe that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you. However if you are the rightful holder of the account, click on the link below and submit, as we try to verify your account. (In case you are not enrolled, use your Social Security Number as User Name and the first 6 digits of Social Security Number as Password): The log in attempt was made from: . . . If you choose to ignore our request, you leave us no choice but to temporarily suspend your account. We ask that you allow at least 48 hours for the case to be investigated, and we strongly recommend not making any changes to your account in that time. If you received this notice and you are not the authorized account holder, please be aware that it is in violation of Bank of the West policy to represent oneself as another Bank of the West account owner. Such action may also be in violation of local, national, and/or international law. Bank of the West is committed to assist law enforcement with any inquiries related to attempts to misappropriate personal information with the Internet to commit fraud or theft. Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the fullest extent of the law. Please do not respond to this e-mail as your reply will not be received. For assistance, log in to your Bank of the West account and choose the "HELP" link. Thanks for your patience as we work together to protect your account. Regards, The Bank of the West Corp. Copyright © 2005. All rights reserved.

- Subject: Amazon Payments Billing Issue — Greetings from Amazon Payments. Your bank has contacted us regarding some attempts of charges from your credit card via the Amazon system. We have reasons to believe that you changed your registration information or that someone else has unauthorized access to your Amazon account. Due to recent activity, including possible unauthorized listings placed on your account, we will require a second confirmation of your identity with us in order to allow us to investigate this matter further. Your account is not suspended, but if in 48 hours after you receive this message your account is not confirmed we reserve the right to suspend your Amazon registration. If you received this notice and you are not the authorized account holder, please be aware that it is in violation of Amazon policy to represent oneself as another Amazon user. Such action may also be in violation of local, national, and/or international law. Amazon is committed to assist law enforcement with any inquiries related to attempts to misappropriate personal information with the intent to commit fraud or theft. Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the full extent of the law. To confirm your identity with us click here: (address deleted by author) After responding to the message, we ask that you allow at least 72 hours for the case to be investigated. E-mailing us before that time will result in delays. We apologize in advance for any inconvenience this may cause you, and we would like to thank you for your cooperation as we review this matter.

  Thank you for your interest in selling at Amazon.com. Amazon.com Customer Service . . . this message and any files or documents attached may contain classified information. It is intended only for the individual or entity named and others authorized to receive it. If you are not the intended recipient or authorized to receive it, you are hereby notified that any disclosure, copying, distribution, or taking any action in reliance on the contents of this information is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately, then delete it from your system. Please also note that transmission cannot be guaranteed to be secure or error-free.
- From: Subject: CommonWealth Central Credit Union Online Multiple Password Failure. CommonWealth Central Credit Union is devoted to keeping a safe environment for its community of consumers and producers. To guarantee the safety of your account, CommonWealth Central Credit Union employs some of the most advanced security measures in the world, and our anti-fraud units regularly screen the CommonWealth Central Credit Union database for suspicious activity. We recently have discovered that multiple computers have attempted to log into your CommonWealth Central Credit Union

> Online Banking account, and multiple password failures were presented before the logons. We now require you to revalidate your account information to us. If this is not completed by . . . we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner. In order to confirm your Online Bank records, we may require some specific information from you. Click here or on the link below to verify your account (address deleted by author). Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account. We apologize for any inconvenience. If you choose to ignore our request, you leave us no choice but to temporarily suspend your account. CommonWealth Central Credit Union Security Team

Interestingly, often the receivers of these messages do not have an affiliation with the senders. When some of these corporations were contacted via separate e-mails, they advise that they do not conduct business this way and did not send out such e-mails.

Also note the similar patterns between these messages. For example:

- They provide the e-mail address that you are to go to instead of allowing you to go to the entities' Web site on your own.
- They imply they will need personal information such as account number and social security number.
- They threaten to cut you off from their services.
- They want you to wait awhile to give them a chance to investigate, and they ask you not to change anything until then (yeah, so they can clean out your account, steal your personal information, or make major charges to it, etc.)

When you read such things, you may wonder why anyone would answer them if they do not have an account with that business. Hopefully, most do not, but some may do so without thinking. Those who may have accounts with these businesses more than likely will answer these e-mails and provide the requested personal information. Such information would allow the defrauder to then use the information of identity theft and other types of frauds.

Why would any miscreants think they could get away with such schemes, especially if the receiver does not have an account with the business? It's simple: do a major broadcast to e-mail addresses across the Internet and see how many reply. After all, if you get one reply that allows you the defrauder to perpetrate some fraud schemes, it will be worth it. Besides, sending such messages is not costly.

Are such defrauders in fear of getting caught? Not very likely as tracking them down is difficult, requiring cooperation that is not easily

forthcoming from various law enforcement agencies. In addition, these defrauders may be living in a foreign country where there is no law enforcement jurisdiction or the amount involved is not sufficient to have law enforcement even take an interest.

And such things as the following do not help:

> **Info on 3.9 M Citigroup customers lost. . . . Computer tapes with information about consumer lending lost by UPS in transit to credit bureau. . . .** EW YORK (CNN/Money) — Citigroup said Monday that personal information on 3.9 million consumer lending customers was lost by UPS while in transit to a credit bureau — the biggest breach of customer or employee data reported so far.[1]

If your employees receive such an e-mail, and they may do so at work through no fault of their own, you would want this information reported to you and also you want to be sure to incorporate such a scheme into your employee fraud awareness program and, through coordination with your information technology department (IT), have this e-mail address blocked as part of the corporation's e-mail filtering process.

Why you may ask? In many cases, the receivers of such messages do not even have an account with this financial institution, and by going to their identified link, you are identifying yourself to the defrauders. In addition, in all probability they will ask for your personal information such as full name, social security number to "prove" your identity, and your account number.

When such e-mails are brought to your attention, you should call the security department of the financial institution or e-mail them the received message asking them to verify it. You may or may not be surprised to receive replies stating that they did not send out such a message. When contacting them, do NOT use a Web site or e-mail addresses supplied by the potential defrauder's e-mail.

CREDIT CARD SKIMMING[2]

The U.S. Secret Service and others warn of credit card skimming. A waiter or waitress (or others) at a restaurant or other place of business uses a magnetic card reader and slides your credit card through it on the way to the cash register or credit card machine — or at another convenient time.

---

[1] http://money.cnn.com/2005/06/06/news/fortune500/security_citigroup/index.htm?cnn=yes.

[2] Broadcast on the History International Channel's World Justice Program, February 23, 2006.

The "skimmer card reader" may then be taken, as an example, to someone in a car parked nearby and loaded into a computer. It is then sent via e-mail to contacts anywhere in the world. From there, it is used to make fraudulent copies of your credit card or otherwise used to get cash and/or make purchases. This may happen while you are finishing your coffee awaiting the credit card slip to sign!

If you are using a corporate credit card, this kind of fraud will obviously impact your corporation. So, it behooves you to determine whether corporate employees use corporate credit cards and to see that there are controls in place to help prevent such a fraud-threat agent attack using this fraud scheme.

Furthermore, such schemes should be incorporated into an employee fraud awareness briefing for all employees but, if you prefer, at least those who use such a corporate credit card. For general dissemination it may help employees protect their own credit cards; prevent them for being misused; and possibly give them a reason to want to perpetrate a fraud or other crime against the corporation in order to pay such debts caused by the fraudulent use of their personal credit card.

As part of your corporate anti-fraud program, you would want to know the processes in place for obtaining such a corporate credit card, as well as the process for monitoring its use, for example, reconciling the credit card bill with the credit card expenses of the employee using the card.

MORTGAGE FRAUDS[3]

According to an article in *Fortune* magazine, the number of reported mortgage frauds increased from under 10,000 reported cases in 2003 to almost 40,000 in 2006. The reported losses inceased from just over $.2 billion in 2003 to about $1 billion in 2006, with 2005 reportedly having losses of over $1 billion.

Three of the known schemes are as follows:

- **Rent-to-steal:** A renter shows up who seems to have all the right documentation to qualify. It's a deal! . . . the renter (using an alias with fake or stolen identification) goes to the local court and files a false "satisfaction of loan" document complete with your forged signature, forged bank officers' signatures, and bank seals. . . . con artist is able to go to lenders and take out new loans on the property — often taking out several, practically simultaneously, in your name. . . . renter vanishes and three or four banks are claiming title to your home.

[3] http://money.cnn.com/popups/2006/fortune/fraud/3.html.

- **Straw-man swindle:** Con artists use a "straw man" or "straw buyer" to purchase a property . . . uses a false identity. . . . The straw buyer gets a mortgage on the property. Then the straw buyer signs the property over to the huckster in a quitclaim deed, relinquishing all rights to the property as well as the underlying mortgage. The straw buyer gives the huckster the mortgage proceeds, taking a small cut — usually 10% — for himself. The huckster doesn't make any mortgage payments and often even pockets rent from unsuspecting tenants until the property falls into foreclosure. Usually the straw man, not the mastermind, is arrested for fraud.
- **The million-dollar dump:** A con artist looks for a low-end, rundown house for sale. He approaches the seller and says he's willing to pay the full asking price — but only if the seller will . . . [give] a bigger mortgage than the house is worth. So if the owner agrees to relist the house at, say, triple the price, then the buyer can apply for a bigger mortgage. The swindler, using a false identity, takes out the supersized mortgage, pays the seller, and pockets the remainder. The house usually ends up in foreclosure.

After reading these schemes, you may think none of them applies to your corporation. However, they may apply without your even knowing it. For example, let's say that your corporation in no conceivable way has anything to do with any type of mortgage financial dealings. Does it take out mortgages on property or sell property such as an old office building or manufacturing facility? Would such schemes as the mortgage frauds described in the foregoing then be possible?

What if one of your employees was a victim to such a mortgage scheme and got deeply in debt and saw no way out? Might that employee revert to perpetrating some fraud against his or her employer, the corporation that employs you to protect the corporate assets?

If you assume that one or more of these schemes apply to your corporation as being a potential victim, what will you do about it? The obvious answer of course is to incorporate controls, awareness training, and proactive actions into your corporate anti-fraud program.

COMPUTER AND TELECOMMUNICATIONS FRAUDS

Computers have become so integrated into the business environment that computer-related risks cannot be separated from normal business risks. There is such an increased trust in computers for safety-critical applications (e.g., medical) that there is increased likelihood that attacks or accidents can cause deaths.

In addition, the use and abuse of computers have become widespread, with increased threats of frauds. Individual privacy is at risk owing to large

databases containing personal information, which is available to many unauthorized people due to poor information protection programs.

A computer and technology fraud is defined as: "Any falsification or embezzlement accomplished by tampering with computer programs, data files, operations, equipment, or media, and resulting in losses sustained by the organization whose computer system was manipulated; knowingly accessing or otherwise using a computer, without authorization or exceeding authorization, with intent to commit a fraudulent act."[4]

In the 1970s, computer frauds were rarely reported because the companies or government agencies did not want the public to lose confidence in either them or computers. Frauds were generally large dollar amounts and spectacular. Perpetrators generally were computer specialists: programmers, computer operators, data entry personnel, systems analysts, and computer managers.

In the 1980s, the type and frequency of computer fraud changed owing to the personal computer, telecommunications advancements, and networking. Perpetrators generally were workers under stress, suffering from financial or personal problems; disgruntled employees; bored; tempted by curiosity; and challenged. This was also the time of the hacker.

In the 1990s–2000s, international crime and frauds are developing as a result of increased international networking. Also, the technologies of the private branch exchange (PBX) and cellular phones brought with them the telecommunications defrauders and other miscreants that have increased as the technology became cheaper, more powerful, more globally connected, and more widely used, while being vulnerable to fraud-threat agent attacks.

Computer and telecommunications perpetrators of frauds generally are the same as in the past but now include more international defrauders and other miscreants.

The basic techniques used in manipulating computer and telecommunications systems that may support fraud-threat agents' attacks include:

[4] U.S. FBI definition.

Viruses and Worms: These represent a set of instructions that propagate themselves through computers and that deliberately perform functions unwanted by the user.

Trojan Horse: Covert placement of instructions in a program causes the computer to perform unauthorized functions but usually still allows the program to perform its intended purpose. This is the most common method used in computer-based frauds and sabotage.

Trap Doors: When developing large programs, programmers tend to insert debugging aids that provide breaks in the instructions for insertion of additional code and intermediate output capabilities. The design of computer operating systems attempts to prevent this from happening. Therefore, programmers insert instructions that allow them to circumvent these controls. Fraud-threat agents can take advantage of these trap doors.

Salami Techniques: This technique involves the theft of small amounts of assets from a large number of sources without noticeably reducing the whole. In a banking system, the amount of interest to be credited to an account is rounded off. Instead of rounding off the number, that fraction of it is credited to a special account owned by the perpetrator.

Logic Bombs: This computer program is executed at a specific time period or when a specific event occurs. For example, a programmer would write a program to instruct the computer to delete all personnel and payroll files if his or her name were ever removed from the file.

Data Diddling: This technique involves changing data before or during entry into the computer system — for example, forging or counterfeiting documents used for data entry; and exchanging valid disks and tapes with modified replacements.

Scavenging: This method includes obtaining information left around a computer system, in the computer room trash cans, and so on.

Data Leakage: Through this technique, information is removed by smuggling it out as part of a printed document, encoding the information to look like something different, and taking it from the facility.

Piggybacking/Impersonation: Physical access is one method used. For example, the fraud-threat agent follows someone in through a door with a badge reader; electronically uses another's user id and password to gain computer access; or taps into the terminal link of a user to cause the computer to believe that both terminals are the same person.

Simulation and Modeling: The computer is used as a tool or an instrument to plan or control a criminal act.

Wire Tapping: The fraud-threat agent taps into a computer's communications links to be able to read the information being transmitted between computers and between computers and terminals.

With regard to telecommunications today, the criminals use stolen authorization codes to hide illegal activities such as frauds. The majority of telecommunications frauds are accomplished using a computer as the weapon of choice. This method should come as a surprise to no one.

Phreakers (those hackers who attack telecommunications systems as their first choice) hack for active long-distance authorization codes on telecommunications switches. They also look for network access numbers, phone numbers, and other types of authorization codes. Once they enter, they may establish a fraudulent account for their use and the use of fellow phreakers. However, they are not above stealing codes from wallets and purses or perpetrating telephone scams via social engineering.

Other techniques include shoulder surfing by which defrauders watch the person using the telephone and see what numbers are being dialed. Once they obtain PINs or authorization codes, they sell them or give them to friends. Many are sold to call-sell operators, who use them to sell overseas, toll-free calls for approximately $20 per call, usually with no time limit. They also will set up independent three-way calls for the same purpose.

The four major types of telecommunications crimes/frauds taking place today are relative to: (1) computer dial-up systems, (2) cellular phones, (3) voice mail boxes, and (4) electronic mail.

Dial-ups are defined as those systems that can be accessed through a computer with a modem to a computer that has a modem. Hackers or phreakers will use a war dialer, social engineering, or other techniques to help them gain access to computers and telephone switches.

These "hack-attacks" are also perpetrated against pay phones, sometimes called "fortress fones" because of their construction. They are also called "single-slot coin telephones." These telephones are hacked to gain free long-distance calls, worldwide. Two pieces of equipment that can be used are:

- Blue Boxes, which imitate tones of telephone switching equipment, tell the switch the call was aborted, but actually allow unrestricted dialing (outward dialing); and
- Black Boxes, which tell the switch the phone is still ringing when it is not, allowing calls to go through (receive calls). In the United States possessing these boxes constitutes a felony.

Hackers and phreakers trade information via e-mail and through Web sites. They are used for trading information, such as dial-up information (e.g., user ids, passwords; credit and ATM card information), as well as how to build hacking tools (e.g., Blue Boxes).

The fraud associated with private branch exchanges alone has forced some U.S. companies into bankruptcy or out of business. Those businesses that are not prepared could face the same end — not to mention the destruction to the national economy that could be caused by these criminals or even by disgruntled employees.

Cellular phones are one of the recent types of technology that has been widely used to perpetrate frauds and other crimes. Criminals often use this tool because on many occasions the call cannot be traced back to them.

Electronic mail is the process of sending and storing written communications through computer networks. Using e-mail through such systems as Internet does provide vulnerabilities in that the true sender of the message can be disguised. Examples of such uses were discussed under the heading Financial earlier in the chapter.

The e-mail method can work well to assist in the economic sabotage of a business. In addition, because a sender's identity can be disguised, sensitive business information can be safely sent forward to an unauthorized address.

Computer and telecommunications defrauders can be organized crime members, white-collar workers, drug dealers, people in debt, people wanting revenge, greedy people — anyone, under the right circumstances.

ATM FRAUDS

In this age of information, financial institutions and their customers increasingly rely on computers and their associated technology to conduct financial transactions. One of the most popular systems is the Automatic Teller Machine (ATM).

The number of ATMs has increased rapidly in the last decade and continues to grow. Their networks are evolving internationally, providing ATM access to millions of people throughout the world.

With the increase in computers, networks, and ATMs comes an increase in criminals who take advantage of this new technology for personal gain. Therefore, the access to ATMs internationally causes more criminals to be able to access more systems from more locations. Also in wide use is the Electronic Funds Transfer System (EFTS), a computerized system that affects the transfer of information necessary to conduct financial transactions.

When we talk about ATM frauds, we are talking about a crime, whether prosecuted or not, that would *not* have occurred but for the presence of the ATM system.

Two basic types of complaints can be indicators of fraud: (1) customer-initiated and (2) bank-initiated.

The customer-initiated complaints include the following:

1. Unauthorized withdrawals where the customer claims the debits were not authorized.
2. Shortage of dispensing funds from the ATM where the customer claims there is a discrepancy in the amount requested from the ATM and the amount that the customer received.
3. Customer claims that the amount deposited was not credited to the customer's account.
4. Customer claims that the amount received was less than the amount posted on the monthly statement.
5. Customer claims that the deposit credited to the account was incorrect.
6. Other claims that are customer–initiated.

The bank-initiated complaints include the following:

1. Bank claims that the check deposited is uncollectible.
2. Bank personnel open the deposit envelope only to discover nothing inside.
3. The deposited checks were stolen or were fraudulent checks.
4. The customer initiated a withdrawal that caused an overdraft.
5. Other claims that are bank-initiated.

Once these complaints are made, it is sometimes difficult to determine who is at fault, and because the banks generally want to maintain good public relations with their customers and the community, they usually assume the customer is being truthful — unless proven otherwise.

Potentially fraudulent incidents can be divided into two basic categories: withdrawal-related and deposit-related.

Withdrawal-related incidents include:

1. The customer's ATM card was lost or stolen.
2. The customer made the withdrawal, but didn't remember it at the time.
3. The customer made the withdrawal with the intent to defraud the bank.
4. The ATM system malfunctioned, causing the error.

Deposit-related incidents include:

1. The customer deposited an empty envelope in the ATM.
2. The deposit was made into the wrong account.
3. The deposit was different from that keyed into the ATM.
4. The deposit was different from that noted on the deposit envelope.
5. The customer deposited a stolen or fraudulent check.
6. The customer deposited an uncollectible check.
7. There was confusion and no error existed.

8. The bank posted the incorrect amount.
9. The bank posted the deposit to the wrong account.
10. A person other than the customer made a bad deposit.

Lost or stolen ATM cards are the biggest problem for both customers and banks. It is also the most common method for perpetrating a fraud, or at least claiming that is the reason for the discrepancies in the customer's account. The ATM card's major problem is their theft, followed by lost cards and the customer's claim that he or she never received the cards through the mail system.

Most cards that are lost or stolen are in the home, followed by the retail store, car, place of employment, the street, school, and miscellaneous other locations.

Most of the stolen cards are not the target of the thief but are located in the customer's wallet or purse, which is the thief's target. Unless it is an organized ATM and credit card criminal ring, the thief does not usually target the ATM card itself.

When a customer loses possession of his card, the time it takes for that loss to be discovered plays a crucial role in whether or not that card will be used for fraudulent purposes. Another critical factor is the location of the loss and whether or not the PIN was also compromised. If the card is lost in a high-crime area, one can almost certainly assume that the card will be used to attempt to perpetrate a fraud. Many customers choose not to remember, or cannot remember, their PIN; therefore, they write it down in a convenient location — on the card itself!

Studies have shown that potentially fraudulent withdrawals can, and are, made by different categories of people, including the customer, his or her spouse or children, a boyfriend or girlfriend, another relative, or someone not related to the customer, but known to the customer, such as a neighbor.

When analyzing the potentially fraudulent incident, it should first be determined whether or not there was a loss, a customer loss or a bank loss. or whether both the customer and bank suffered a loss. This finding is important because if there was no loss, then the problem is less serious and may lead to identifying a problem in the process rather than determining that a fraud has taken place.

It has been noted that the bank denies customer claims for one or more of the following reasons:

1. The customer withdraws the claim.
2. The customer was confused and after discussions with banking officials determines the claim was not valid.
3. The customer still has his ATM card in his possession.
4. The customer gave his PIN to another.
5. The customer claimed the PIN was protected and was still in possession of his card.

6. The customer cannot or refuses to provide details relative to the loss or transaction.
7. The bank does not have any record of the transaction.
8. Other miscellaneous reasons.

What are some of the vulnerabilities or weaknesses in the ATM system that makes fraud possible? The following are a few of the most common ones:

1. The account was established with intent to defraud.
2. The ATM card was stolen from a vendor, processing center, or storage.
3. The ATM card and/or PIN was stolen through the mail system.
4. The ATM card was stolen from the mailbox.
5. Cash or checks were stolen from the deposit envelope.
6. The ATM card was not protected from family or friends.
7. The customer misrepresented himself.
8. An active ATM card was accidentally left in the machine.
9. The customer deposited an empty envelope.
10. The customer deposited a fraudulent check.
11. The customer made an offline overdraft.
12. The customer falsely reported a transaction problem.
13. A physical attack was made on the ATM.
14. A robbery took place at or near the ATM.
15. There was a wiretap on communications links.
16. Manipulation of the ATM and/or its system software took place.
17. Theft of account information occurred.
18. Account and/or transaction information was manipulated.
19. Other miscellaneous items.

As the improvement and use of computers and telecommunications systems increase, one can expect more threats from sophisticated, international defrauders and other criminals. The technology defrauder (techno-defrauder) of the future not only has the potential to steal great amounts of money through the weak systems, but also the opportunity to blackmail companies with the destruction of their automated information, not to mention sophisticated terrorist threats.

Note: the information on ATM Fraud was taken from several old U.S. government documents no longer available and whose sources have been lost, as well as the author's personal experiences.

CLICK FRAUD

> Click fraud[5] occurs in pay per click online advertising when a person, an automated script, or a computer program imitates a legitimate user

[5] http://en.wikipedia.org/wiki/Click_fraud.

of a Web browser clicking on an ad for the purpose of generating a charge per click without having actual interest in the target of the ad's link. Click fraud is the subject of some controversy and increasing litigation owing to the advertising networks being a key beneficiary of the fraud whether they like it or not.

Use of a computer to commit this type of Internet fraud is a felony in many jurisdictions, for example, as covered by Penal Code 502 in California in the United States and the Computer Misuse Act 1990 in the United Kingdom.

Click fraud has brought arrests with regard to malicious clicking in order to deplete a competitor's advertising budget.

In 2004, a California man created a software program that he claimed could let spammers defraud Google out of millions of dollars in fraudulent clicks. Authorities said he was arrested while trying to blackmail Google for $150,000 to hand over the program.[6]

According to the Click Fraud Network (CFN), "the costs for pay-per-click search advertising have skyrocketed. Click fraud is a significant problem that needs to be addressed. Over 70% of search advertisers are worried about this threat to search campaign ROI" (Return on Investments).[7]

The CFN identified five signs of click fraud:

1. Your pay-per-click campaign costs are continuing to rise while your online sales are not meeting expectations.
2. Your conversion rate for paid search is lower than the conversion rate for your free listings.
3. The cost-per-click for each of your best performing search terms has been steadily increasing.
4. You suspect your competitors are deliberately driving up your costs by generating fraudulent clicks.
5. You do not have a tool in place that is specifically designed to catch click fraud.

Click fraud is a perfect example of a scheme that could not have been perpetrated in the past. The primary reason is that the technology was not

[6] Ibid.
[7] http://www.catchclickfraud.com/?campaign=google&adgroup=CCF.

available or was being used in such a manner that could not even provide for the idea of such a fraud scheme.

This is also an example of why every corporate anti-fraud program must provide processes to keep up with high-technology developments, new fraud schemes, and also brainstorming sessions to identify ways to perpetrate new frauds. Based on the information developed, the anti-fraud program would then be updated to provide defenses against such attacks even before some fraud-threat agents tried such attacks.

CLIP-ON FRAUD[8]

Tele-defrauders and other criminals are always looking for innovative ways to steal telephone service. They are driven by the free services and by the prospects of the profit to be derived from the illegal activity. A vast majority of tele-abuse is committed through Customer Premise Equipment. Defrauders and other miscreants will continue to take advantage of the vulnerabilities of unsecured PBXs and communications networks.

Although it is essential that network risk management strategies continually be considered, let's not forget some of the old and tried fraud methods. Clip-on fraud, which was prominent in the 1970s and ebbed in the 1980s, may be making a comeback. It is unknown exactly how much clip-on fraud has cost corporations, such as telecommunications corporations, but hundreds of thousands of dollars in illegal calls are currently being rung up.

Typically, the way clip-on fraud works is as follows: a tele-defrauder will attach a butt phone to the copper connectors in a "b-box," which is generally located on a sidewalk. The b-box serves as a junction for the phone lines to hundreds of homes and businesses in a particular area. Once inside the b-box, the tele-defrauder clips on to the phone lines and finds the dial tone. A newer variation of clip-on fraud involves the use of a cordless telephone and a portable battery. After the base station is connected to the terminals in the b-box, the phone moves with the tele-defrauder, allowing him to operate in a secure location 200′ to 300′ from the terminal, reducing the possibility of detection. In more sophisticated cases, the phone line's dial tone is forwarded to a nearby pay phone. In either scenario, after having established a base of operation, the call-sell operation begins where people line up to pay for calls.

The vast majority of clip-on fraud cases have occurred in Southern California with its vast immigrant population. The tele-defrauders have a

---

[8] Information based on a discussion between the author and Jerry Swick, former senior investigator — MCI and retired Los Angeles Police Department Lieutenant, Computer Crime Unit.

ready market of people wanting to make inexpensive international calls to their friends and families. This fraud occurs primarily on the weekends in light industrial or commercial areas.

Clip-on fraud activity shows up as direct dial calls on the customers' bills. When the customers receive their bill, they are confused and do not realize they have been victimized. A company in Los Angeles racked up more than $30,000 in fraudulent long-distance calls not realizing that telefraudulers clipped on to their phone lines from a b-box located blocks from their location. Moreover, to make matters worse, the company's ability to conduct business was affected because their lines were tied up. It is important to note that the FCC has ruled that clip-on fraud that can be proved to be on the local exchange carrier's end of the demarcation line is the responsibility of the local exchange carrier (LEC). This ruling establishes an important precedent when trying to resolve billing issues.

Clip-on fraud is a complicated problem and is not easily detected. The users and carriers are at risk and should consider some basic security measures. The LECs are upgrading security at the b-boxes in the affected areas. Monitoring for suspicious activity on the network and international call blocking are among the practical attempts to get a handle on the problem.

Most importantly, users should check monthly bills for any unauthorized calls. It is clear that no one solution will prevent clip-on fraud from occurring. A company should tailor security measures to the way they conduct business, as what works for one may not work for all. A collaborative effort on the part of both local and long-distance carriers as well as the customer is very important.

When developing your corporate anti-fraud program, be sure to look at the various computer and telecommunications schemes to determine which ones may apply to your corporation. Then ensure that your anti-fraud program includes controls and other defenses in place to mitigate the risk of such fraud-threat agent attacks. This would include an evaluation of the corporate processes in place in dealing with the uses of these technologies.

SECURITIES FRAUDS

Securities fraud (e.g., stock fraud) affects many corporations and obviously their owners, the corporate owners (stockholders).

Since the Crash of 1929, securities fraud has affected the average investor more and more. Retirees, single parents, and people saving for their children's educations lose their life savings to fly-by-night con men. . . . What is securities fraud? In most cases, it's nothing more than stealing. Sure, the securities laws contain a more technical definition. But

when investors are enticed to part with their money based on untrue statements, it's securities fraud — and it's illegal.[9]

The schemes to inflate or deflate stock prices for personal or corporation gain is not new. However, such schemes seemed to have increased during the last years of the twentieth century and into the twenty-first century.

There have been security frauds related to "penny stocks," hedge funds, mutual funds, and the like. The schemes and actions taken against them are too numerous to mention here. As with all fraud schemes, by using an Internet search engine one can find numerous sites that discuss this fraud scheme as well as many more that have not been mentioned in this chapter.

EMPLOYMENT APPLICATION FRAUDS

Today's job searchers must aggressively compete for jobs. This fierce competition pits applicant against applicant, with each applicant's formal education and experience being the baseline for qualifying for a job interview.

With such fierce competition, many applicants falsify their experiences and education, sometimes claiming to have a graduate degree when they do not. The applicant hopes that the corporation does not have a policy with related procedures and processes in place to verify their education and experience claims.

If your corporation does not have such a process and one that can be considered incorporated into an anti-fraud program, you do so at your corporation's peril. Think about it. If the employee will falsify such records and rationalize it, how strong are their moral and ethical beliefs to stop them from perpetrating additional frauds on the corporation and in doing so being able to rationalize it?

One security professional at a major international corporation, who had a system in place to interview an applicant's character references, check credit records; and verify previous employment and education, stated that about 15% of all applicants included false information on their application (personal interview with author).

IDENTITY THEFT SCAMS

We have heard the many horror stories about identify thefts and identity scams. Therefore, there is little need to discuss them in depth in this

[9] http://www.fool.com/specials/2000/sp000223fraud.htm.

chapter. However, to make the point that fraud-threat agents are continuously trying various old and new fraud schemes to separate people and corporations from their assets, the following vignette is offered:

A new identity theft scam is being perpetrated on unsuspecting victims. In this scam, the scammer calls the residence or office number of the victim and identifies him/herself as an officer or employee of the local court of jurisdiction. The scammer announces to the victim that he/she has failed to report for jury duty, and that a bench warrant was issued against them for their arrest. The victim's reaction is one of shock and surprise, which places them at an immediate disadvantage and thus much more susceptible to the scam. The victim will rightly deny knowledge of any such claim, that no jury duty notification was ever received.

The scammer shifts into high gear, reassuring the victim of the possibility this is all "just a misunderstanding" or "some sort of clerical error" that can be straightened out on the phone. All they need to do is "verify" their information with a few simple questions. Any reluctance on the victim's part and the scammer will threaten that the failure to provide the information will result in an immediate execution of the arrest warrant.

The scammer obtains names, social security numbers, and dates of birth, and will solicit credit card or bank account numbers claiming these will be used by their credit bureau to "verify" the victim's identity. Family members who receive these calls are especially vulnerable to coercion. Threats against the victim's career, should he/she be arrested and now have a criminal record, are frightening and persuasive.[10]

Although such a scheme may not have direct implications for the corporation, as with other more personal-related schemes, such attacks may cause employees to consider perpetrating frauds against the corporation to recoup their losses. Often they see no way out other than to take such action. They may also do so out of fear that their corporation may be notified and consider them a "security risk" and mark them for a layoff at the first opportunity.

If the employee were to bring his or her problems to someone in the corporation, what would be the reaction of your corporation? How would that reaction impact the corporation's protection of assets and the anti-fraud program?

"NIGERIAN SCAM"

> The Scam operates as follows: the target receives an unsolicited fax, email, or letter . . . containing either a money laundering or other illegal proposal OR you may receive a Legal and Legitimate business proposal

[10] The author received this via email and the sender wanted to remain anonymous.

> by normal means. Common variations on the Scam include "overinvoiced" or "double invoiced" oil or other supply and service contracts where your Bad Guys want to get the overage out of Nigeria (Classic 419); crude oil and other commodity deals (a form of Goods and Services 419); a "bequest" left you in a will (Will Scam 419); "money cleaning" where your Bad Guy has a lot of currency that needs to be "chemically cleaned" before it can be used and he needs the cost of the chemicals (Black Currency 419); "spoof banks" where there is supposedly money in your name already on deposit; "paying" for a purchase with a check larger than the amount required and asking for change to be advanced (cashier's check and money order 419); fake lottery 419; chat room and romance 419 (usually coupled with one of the other forms of 419); employment 419 (including secret shopper 419); and ordering items and commodities off "trading" and "auction" sites on the web and then cheating the seller. The variations of Advance Fee Fraud (419) are very creative and virtually endless, so do not consider the above as an all-inclusive list!
>
> At some point, the victim is asked to pay up front an Advance Fee of some sort, be it an "Advance Fee", "Transfer Tax", "Performance Bond", or to extend credit, grant COD privileges, send back "change" on an overage cashier's or money order, whatever. If the victim pays the Fee, there are often many "Complications" which require still more advance payments until the victim either quits, runs out of money, or both. If the victim extends credit on a given transaction etc. he may also pay such fees ("nerfund" etc), and also stiffed for the Goods or Service with NO Effective Recourse.
>
> Quoted from http://home.rica.net/alphae/419coal/. See that site for more details.

This fraud scheme has been around for some time, but it is interesting to look at all its many recent "variations on a theme." It began in the early 1990s in West Africa by miscreants there who began by sending out about 30,000 letters a week. They identified their potential fraud victims through country telephone books. It has gotten so bad now that this fraud scheme has gone from letters to faxes to e-mails. The Criminal Code in Nigeria identified this scheme as a fraud under Law 419, the so-called 419 scheme — taking money under false pretenses.

For some of the victims the old adage "If it is too good to be true, it usually is" never crossed their minds as they accepted the offers. At least three victims were reportedly murdered when they went to Nigeria to collect their money.

This "419" fraud scheme is somewhere between Nigeria's third to fifth largest industry! It apparently all began in the 1980s–1990s when the Nigerian economy collapsed and some out of luck people turned to this fraud, also known as an Advanced Fee Fraud. It has grown to such a large global scale that the U.S. Secret Service set up a task force in Lagos in 1995

mostly to address the issues associated with this scam. Some of these fraudsters have since moved on to drug trafficking.

This is one type of fraud that leads to the death of its victim, and obviously this type of scheme should be part of a corporate anti-fraud program and be included in the fraud awareness briefings to employees. After all, many of these e-mails are received at work. Furthermore, the protection of corporate assets includes corporate employees as one of the corporation's most valuable asset groups.

The number of e-mails sent out relative to this type of fraud can be done easily and cheaply from anywhere in the world to anyone in the world. As a result of improved Internet and e-mail technologies, the defrauders no longer even need to pay for stamps or long-distance telephone calls to fax machines around the world.

ACCOUNTING FRAUD SCHEMES

There are many type of accounting fraud schemes.[11] Following are just some of them that may apply to your corporation and must be considered in any successful corporate anti-fraud program:

On-Book Frauds

On-book frauds are those that occur within a corporation or other entity. It includes illicit payments or activities that are recorded, generally in some disguised manner, in the corporation's regular books and records. Some examples include payments to a phony vendor generated by fictitious charges to travel, entertainment, or other miscellaneous accounts.

On-book frauds are normally detected at the point of payment. For example, if a payment is made to a fictitious vendor, the fraud might be discovered by examining the addresses of all vendors. The address for a fictitious vendor may match up with either a post office box or an employee's address.

Off-Book Frauds

Off-book frauds normally occur outside the accounting mainstream and, therefore, no audit trail is likely to exist. Generally, for an off-book fraud to occur, the corporation usually has unrecorded vendor rebates or significant cash sales.

---

[11] Some of this information was provided by ACFE as incorporated into their training courses, and is stated here with their permission, as well as U.S. government anti-fraud courses and the author's personal investigative experiences.

Some examples of off-book frauds include bribery and kickbacks. Off-book frauds are typically proved at the point of receipt; that is, the initial "red flag" will appear with regard to the receipt of illicit funds. For example, if an employee has suddenly purchased a new car and a new home, but the employee's salary has not changed, then one might conclude that the employee has received wealth from an outside source. If there is no logical explanation for the increased wealth, and irregularities are suspected, further investigation may be recommended to determine the source of the possible outside income.

Cash

Cash is the focal point of many accounting entries. Cash, both on deposit in banks and petty cash, can be misappropriated through many different schemes that include:

— Skimming
— Voids/Under-rings
— Swapping checks for cash
— Alteration of cash receipt tapes
— Fictitious refunds and discounts
— Journal entries
— Kiting

Skimming

Skimming is the process by which cash is removed from the entity before the cash is recorded in the accounting system. This is an off-book scheme; receipt of the cash is never reported to the entity. A related type of scheme is to ring up a sale for less than the actual sale amount. (The difference between the actual sale and the amount on the cash register tape can then be diverted.) This is of particular concern in retail operations (for example, fast food restaurants) in which much of the daily sales are paid by cash, and not by check or credit card.

Voids/Under-Rings

There are three basic voids/under-ring schemes.

- The first is to record a sale/cash receipt and then void the same sale, thereby removing the cash from the register.
- The second, and more common, variation is to purchase merchandise at unauthorized discounts.
- The third scheme, which is a variation of the unauthorized discount, is to sell merchandise to a friend or co-conspirator utilizing the

employee's discount. The co-conspirator then returns the merchandise for a full refund, without regard to the original discount.

Swapping Checks for Cash

One common method in which an employee can misappropriate cash is to exchange his or her own check for cash in the cash register or cash drawer. Periodically, a new check is written to replace the old check. This process can be continued such that, on any given day, there is a current check for the cash removed. This is a form of unauthorized borrowing from the company. Obviously, if it is the company policy that cash drawers or registers must be reconciled at the conclusion of each day and turned over to a custodian, then this fraud scheme is less likely to be committed. However, if personnel are allowed to keep their cash drawers and only remit the day's receipts, then this method of unauthorized borrowing is allowed to continue.

Alteration of Cash Receipts Documentation

A lack of segregation of duties can create an opportunity for that employee to misappropriate company funds. For example, if the same person is responsible for both collecting and depositing the cash receipts, then this person has the ability to remove funds from the business for his or her own personal use and conceal such theft through the deposits. This is often the case in smaller organizations in which there are few personnel to divide the daily operations between. A variation of this scheme is to mutilate or destroy the cash receipt documentation in order to thwart any attempt to reconcile the cash deposited with the cash receipts.

Fictitious Refunds and Discounts

Fictitious refunds are those in which the employee enters a transaction as if a refund were given; however, no merchandise is returned, or no discount is approved, which substantiates the refund or discount. The employee misappropriates funds equal to the fictitious refund or discount. This scheme is most prevalent in the retail/merchandise industry.

Journal Entries

Unauthorized journal entries to cash are not as common as the preceding schemes. This type of scheme may be easier to detect because its method of concealment is more obvious. The typical journal entry scheme involves

fictitious entries to conceal the theft of cash. If the financial statements are not audited or reviewed, this scheme is relatively easy to employ. However, for larger businesses with limited access to journal entries, this concealment method may be more difficult to use. Generally, fraud schemes that involve journal entries to cash are more likely in financial institutions where there are numerous, daily entries to the cash account.

Kiting

Kiting is the process whereby cash is recorded in more than one bank account, but in reality, the cash is either nonexistent or is in transit. Kiting schemes can be perpetrated using one bank and more than one account or between several banks and several different accounts. Although banks generally have a daily report that indicates potential kiting schemes, experience has shown that they are somewhat hesitant to report the scheme until such time as the balance in their customers' accounts is zero.

There is one important element common to check kiting schemes: all kiting schemes require that banks pay on unfunded deposits. This is not to say that all payments on unfunded deposits are kiting schemes, but rather, that all kiting schemes require that payments be made on unfunded deposits. In other words, if a bank allows its customers to withdraw funds on deposits on which the bank has not yet collected the cash, then kiting schemes are possible. In today's environment whereby customers are utilizing wire transfers, kiting schemes can be perpetrated very quickly and in very large numbers.

Accounts Receivable — Four Basic Schemes

There are four basic accounts receivable schemes:

— Lapping
— Fictitious sales with corresponding accounts receivable
— Diversion of payments on old written-off accounts
— Borrowing against accounts receivable

Lapping

Lapping is the recording of payment on a customer's account sometime after the payment has been received. The term lapping is used to describe a method of concealing a defalcation, wherein cash received from a customer is originally misappropriated by the employee, and, at a later date, cash received from another customer is credited to the first customer's account.

The second customer's account is credited still later by cash received from a third customer. This delay of payment applications (credits) continues until it is detected, the cash is restored, or it is covered up by credit to the proper customer and a fictitious charge to operating accounts.

The basic lapping scheme operates as follows: the employee has misappropriated company funds through customer A's account (for example, by diverting a cash payment or issuing a refund payable to the employee). In order to conceal the misappropriation, the employee must now record payments to customer A's account. When customer B makes a payment, the employee posts the payment to customer A's account. When customer C makes a payment, the employee posts it to customer B's account, and so on. Often the employee will falsify documents to conceal the misappropriation of the funds in a lapping scheme.

Fictitious Accounts Receivable

Generally, the motive for adding fictitious accounts receivable to the records is to disguise fictitious sales. There are two primary motives for fictitious accounts receivable:

— Meet sales quotas, or "window-dressing" the company
— Receive sales-based compensation

Diversion of Payments on Old Written-Off Accounts

Another internal fraud scheme in the accounts receivable is the diversion of payments on old or slow-paying accounts. In this scheme, once an account has been written off, the employee has the opportunity to collect the receivable and divert the funds to himself or herself, because companies typically do not keep track of old, written-off accounts receivable.

Often old accounts receivable are assigned to a collection agency for collecting. These agencies typically are paid on a percentage of the collected amounts. Fraud schemes can be perpetrated by these collection agencies if the company does not monitor the method by which the agency receives old accounts and the collection process itself.

The assignor company needs to assure itself that the collection agency is being assigned only truly old accounts and not good accounts that can reasonably be expected to pay within the normal course of business. In addition, the company needs to be sure that the collection agency cannot compromise the indebtedness such that collections are not reported to the company. This would allow the collection agency to compromise indebtedness for its own collection and not remit amounts owed the company.

Borrowing Against Accounts Receivable

Infrequently, employees will use the company's accounts receivable as collateral for their own personal loans. This is similar to schemes in which employees use the company's investments for the same purpose. This scheme is described in more detail in another subsection of the present work.

BRIBERY AND CORRUPTION

When talking about bribery and corruption (e.g., illegal gratuity), we are talking about giving or receiving (or offering or soliciting) something of value in order to influence some official act. The illegal gratuity is basically giving or receiving (or offering or soliciting) something of value for performing some official act.

There is also the fraud scheme associated with kickbacks — giving or receiving anything of value to influence a business decision, without the employer's knowledge or consent. The scheme is also known as commercial bribery.

CONFLICTS OF INTEREST

Conflict of interest schemes are related, for example, to a corporate employee taking an interest in a transaction that can be or is adverse to the interest of the corporation or other entity. These conflicts of interest may result in fraud schemes associated with:

— Gifts, travel, and entertainment
— Cash payments
— Checks and other financial instruments
— Hidden interests
— Loans
— Payment of credit card bills
— Transfers at other than fair market value
— Promises of favorable treatment

PURCHASING — FOUR BASIC CATEGORIES

There are four basic categories concerning fraud schemes related to purchasing:

1. Fictitious invoices
2. Overbilling
3. Checks payable to employees, including duplicate payments
4. Conflicts of interest

Fictitious Invoices

Fictitious invoices are invoices that are not represented by a legitimate sale and purchase (e.g., a vendor that does not exist).

Overbilling

Overbilling is a fraud scheme concerning the submission of an artificially inflated bill that has been submitted to the corporation for payment, with the overpayment diverted or paid to one or more employees or accomplices.

Checks Payable to Employees, Including Duplicate Payments

Checks that are payable to employees (including duplicate payments) relate to employees creating payment to themselves by circumventing the control system, such that company payments are diverted to themselves or to companies they control. In addition, duplicate payments may be submitted, and as processes are not set up to catch duplicates, an employee overrides the system controls. Often the person with authority to override controls is a supervisor or manager, who is in a position to defraud the corporation.

Conflicts of Interest

Conflicts of interest can occur when an employee has an economic interest in a transaction that adversely affects the company. As is true of all of these fraud schemes, several may be used simultaneously to perpetrate the fraud.

INVENTORY

Most frauds perpetrated in inventory and warehousing seem to involve:

— Theft of goods
— Personal use of goods
— Charging embezzlements to inventory

Theft of Goods

This is simple theft that can be perpetrated by an employee who has access to that inventory worth stealing. Methods include hiding the item in their

clothing, placing it in garbage cans to recover later, and placing the items in other opened boxes that are being shipped out of the security enclosure. Computer software and hardware are some of the major theft items in today's modern businesses and government agencies.

Personal Use of Goods

An employee states that he or she is just going to "borrow" the item. A hand receipt is not used or tracked, and soon everyone forgets the item had been borrowed.

Charging Embezzlements to Inventory

Since inventory accounts are generally not reconciled until the end of each year, it is a simple matter to charge embezzlements to these accounts. Embezzlements are often concealed through the use of an expense or inventory account. This is because at the conclusion of each fiscal year, the expense accounts are closed to retained earnings (or fund balance).

Therefore, the audit trail becomes very obscure or even disappears at the conclusion of each year. Inventory accounts are often used as the concealment account for large embezzlements because the account balances are large enough to accommodate the entries required to conceal large losses.

INVESTMENTS AND FIXED ASSETS

Internal fraud schemes using investment assets are generally perpetrated by employees who are "borrowing" or using the asset for their personal benefit.

Investments

The three basic investment fraud schemes have to do with:

1. Use as collateral
2. Borrowing on earned interest
3. Avoidance of other losses or expenses

Use as Collateral

Using corporate assets as collateral relates to those assets used by employees who have the ability to "use" company investments without detection and can "borrow" the asset for their personal use.

Borrowing on Earned Interest

Borrowing on earned interest is a fraud scheme relating to corporations with cash on deposit. If controls are inadequate, an employee may have the ability to "borrow" the cash for personal use.

Avoidance of Other Losses or Expenses

Employees may have the ability to use company assets, in particular liquid assets, for unauthorized purposes such as to avoid other losses or expenses.

PAYROLL AND PERSONAL EXPENSES

The primary fraud schemes under payroll and personal expenses include:

— Ghost employees
— Overtime abuses
— Withholding tax schemes

Ghost Employees

Ghost employees are fictitious employees on the payroll employee list or in the payroll computerized database. Obviously, no services are received in exchange for payment to the nonexistent employee.

Overtime Abuses

Overtime abuses include such things as corporate employees charging and getting paid overtime when they did not perform the overtime work. Another type of overtime fraud scheme would be for employees to work overtime when no overtime work was required.

Withholding Tax Schemes

Withholding tax schemes include "borrowing" trust account taxes from a corporation until required for deposit. The person in the corporation that does the payroll "borrows" the money.

PROCUREMENT/CONTRACTS

One of the major and most lucrative areas for defrauders is in the procurement and contract areas.

In order to be able to bid on a contract, the bidder must be "responsible and responsive." This means that they provide a bid that addresses the contract specifications and not some they decided to make up and/or add. Furthermore, they must have the capability to actually do the work according to the contract's specifications.

There are various types of contracts, and although they all have some things in common, they also share some differences. Contracts can be fixed price, fixed price plus, cost plus, and the like.

These contracts can also cover anything and everything that a corporation wants to outsource to allegedly save money. The word "allegedly" is used here because sometimes the corporation ends up paying more for the services or products outsourced than if they did it "in-house".

Some fraud schemes include:

— Using cheaper materials than what the contract called for.
— Buying into a contract by providing a low bid and then coming up with ways to increase the contracts' costs and thus the defrauders' profits; for example, a painting contract in which the contractor proposes adding a sealer before painting, even though one may not be needed, nor is it in the original painting contract.
— Not meeting contract specifications; for example, a roofing job requiring asphalt with clean rock of certain sizes being added when dirty rocks are used in sizes including those out of specifications with the contract.

Many of the procurement and fraud schemes will include other fraud schemes; for example, a construction contract's corporate inspector may receive kickbacks to look the other way when specifications are not being met.

TELEMARKETING FRAUD

When you send money to people you do not know personally or give personal or financial information to unknown callers, you increase your chances of becoming a victim of telemarketing fraud.[12]

Warning signs: What a caller may tell you:

— "You must act 'now' or the offer won't be good."

[12] This scheme and subsequent schemes of this chapter are quoted from the FBI web site: http://www.fbi.gov/majcases/fraud/fraudschemes.htm.

— "You've won a 'free' gift, vacation, or prize." But you have to pay for "postage and handling" or other charges.
— "You must send money, give a credit card or bank account number, or have a check picked up by courier." You may hear this before you have had a chance to consider the offer carefully.
— "You don't need to check out the company with anyone." The callers say you do not need to speak to anyone, including your family, lawyer, accountant, local Better Business Bureau, or consumer protection agency.
— "You don't need any written information about their company or their references."
— "You can't afford to miss this 'high-profit, no-risk' offer."

ADVANCE FEE SCHEME

An advance fee scheme occurs when the victim pays money to someone in anticipation of receiving something of greater value, such as a loan, contract, investment, or gift, and then receives little or nothing in return.

The variety of advance fee schemes is limited only by the imagination of the con artists who offer them. They may involve the sale of products or services, the offering of investments, lottery winnings, "found money," or many other "opportunities." Clever con artists will offer to find financing arrangements for their clients who pay a "finder's fee" in advance. They require their clients to sign contracts in which they agree to pay the fee when they are introduced to the financing source. Victims often learn that they are ineligible for financing only after they have paid the "finder" according to the contract. Such agreements may be legal unless it can be shown that the "finder" never had the intention or the ability to provide financing for the victims.

COMMON HEALTH INSURANCE FRAUDS

Medical Equipment Fraud

Equipment manufacturers offer "free" products to individuals. Insurers are then charged for products that were not needed and/or may not have been delivered.

"Rolling Lab" Schemes

Unnecessary and sometimes fake tests are given to individuals at health clubs, retirement homes, or shopping malls and billed to insurance companies or Medicare.

Services Not Performed

Customers or providers bill insurers for services never rendered by changing bills or submitting fake ones.

Medicare Fraud

Medicare fraud can take the form of any health insurance frauds. Senior citizens are frequent targets of Medicare schemes, especially by medical equipment manufacturers who offer seniors free medical products in exchange for their Medicare numbers. Because a physician has to sign a form certifying that equipment or testing is needed before Medicare pays for it, con artists fake signatures or bribe corrupt doctors to sign the forms. Once a signature is in place, the manufacturers bill Medicare for merchandise or service that was not needed or was not ordered.

LETTER OF CREDIT FRAUD

Legitimate letters of credit are never sold or offered as investments. Legitimate letters of credit are issued by banks to ensure payment for goods shipped in connection with international trade. Payment on a letter of credit generally requires that the paying bank receive documentation certifying that the goods ordered have been shipped and are en route to their intended destination.

Letters of credit frauds are often attempted against banks by providing false documentation to show that goods were shipped when, in fact, no goods or inferior goods were shipped.

Other letter of credit frauds occur when con artists offer a "letter of credit" or "bank guarantee" as an investment wherein the investor is promised huge interest rates on the order of 100 to 300% annually. Such investment "opportunities" simply do not exist. (See Prime Bank Notes for additional information.)

PRIME BANK NOTES

International fraud artists have invented an investment scheme that offers extremely high yields in a relatively short period of time. In this scheme, they purport to have access to "bank guarantees" that they can buy at a discount and sell at a premium. By reselling the "bank guarantees" several times, they claim to be able to produce exceptional returns on investment. For example, if $10 million worth of "bank guarantees" can be sold at a

2% profit on ten separate occasions, or "traunches," the seller will receive a 20% profit. Such a scheme is often referred to as a "roll program."

To make their schemes more enticing, con artists often refer to the "guarantees" as being issued by the world's "Prime Banks," hence the term Prime Bank Guarantees. Other official sounding terms are also used such as Prime Bank Notes and Prime Bank Debentures. Legal documents associated with such schemes often require the victim to enter into nondisclosure and noncircumvention agreements, offer returns on investment in "a year and a day," and claim to use forms required by the International Chamber of Commerce (ICC). In fact, the ICC has issued a warning to all potential investors that no such investments exist.

The purpose of these frauds is generally to encourage the victim to send money to a foreign bank where it is eventually transferred to an offshore account that is in the con artist's control. From there, the victim's money is used for the perpetrator's personal expenses or is laundered in an effort to make it disappear.

While foreign banks use instruments called bank guarantees in the same manner that U.S. banks use letters of credit to insure payment for goods in international trade, such bank guarantees are never traded or sold on any kind of market.

THE PONZI SCHEME

A Ponzi scheme is essentially an investment fraud wherein the operator promises high financial returns or dividends that are not available through traditional investments. Instead of investing victims' funds, the operator pays "dividends" to initial investors using the principal amounts "invested" by subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends."

This type of scheme is named after Charles Ponzi of Boston, Massachusetts, who operated an extremely attractive investment scheme in which he guaranteed investors a 50% return on their investment in postal coupons. Although he was able to pay his initial investors, the scheme dissolved when he was unable to pay investors who entered the scheme later.

PYRAMID SCHEME

Pyramid schemes, also referred to as franchise fraud, or chain referral schemes, are marketing and investment frauds in which an individual is offered a distributorship or franchise to market a particular product. The real profit is earned not by the sale of the product, but by the sale of new

distributorships. Emphasis on selling franchises rather than the product eventually leads to a point where the supply of potential investors is exhausted and the pyramid collapses. At the heart of each pyramid scheme there is typically a representation that new participants can recoup their original investments by inducing two or more prospects to make the same investment. Promoters fail to tell prospective participants that this is mathematically impossible for everyone to do, since some participants drop out, while others recoup their original investments and then drop out.

CASE STUDY

If an employee came to you and stated that she had just received a strange e-mail advising her that she had the opportunity to receive millions of dollars and she thought it was too good to be true, what would you do?

Of course, depending on the contents of the e-mail, the corporate culture, and your anti-fraud program reporting requirements and follow-up actions, you might want to consider the following:

- Thank the employee for reporting the matter and advise the employee not to take any action and you will get back to her with more information.
- See if you can trace the e-mail to the sender.
- Do an Internet search for that and similar fraud schemes that may apply, and collect all pertinent information.
- Contact local, state, or federal law enforcement authorities who work on fraud matters and determine if they have heard of such e-mails being circulated.
- If so, obtain full details from them.
- As applicable,
  - Update the anti-fraud program database of fraud schemes.
  - Update the employee awareness briefing based on the collected information.
  - Send out an e-mail broadcast fraud alert so that all corporate employees are aware of this fraud scheme and what to do about it.
  - Update fraud scheme defenses and be sure that controls are in place to stop such e-mails (e.g., firewall, e-mail filters block e-mails from this address).
  - Update the fraud-reporting metrics management system to show this employee's reporting of the fraud scheme. (See Chapter 13) as an indication of the cost-benefits of an anti-fraud program awareness briefing policy.
  - Contact the employee and thank the employee for her conscientious efforts.

SUMMARY

Fraud schemes of one kind or another have been around since the first human tried to obtain the assets of another through fraudulent means. The days of the snake oil salesmen of the Wild West continue. However, today's fraud-threat agents are much more sophisticated, as are their fraud schemes. They are also more global, and the successfully perpetrated frauds often provide higher rewards than ever before, thanks to modern technology such as the cheap use of the Internet.

One must be ever-alert for new fraud schemes and learn the lessons of others who have fallen victim to the fraud schemes of old, as well as those of today. A database of fraud schemes should be part of any anti-fraud program.

One thing about fraud schemes, as the old adage states: "Where there is a will, there is a way"! It is often amazing how ingenious defrauders are at coming up with new fraud schemes.

One must also begin now to establish an aggressive and proactive anti-fraud program that will incorporate assets defenses and controls in order to protect the corporate assets from future fraud scheme attacks.

This page intentionally left blank

7

Fraud Cases and Analyses — Learning by Example

INTRODUCTION

This chapter presents actual fraud or fraud-related cases along with the author's commentary. Some of the cases presented are new, and others are a year or two old. However, don't let their dates of occurrence fool you, as many are still being tried today, albeit maybe with a little different "twist." The point is to understand the modus operandi, try to theorize the defrauders' rationales and profiles, and then learn from them.

Once you become familiar with the fraud schemes of Chapter 6 and read through the actual fraud cases discussed in this chapter, you should be in a better position to move on to Section II of this book, which discusses the establishment and management of a corporate anti-fraud program, based on the fraud-threat agents' mindsets and attack schemes.

Many of the cases cited are related to our use of high technology. That is understandable as today's and definitely tomorrow's high-technology environment provides the ability to perpetrate old fraud schemes in a new environment with new tools and to perpetrate new fraud schemes in this our modern information-driven and information-dependent world supported by the microprocessor-based high technology.

ACTUAL FRAUD AND FRAUD-RELATED CASES

The cases provided are in no particular order of importance and are used to provide a general awareness of the "talent" of various defrauders and/or some of their modus operandi.

It is important to remember that we know of these fraud cases because they were not successful in that someone found out about them. As Honore de Balzac so correctly stated: *The secret of a great success for which you are at a loss to account is a crime that has never been found out, because it was properly executed.*

One never knows how many successful frauds are committed around the world on a daily basis. The scary part is, of course, the fact that since they are successful, we do not know about them. Compounding this fact is the fact that most corporations and other entities have little or no formal anti-fraud program, one that is proactive and not just reactive.

PHISHERS AND TAXPAYERS

The following is an example of a fraud scheme showing another use of e-mail, Web sites, and technology to perpetrate a fraud where none was possible only a few years back.

> **A British Internet-security firm is warning people to not get hooked by an e-mail scam promising tax refunds from the U.S. Internal Revenue Service.** The e-mails, known as a "phishing" scam in technology speak, exploit a loophole allegedly built into the real IRS Web site, according to the firm, but instead of getting money back from the government, those biting on the scam could be giving away the contents of their bank accounts. . . . Phishing scams have been around for years and their success usually hinges on the perceived legitimacy of the e-mails, which often include official logos and language. Typically, they ask for personal information like Social Security or bank account numbers. Making the scam even more effective is that the address appears legitimate — an extension of the www.govbenefits.gov site — but the site is bogus.
>
> It appears real because the phishers have found a flaw in the design of the IRS Web site, one that allows them to "bounce" people to the fake site, according to Sophos, a company that tracks malicious Internet programs. . . . The IRS is contesting this claim, saying its site is completely secure. "Any Web vulnerabilities exploited by this scam are not caused by the IRS site," said an e-mail from an IRS representative, who added that no changes have been made to the site as a result of this scam. In a written statement, the IRS reminded taxpayers that it doesn't send unsolicited e-mails, it will never ask for personal or financial information via e-mail and there is no special form to obtain tax refunds.[1]

[1] http://edition.cnn.com/2005/TECH/internet/11/30/phishing.irs/index.html.

Commentary: A typical government or corporate response is to say their site is "completely secure." This is impossible! No Web site and nothing on the Internet can be guaranteed to be safe. Why is that? It is because there are inherent vulnerabilities in high-technology hardware and software. After all, that should be expected since they were developed by human beings and human beings are far from perfect. Should we expect otherwise from man-made things?

A good point to remember is that most corporations or government agencies will never ask for personal information over the Internet. If you find one that does and it is a legitimate site, stay away from that business because they may not adequately protect vital information such as your credit card or social security number. Of course, this does not include businesses operating in a secure mode asking for your credit card information for some purchase you are making. However, even in those instances, be sure you are shopping on a legitimate site that uses encryption (e.g., see the little yellow lock on the Web site page when you are about to do business on line).

Unfortunately, even in those cases where the information seems to be secure, you have no guarantees, as some hackers have in the past broken into shopping Web sites and set up false home Web sites that collect your information and then may ask you to log in again as your information was incorrectly entered. You may think it is a typo when it is not. The second login will then take you to do the legitimate Web site.

FRAUD BY CORPORATE EXECUTIVES

> **Adelphia founder sentenced to 15 years**[2] NEW YORK (CNN/Money) — The founder of Adelphia Communications was sentenced Monday to 15 years in prison . . . for his role in a multibillion-dollar fraud that led to the collapse of the nation's fifth-largest cable company . . . deals the father and son were convicted of helped drive Adelphia into bankruptcy. . . . The sentencing comes as prosecutors have achieved some big wins in their fight against corporate corruption. Three days ago a New York state jury convicted former Tyco CEO Dennis Kozlowski and CFO Mark Swartz on charges that they looted the manufacturing conglomerate of $600 million.
>
> In March, a federal jury in New York found former WorldCom CEO and co-founder Bernard Ebbers guilty on charges related to an $11 billion accounting scandal at the telecommunications giant, now known as MCI. WorldCom filed the largest bankruptcy in U.S. history just a

[2] http://money.cnn.com/2005/06/20/news/newsmakers/rigas_sentencing/index.htm?cnn=yes

> month after Adelphia went bankrupt. . . . conspiring to hide $2.3 billion in Adelphia debt, stealing $100 million, and lying to investors about the company's financial condition.[3]

Commentary: In the United States and other "modern" nation-states, we have seen the rise of massive amounts of frauds perpetrated by corporate executives. It seems to be a combination of quests for more power, selfish greed, and little regard for the impact of their massive frauds on the stockholders and employees, many of whom have lost all their savings, retirement opportunities, and such.

Some of the frauds are made possible because there are times when not only collusion occurs, thereby negating many controls in place based on separation of functions, but also perhaps due to more and more complicated regulations. Furthermore, new fraud-related laws make new fraud crimes possible. As legislatures such as the U.S. Congress seem to be more and more involved in micro-legislating, the laws seem to become more complicated and full of ambiguities.

Such types of frauds by corporate executive management are very difficult to deter and detect. After all, when you have the combination to the corporate assets safe, how can an accountant, auditor, chief security officer (CSO), or others identify such frauds and take action to stop them? Who wants to be the first to accuse a CEO or other member of the corporate executive management team of being defrauders?

If you do so, you do so at your personal and professional peril. For even if you are right, as some whistleblowers have found out, you will eventually be not only out of work but maybe even sued by these powerful defrauders. After all, they have massive amounts of funds to use for their lawyers. Do you? Even if they don't have a chance to win, they will make you pay a financial price as well as add massive amounts of stress to your life and the lives of your loved ones.

As for new employment, good luck! Other managers will not hire you just because you are a very honest and brave person. No, they will not hire you because they are concerned that you may again blow the whistle based on some of their actions, even if they can be legitimately explained. Here

---

[3] All individuals listed in this chapter were listed as they appeared in the footnoted and edited article. However, the readers must understand that this does not imply that they have been finally found guilty as there are appeals that take place and the persons cited may actual by subsequently be found not guilty. The information provided in this chapter is for education purposes only so that the CSO or other individual who wants to build a anti-fraud program can learn for these cases and ensure that their anti-fraud program incorporates "lessons-learned" from these cases in the form of controls and other defensive measures as well as proactive measures.

in the United States, we compound the reporting dilemma as we are often brought up being told "Don't be a fink!" "Don't be a tattletale!"

So, you may be right, but you will pay a price. If you have bills and family, and want your current career and profession to continue and not have to move to a deserted island and eat raw fish and drink coconut milk the rest of your life, you must really think about your actions. That is a very sad thing to have to state, but that is life in today's environment — and maybe always was and will be.

FOREIGN EXCHANGE TRADING FRAUD

> **Allied probes $750 million fraud . . .** LONDON, England (CNN) — Allied Irish Banks has suspended nearly all foreign exchange trading and has opened an investigation into a suspected fraud totalling an estimated $750 million at a U.S. subsidiary, . . . an American in his 40s who had worked at the bank for seven years. "Allied Irish Banks, p.l.c. is undertaking a full investigation into foreign exchange trading operations at the Baltimore headquarters of its U.S. subsidiary Allfirst," a news release from AIB said on Wednesday. "This decision follows the uncovering by Allfirst management of suspected fraudulent activities by one trader who has since failed to report for work."
>
> The married father has been a "respected member of his local commun ity,". . . . "He has never given anybody any reason to believe from his performance and his job until now that he was an unusual individual in any way." Indications of suspected fraudulent activity in the foreign exchange trading area at Allfirst were discovered during a management review within the treasury division of the subsidiary, . . . the losses arose on a series of unauthorised transactions in a number of foreign currency contracts. . . . the alleged fraud as "complex," where the trader required varying amounts of cash for different reasons at different times of the year. Alarm bells sounded over sums. . . . Ultimately, it was the increase in the amount of cash that he was requiring that set off the alarm bells.[4]

Commentary: Such scams have been around for some time. One of the common, yet unexpected, aspects of such frauds is identifying who the fraud-threat agents are. For example, in this case it was a "married father and a respected member of the community." This points out that anyone can be a defrauder, even those who appear to be good workers. A potential fraud indicator is a person who seems to always be working late, on weekends and doesn't take vacations. In one such case, the "sweet, little old

[4] CNN televised story — 2002.

lady" who worked for a small company doing their accounting functions and of course with no separation of functions defrauded the company out of more than $1,000,000 over 30 years!

As an anti-fraud leader, beware of good workers! Maybe a sad thing to say but history has shown that many defrauders appear to be the hardest workers, coming in early, staying late, and so forth.

KATRINA WASTE AND FRAUDS

Auditors: Katrina waste could top $2 billion: Story Highlights

- Waste after Hurricane Katrina could top $2 billion, government auditors say;
- Wasteful spending already has been tabbed at $1 billion
- $500,000 worth of contracts have been awarded without little or no competition; . . . Federal investigators have already determined the Bush administration squandered $1 billion on fraudulent disaster aid to individuals after the 2005 storm. Now they are shifting their attention to the multimillion dollar contracts to politically connected firms that critics have long said are a prime area for abuse.[5]

Commentary: When anti-fraud defenses are circumvented in the name of getting aid to victims quickly, the chances for frauds naturally go up. It is a "Catch-22" for the government agencies: either respond slowly and be sure controls are in place to minimize fraud or get aid quickly to victims and worry about the potential for fraud later. It is difficult to go out for bids on contracts using generally accepted processes, including anti-fraud defenses, which are inherently slow while people are in need of immediate help.

ORGANIZED CRIME AND CYBERCRIME

> **Cybercrime More Widespread, Skillful, Dangerous Than Ever** eWeek.com . . . malware hunters infiltrate black hat hacker forums, chat rooms and newsgroups, posing as online criminals to gather intelligence on the dramatic rise in rootkits, Trojans and botnets. . . . well-organized mobsters have taken control of a global billion-dollar crime network powered by skillful hackers and money mules targeting known software security weaknesses. . . . "There's a well-developed criminal underground market that's connected to the mafia in Russia and Web gangs and loosely affiliated mob groups around the world. They're all involved

[5] http://www.cnn.com/2006/US/12/26/katrina.waste.ap/index.html

> in this explosion of phishing and online crime activity,". . . . Just two years after the Secret Service claimed a major success with "Operation Firewall," an undercover investigation that led to the arrest of 28 suspects accused of identity theft, computer fraud, credit card fraud and money laundering, security researchers say the mobsters are back, with a level of sophistication and brazenness that is "frightening and surreal." . . . A law enforcement official familiar with several ongoing investigations showed eWEEK screenshots of active Web sites hawking credit card numbers, Social Security numbers.[6]

Commentary: Although still slow to react and especially now when, at least in the United States and some other nation-states, law enforcement and intelligence resources are directed primarily at antiterrorist activities, some investigative agencies are trying to stem the tide of frauds perpetrated internationally and nationally by these miscreants.

SECURITIES FRAUD IN CYBERSPACE

> **L.A. pair charged over cyberfraud . . .** The FBI charges that two L.A. men artificially inflated stock price by posting false information on Internet bulletin boards. . . . Two men have been charged in federal court here with conspiracy to commit securities fraud for allegedly artificially inflating a company's stock price by posting false information about the firm in Internet bulletin boards.[7]

Commentary: The Internet has become a great and cheap tool through which rumors and other modus operandi can lead to frauds that were nonexistent a few years ago or that reflect the ability to do so on a grander scale.

COMPUTER HARD DRIVES LEAD TO FRAUDS

> **Dead disks yield live information . . .** Identity thieves are gleaning personal information from scrapped computers. A hard drive from a personal computer that a man had thought he had disposed of properly yielded highly personal letters relating to his financial affairs including details of bank accounts and insurance claims. All of which is potential gold dust for the UK's fastest growing crime trend, identity theft. As the university's forensic team conducted the research, it peeled back the layers on the disk. Web searches, phone numbers of employees, email

---

[6] http://www.foxnews.com/story/0,2933,191375,00.html
[7] ZDNet News, December 15, 1999

> conversations with family friends and details of their daughter's boyfriends — all spilled onto the university computers. There was enough data for a would-be identity thief to garner more information by ringing up those people identified and "socially engineer" more relevant details. . . . "Impersonation and bribery are used to get inside information ranging from car registration details to bank records." Being careless with personal information also breaks the Data Protection Act, . . . a point forcibly made by a spokeswoman for the Information Commissioner. The company, which has a worldwide workforce of 58,000 and sales of €14.7 bn, had again disposed of hard drives from computers that contained highly detailed company information including personal details on staff payroll, internal contact details, internal planning and strategy documents, written warnings to staff plus copies of invoices and orders.[8]

Commentary: It is amazing how many people and those in responsible positions in corporations allow their computer systems to be disposed of without wiping out the data of their hard drives. This is especially important these days where the hard drives are so massive and can literally hold all the information of a corporation on one drive.

Not that many years ago, miscreants were involved in "dumpster diving" to gather corporate information. By that, I mean literally go into the trash containers outside corporations looking through the garbage for information that can help them commit identity frauds and break into computers. Now, they just have to buy or otherwise obtain the old computers of corporations and get more information than they ever could have from the dumpsters.

DEBT-COLLECTING FRAUDS

> **Debt "counselors" hit for $100 M scam: FTC settles with agencies that promised consumers free debt counseling, but took their money anyway . . .** Regulators announced settlements Wednesday with three debt-counseling agencies that they said had bilked consumers out of more than $100 million, a scam they said was becoming increasingly common. The three companies promised to help consumers manage their debts but in fact only made their problems worse, the Federal Trade Commission said. Clients paid thousands of dollars to keep bill collectors at bay, but instead saw their debts, interest rates and late fees increase as the companies did little to help, . . . Some consumers were forced to declare bankruptcy when the companies told them to stop paying their

[8] http://technology.guardian.co.uk/weekly/story/0,,1840396,00.html

> bills but then didn't negotiate on their behalf, . . . "All three companies lied about who they were, what they could do for consumers and how much they charged,". . . . The companies agreed to give back a total of more than $25 million to consumers, and two are in the process of being shut down. None of the owners face jail time as the FTC does not have criminal authority.[9]

Commentary: As modern-day consumers continue to buy, buy, buy and charge, charge, charge their goods to their multiple credit cards, some reach a point of financial crisis. One cannot expect them to be able to get out of their debts by themselves. After all, they didn't have enough sense to use financial planning; therefore, they often have little chance of knowing how to get out of debt.

These consumers are ripe for the defrauders who take advantage of their "stupidity" and their financial naiveté. Remember that these people are also desparate and are also corporate employees who may have access to valuable corporate assets.

GOVERNMENT CONTRACTING FRAUD

> **Defense contractor . . . paid $1 million in bribes . . .** A defense contractor admitted Friday that he paid a California congressman more than $1 million in bribes in exchange for millions more in government contracts. Mitchell Wade pleaded guilty in U.S. District Court to conspiring with former Rep. to bribe the lawmaker with cash, cars and antiques, and to help him evade millions of dollars in tax liability. . . . entering his plea to charges that carry a maximum prison sentence of 20 years. . . . quit Congress last year after he pleaded guilty to taking bribes from Wade and others. Wade, former president of defense contractor. . . . in Washington, also acknowledged making nearly $80,000 in illegal campaign contributions in the names of . . . employees and their spouses to two other members of Congress, who were not identified. The lawmakers apparently were unaware the donations were illegal, according to court papers. Prosecutors also laid out a second, separate conspiracy in which Wade was alleged to have paid bribes to a Defense Department official and other employees in return for their help in awarding contracts to his company. . . . pleaded guilty to this scheme as well. The Pentagon employees were not named in court filings.[10]

Commentary: This is an old fraud and has been around for many decades. Many defrauders take advantage of government agencies due to the massive

---

[9] CNN Money, 30 March 2005; also see http://www.ftc.gov

[10] http://www.usatoday.com/news/states/2006–02–24-contractor_x.htm

amount of contracts and money that is available. Often the oversight for such contracts is handled by government employees whose salaries pale in comparison to the money being made by contractors and the money available for bribing these government employees.

In addition, many of these government employees may be overseeing numerous contracts and cannot be everywhere at once. Their lack of experience and training in how to properly do their job and how to look for fraud indicators adds to the lure of this lucrative fraud area. By the way, this also applies to other corporate employees who oversee other types of corporations and their contracts.

FRAUD-THREAT AGENTS CAN BE ANYONE IN ANY POSITION

> **Dish washer "raids USA's richest":** A trainee waiter and dish washer has been arrested for swindling millions of dollars after "cloning" the identities of 200 of America's richest people. . . . spent his spare time surfing the internet, . . . allegedly defrauding millions of dollars from some of the most protected and high-powered figures in the US. . . . described him as supremely talented at obtaining the credit card details and stockbroker accounts . . . operated a complex series of PO boxes, untraceable mobile phones and virtual voicemail services to clone the identities of 200 celebrities he picked from the Forbes magazine list of the "Richest people in America. . . ."
>
> When he was eventually arrested, police found lists of home addresses, National Insurance numbers, telephone and brokerage account details and bank balances for his famous victims scrawled beside their entries in the magazine's list. He even knew the bank account passwords and mother's maiden names of some of the tycoons he targeted and had fake corporate papers, writing paper and stamps from respected financial firms. . . . The alarm was raised because the transfer would have put . . . account into debt. . . . Detectives investigated and found that more than 29 post office boxes had been taken out in the name of tycoons and rich stars in New York into which cash and cheques were delivered. . . . employed prostitutes and cab drivers to collect the fraudulent packages that were often sent to non-existent addresses.[11]

Commentary: The ingenuity of these miscreants is truly amazing at times, and one must admire their innovative approaches to committing frauds. Sometimes one wonders what such defrauders could accomplish if they

[11] http://www.thisislondon.com/dynamic/news/story.html?in_review_id=372288&in_review_text_id=318092

would set their minds to honest pursuits! Never underestimate the potential for some employees or others to commit fraudulent acts based on their positions or perceived level of intelligence.

Identity theft: Usually, a scam involves the theft and use of someone's credit card information. In more serious cases, a victim's entire identity is absconded with, and the criminal gets new credit cards and loans in the victim's name. Obviously, this can be a nightmare for the unwitting person who must deal with credit issuers and reporting agencies. . . . victims find themselves "in the position of having to prove they didn't do something."[12] *(The credit card may be a corporate or government agency credit card!)*

U.S SECURITIES AND EXCHANGE COMMISSION (SEC) FIGHTING FRAUD

SEC Conducts "Pump-And-Dump" Net Stock-Fraud Sweep . . . The Securities and Exchange Commission (SEC) today took action against 33 companies and individuals accused of engaging in "pump-and-dump" microcap stock schemes that brought in illegal profits of more than $10 million. The SEC brought the actions after conducting its fourth nationwide Internet fraud sweep, in which it searched the Internet for misleading and illegal messages on Web sites, electronic newsletters and Internet message boards touting more than 70 thinly traded microcap stocks. Pump-and-dump operators typically use such venues to generate enthusiasm for a particular small stock, which artificially inflates the shares' value. Once the stock has reached a certain valuation, the fraudsters sell off or "dump" their shares for a profit, leaving bamboozled investors holding essentially worthless stock.

The SEC said the perpetrators of the schemes targeted in its sweep pumped up the total market capitalization of their stocks by more than $1.7 billion before unloading them on the market. The commission said many of the fraud perpetrators appeared to have no securities industry experience whatsoever: one was a bus mechanic, while another turned out to be a student moonlighting as a chauffeur. Other parties implicated in the stock scam included foreign-based individuals and entities that used the Internet to reach US investors, the SEC said.[13]

---

[12] http://www.usatoday.com/tech/2001–08–03-net-dangers.htm

[13] http://findarticles.com/p/articles/mi_m0NEW/is_2000_Sept_6/ai_65024697, Newsbytes News Network, 6 September 2000.

> SEC . . . action brings the total number of Internet fraud cases filed by the SEC to 180. The commission conducted previous sweeps . . . which dealt with the fraudulent touting of publicly traded companies through the Internet. . . . the SEC conducted a sweep to uncover sales of bogus securities over the Internet.[14]

Commentary: Government agencies such as the SEC are overworked, understaffed, and overwhelmed by the job they have to do when it comes to deterring and investigating potential frauds. Sadly, the matter can probably only get worse as legislative bodies seem to make more detailed and more complicated laws as frauds are discovered. The government agencies don't help as they spew out regulations by the hundreds. Add to that the ability of international fraud-threat agents to attack corporate assets anywhere in the world from anywhere in the world.

FRAUD IN SCHOOL SYSTEMS

> **Eleven indicted in school corruption probe . . .** Eleven people, including teachers and school secretaries, were indicted Thursday on fraud and theft charges in a continuing FBI probe of corruption in the city's school system. Those indicted included three employees of the school system's credit union, accused of stealing nearly $150,000 by withdrawing money from accounts of customers who were dead or had moved. Two insurance brokers were also accused of paying kickbacks to a school system administrator in return for contracts.
>
> More than a dozen people have pleaded guilty, or agreed to do so, to charges of fraud and bribery in various schemes that have bled millions from the city's school system, considered one of the country's worst. Twenty-four people have been indicted this year . . . indictments came days after schools Superintendent Anthony Amato announced that the system faces a multimillion dollar deficit — and blamed the deficit partly on years of theft by its workers.[15]

Commentary: If you name a business or public entity or even a job description, you will no doubt be able to find someone somewhere in one of these entities (e.g., schools) perpetrating a fraud. After all, where there are valuable assets that someone wants or wants to convert into cash, there will be

---

[14] Ibid; also see http://www.sec.gov

[15] http://www.cnn.com/2004/EDUCATION/12/17/schools.corruption.ap/index.html

a way to do it. As many rationalize; "I am not stealing from anyone, just a corporation, just a public entity. Besides, they are insured." As in the case just cited, frauds can have a devastating effect on an entity's budget. Frauds may also be perpetrated for other than financial gain, even for altruistic reasons. (e.g. The "Robin Hood" rationale.)

DEAD SOLDIERS AND E-MAIL SCAMS

> **U.S. warns of online schemes that make reference to Iraq:** WASHINGTON (AP) — Federal authorities are investigating two e-mail scams, including one targeting families of troops killed in Iraq, that claim to be connected to the Homeland Security Department. The scams "are among the worst we have ever encountered," Michael J. Garcia, director of the department's Immigration and Customs Enforcement bureau, said Friday. Both of the online pleas for help — and money — link themselves to the bureau. In one scheme, e-mail sent to families of U.S. soldiers killed in Iraq includes a link to the bureau's Web site. The e-mail seeks to recover money from a friend of the slain soldier.
>
> In the other, the e-mail identifies itself as being sent by a federal agent trying to track down funds looted from the Iraqi Central Bank by one of Saddam Hussein's sons. The e-mail also links to the bureau Web site and asks for confirmation of the recipient's address by urging, "There is a very important and confidential matter which I want us both to discuss."
>
> . . . The bogus e-mails resemble the so-called "Nigerian letter." In that persistent scam, victims are told they will receive money, often from the "Government of Nigeria," after paying a fee often characterized as a bribe to that government.[16]

Commentary: All fraud-threat agents are bad; however, it seems that many sink to the bottom of the food chain. These slime bags and scum of the earth who take advantage of the families and friends of fallen soldiers should be sentenced to long prison terms, or worse sentences which I won't mention here (*Hint:* Sometimes torture is a good thing!). Their types of frauds are the most despicable of frauds.

ANOTHER EXAMPLE OF INSIDER FRAUD

> **Emulex Fraud Suspect Was Former Internet Wire Employee** The FBI said today that the Los Angeles man arrested for posting a bogus press

[16] http://www.goldstarwives.org/iraq-email-scam.htm, Associated Press 18 February 2005.

> release that sent shares of Emulex Corp. stock plummeting last Friday was a former employee of the Internet wire service that distributed the fraudulent information. . . . charged him with securities and mail fraud for earning more than $225,000 in short trades after sending the bogus release via e-mail to Internet Wire, his former employer. . . . investigators were able to trace the release back . . . because the e-mail included language that suggested the author had a familiarity with the procedures used at Internet Wire, and that the message represented that the company's sales department had already reviewed and approved the release. . . .
>
> The FBI said a recording of . . . stock trading records indicate that he executed a series of short sales of 3,000 shares of Emulex stock at prices between $72 and $92 per share. During the following week, Emulex's stock prices rose to more than $100 per share. After issuing the bogus release Friday morning, the bureau said . . . executed trades to cover earlier short sales losses by buying 3,000 shares of Emulex, yielding a profit of more than $50,000. Later in the day, . . . purchased an additional 3,500 Emulex shares on a margin account at $52 per share, for a total expenditure of $180,000. Three days later, he sold those shares for a profit of $186,000.[17]

Commentary: Stock-related frauds are not only common but often cause major problems for the targeted corporations. Sometimes such frauds cause the corporation or other entity to declare bankruptcy. This type of fraud scheme has happened so often that the SEC and others have been able to more rapidly identify these frauds and are in a better position to take action faster than before, often aided by computer monitoring programs that would identify some of these types of potential fraud indicators.

The computer can be used as a weapon by defrauders, but it can also be used by investigators and others who fight fraud. Unfortunately, it seems the fraud fighters don't seem to take advantage of these high-technology tools as much as the defrauders do.

EXECUTIVE MANAGEMENT AND ACCOUNTING FRAUD

> **Enron's whistle blower details sinking ship: . . .** Enron's most prominent whistle blower Sherron Watkins . . . described a company that increasingly became mired in accounting fraud in 2001, prompting her to send an anonymous letter to Enron founder Kenneth Lay in August warning him that the company "had a hole in the ship and we're going to sink."

[17] Newsbytes News Network, 31 August 2000.

> Watkins, a former vice president at Enron, testified that in mid-2001 she began investigating Enron's relationship with LJM (a special purpose entity designed to take high-risk poor-performing assets off Enron's balance sheet) and was increasingly alarmed as it became apparent that the relationship didn't stand up to accounting scrutiny. . . .
>
> She went on to predict that Enron "will implode in a wave of accounting scandals."[18]

Commentary: It is interesting to note that no matter what the government, auditing, or accounting oversight, some frauds go undetected unless a whistleblower, usually from the inside of the corporation or entity, steps forward. That takes real courage as the life of the whistleblower will change drastically and generally not for the good, when the first alarm of a potential fraud is sounded.

MERCHANDISE RECEIPT AND EXCHANGE FRAUD

> **Ex-White House aide admits to fraud . . .** A former top White House aide who was arrested on a theft charge admitted to a store investigator he fraudulently returned merchandise that he didn't buy, according to charging documents . . . a former domestic policy adviser to President Bush, made fraudulent returns worth at least $5,000 at Target and other stores in the Washington suburbs on 25 different occasions. . . . he stopped . . . outside the company's Gaithersburg store after . . . allegedly received a refund for items using a receipt from an earlier purchase. . . . had receipts from previous purchases at Target stores and admitted to . . . that he was committing fraudulent returns," . . . According to authorities, . . . would buy items and take them to his car, then return to the store, pick up identical items from store shelves and take them to the return desk, presenting his original receipt.[19]

Commentary: Not so surprisingly, anyone in any position at work or in life is susceptible to perpetrating frauds if the circumstances are right. However, it is still surprising to learn of the fraud-threat agent's profile, and one wonders why on earth someone would perpetrate such a fraud. This is especially true for those whose monetary reward is so small.

A scarier thought is what national security secrets does this person know, and if he is so desperate to perpetrate a $5,000 fraud, what would he do for $10,000 or more in bribes?

If your corporation is involved in retail merchandising or even if your corporation has a company store for employees, such a fraud scheme must be considered when developing an anti-fraud program.

---

[18] http://money.cnn.com/2006/03/15/news/newsmakers/enron/index.htm

[19] CNN, 14 March 2006.

CLICK FRAUDS

> **FBI, SEC Probe Web Sites Offering Large Returns Looking at Ads . . .** Federal investigators are examining Web sites . . . autosurf pages that promise to pay members simply for viewing advertisements. The FBI and SEC are taking a closer look at these sites that bear a similarity to the famous Ponzi scheme, where investors are lured in by promises of lavish returns, but are paid with the money from future investors, rather than money earned from a legitimate business activity. . . . offers free membership, but only pays users who have upgraded, investing in $6 increments, with a maximum of $6,000. . . . the FBI has elevated Internet crime to its third-highest priority. . . . In 2004, the FBI's Internet Crimes Complaint Center fielded 207,000 complaints, up 66 percent from the year before, though most were not related to investment scams. Still, the agency notes that many people who are conned out of small sums would be unlikely to report the crime.[20]

Commentary: This is another example of the use of today's Internet and high-technology devices as tools to perpetrate old fraud schemes. Fraud-threat agents will use the tool available and the opportunity presented to attack assets. When developing an anti-fraud program, be sure to include these "oldies but goodies" fraud schemes and project them into the future, incorporating the future technology that will be common and available to them.

MORTGAGE FRAUD

> **FBI warns of mortgage fraud "epidemic" . . .** Seeks to head off "next S&L crisis": Rampant fraud in the mortgage industry has increased so sharply that the FBI warned . . . of an "epidemic" of financial crimes which, if not curtailed, could become "the next S&L crisis." . . . Assistant FBI Director . . . said the booming mortgage market, fueled by low interest rates and soaring home values, has attracted unscrupulous professionals and criminal groups whose fraudulent activities could cause multibillion-dollar losses to financial institutions.
>
> . . . In one operation, six individuals were arrested Thursday in Charlotte, charged with bank fraud for their roles in a multimillion-dollar mortgage fraud, officials said. The two-year investigation found fraudulent loans that exposed financial institutions and mortgage companies to $130 million in potential losses, . . . some organized ethnic groups are becoming involved in mortgage fraud schemes, but he declined to identify the groups.

[20] http://online.wsj.com/article/SB113953819846670333.html

> Officials said mortgage fraud is one prominent aspect of a wider problem of fraud aimed at financial institutions. The FBI said action has been taken against 205 individuals in the past month in what it described as the "largest nationwide enforcement operation in FBI history directed at organized groups and individuals engaged in financial institution fraud."
>
> In addition to mortgage fraud, "Operation Continued Action" also targeted loan fraud, check kiting, and identity theft as major problems. In one check-kiting scheme in Binghamton, New York, the operator of a recycling business wrote in excess of $1 billion in worthless checks over a 14-month period, officials said. Not all of the checks were cashed.[21]

Commentary: This is yet another example of innovative fraud-threat agents operating in any environment where they can attack and gain control of some form of corporate or other entity's assets. It is also another illustration of an old fraud scheme that must be considered when developing an anti-fraud program. If you don't think it applies to your corporation, please be sure before you ignore this or any other fraud scheme. You may be surprised by the kinds of activities your corporation or its subsidiary may be involved in.

GOVERNMENT CONTRACTORS AND FRAUD

> **Former Air Force buyer jailed over Boeing deal: . . .** The U.S. Air Force's former No. 2 weapons buyer was sentenced to nine months in prison on Friday after telling the court she had given Boeing Co. a rival's secret data and inflated weapons deals to ingratiate herself with the company, her future employer. The disclosure . . . could spark a new round of ethical, legal and business headaches for the Chicago-based aerospace giant, the Pentagon's No. 2 supplier after Lockheed Martin Corp . . . she had agreed to a higher price than she thought was appropriate for what became a $23.5 billion plan to acquire modified Boeing 767 aircraft as refueling tankers. "The defendant did so, in her view, as a 'parting gift to Boeing' and because of her desire to ingratiate herself with Boeing, her future employer," according to a statement of facts she signed.[22]

Commentary: This is another example of an old type of contract fraud. There are literally thousands of such types of frauds perpetrated for many, many decades. If your corporation has any type of contracts with businesses

---

[21] http://www.cnn.com/2004/LAW/09/17/mortgage.fraud/index.html

[22] Reuters, 02 October 2004.

or government agencies, and obviously it does, one must definitely consider such fraud schemes in an anti-fraud program.

One SEC commissioner reckons that Internet fraudsters are scamming more than $1 billion (#600 million) a year from investors worldwide. "These people," he says, "want your money and they recognise that the Internet provides them with anonymity. With the press of a button, they can get bogus information out to millions of people 24 hours a day." Because the Internet reaches all of us, and is essentially an unregulated marketplace, these warnings should also be taken seriously in Britain.[23]

FRAUDS AND MICROSOFT SOFTWARE

> **Fraudster Snares Microsoft Certificates; Users Warned . . .** Software titan Microsoft Corp. [NASDAQ:MSFT] today warned that two of its digital certificates were erroneously issued to an imposter seeking to trick users of Microsoft products into running harmful programs. . . . The certificates could be used to sign executable content under the Microsoft name, enabling the attacker to "create a destructive program or ActiveX control, then sign it using either certificate and host it on a Web site or distribute it to other Web sites," Verisign said.[24]

Commentary: Here again we have innovative miscreants using today's high-technology tools to help perpetrate some unauthorized activities. Such types of actions can easily be used to support some fraud schemes.

Y2K-RELATED FRAUD

> **FTC Nabs Mining Co Pitching Y2K-related Fraud: . . .** The Federal Trade Commission secured court backing to stop a California businessman from using year 2000-related fears to con investors into buying stocks and options in his mining company. . . . agreed to stop marketing investments in the gold mining company as an option ahead of a financial breakdown related to the change in the millennium.[25]

---

[23] 16 August 1999, infowar.com.

[24] Newsbytes News Network, 22 March 2001. Also see http://www.microsoft.com/technet/security/bulletin/MS01–017.asp

[25] Dow Jones News Service, 17 November 1999.

Commentary: Although the Y2K crisis is well behind us, the fraud scheme used here is still valid — using fear tactics to manipulate the thinking of potential fraud victims to act in a certain way conductive to the fraud-threat agent being successful.

Fear, and especially financial fears, is a strong motivator that often drives the intended fraud victims to take actions conducive to perpetrating a successful fraud. These defrauders know that and use human nature to their advantage. That is why as a fraud fighter developing an anti-fraud program, you, too, must understand human nature and the thinking and fear processes of victims, as well as the defrauders.

If a fraud-threat agent used fraud scheme tactics but the targeted victims did not act to help the fraud to succeed, then the "good guys" win. The potential fraud then is not successful. That is why it is imperative that any anti-fraud program include an employee awareness program so that potential victims or fraud targets do not facilitate the fraud attacks.

DATA STORAGE CONDUCIVE TO FRAUD-THREAT AGENTS

> **Google's long memory stirs privacy concerns: . . .** When Google Inc.'s 19 million daily users look up a long-lost classmate, send e-mail or bounce around the Web more quickly with its new Web Accelerator, records of that activity don't go away. In an era of increased government surveillance, privacy watchdogs worry that Google's vast archive of Internet activity could prove a tempting target for abuse. Like many other online businesses, Google tracks how its search engine and other services are used and who uses them. Unlike many other businesses, Google holds onto that information for years. Some privacy experts who otherwise give Google high marks say the company's records could become a handy data bank for government investigators who rely on business records to circumvent Watergate-era laws that limit their own ability to track U.S. residents.[26]

Commentary: As corporations and government agencies continue to compile information on employees, consumers, and the like, owing in part to more powerful and cheaper high technology, we are all more vulnerable to fraud-threat agents obtaining that information and using it to perpetrate one or more frauds.

Is it too late to protect private information, or is the genie out of the bottle and can't be put back in? One corporate executive once said, "There is no privacy. Get over it!" I tend to agree with that statement. However, we can still put controls and anti-fraud processes in place that will help protect the privacy of employees and corporate sensitive information as best we can.

---

[26] Reuters, 3 June 2005.

ANOTHER EXAMPLE OF CLICK FRAUD

> **Google settles "click fraud" case: . . .** Google Inc. has agreed to pay up to $90 million to settle a lawsuit alleging the online search engine leader overcharged thousands of advertisers who paid for bogus sales referrals generated through a ruse known as "click fraud." The proposed settlement, announced by the company Wednesday, would apply to all advertisers in Google's network during the past four years. . . . The total value of the credits available to advertisers will be lower than $90 million because part of that amount will be used to cover the fees of lawyers who filed the case last year in Arkansas state court.
>
> . . . Google makes virtually all of its money from text-based advertising links that trigger commissions each time they are clicked on. Besides enriching Google, the system has been a boon for advertisers, whose sales have been boosted by an increased traffic from prospective buyers. But sometimes mischief makers and scam artists repeatedly click on specific advertising links even though they have no intentions of buying anything. The motives for the malicious activity known as click fraud vary widely, but the net effect is the same: advertisers end up paying for fruitless Web traffic.
>
> The lawsuit alleged Google had conspired with its advertising partners to conceal the magnitude of click fraud to avoid making refunds. . . . The company's shares fell $10.57 to close at $353.88 on the Nasdaq Stock Market, then shed another $2.11 in extended trading.[27]

Commentary: Click fraud! Who would have "thunk" it? When it comes to fraud-threat agents, once again the old adage, "Where there is a will there is a way!" seems to apply. Although stated more than once, I'll state it once again: your anti-fraud program must consider old and new fraud schemes, incorporate today's and tomorrow's high technology as tools for perpetrating frauds, and build an anti-fraud program with the controls and defense against such attacks.

In addition, be sure to incorporate proactive fraud surveys to aggressively look for fraud indicators and, where found, follow up with an aggressive and immediate inquiry to prove or disprove that a fraud has taken or may take place.

PYRAMID SCHEMES MOVE ON TO THE INTERNET

> **Internet company settles pyramid scheme claim . . .** An Arizona company that sells "Internet malls" — Web sites with links to retail-

[27] CNN, 9 March 2006.

> ers — will pay $5 million back to its customers to settle charges that it operated an illegal pyramid scheme, . . . charged more than $100 for each mall, the FTC said, and claimed that customers would make substantial income on the deal if they continued to recruit more participants. Customers received commissions if visitors clicked links on their site and made purchases at the stores. . . . Explanations on the site state that the company blames some of its members for "unscrupulous" conduct, which led to the federal investigation.[28]

Commentary: I am being redundant, but hopefully repetition will help drive home the main points. This is another example of an old fraud scheme being used in today's and probably tomorrow's high-technology, information-dependent, and information-driven world.

> In the . . . Financial Director, . . . was quoted in an article on computer fraud . . . detailed the method of dealing with internal fraud: "The first thing that you do is to make sure that you do not disclose to the internal . . . that he has been discovered. You then monitor what he does to discover where the money or information is going." On the subject of whether or not a victim should bring civil proceedings or rely on criminal proceedings, . . . "Limited police resources mean that there is at least a risk of action not being taken. The police have different priorities and, in the end, a victim will have to decide what is important to him."[29]

PREPAID CELLULAR PHONE FRAUD

> **Ex-Verizon employee charged with fraud . . .** A former Verizon Wireless employee was indicted by a federal grand jury Thursday on charges he stole more than $20 million from the company's prepaid cellular telephone service. . . . indicted on 10 fraud and money laundering counts. As a customer service representative, . . . had access to a password-protected Verizon computer account in which the company kept a record of prepaid cell phone minutes. Customers on the plan could buy cards on which were printed 15-digit personal identification numbers. They would then call a telephone number to activate the prepaid minutes to make a telephone call. . . . alleged to have copied more than $20 million worth of the 15-digit numbers and sold them on his. . . . He continued accessing the Web site and copying the numbers even after he left the company.[30]

---

[28] CNN, 27 March 2001.

[29] Reuters.

[30] Associated Press, 13 August 2004.

Commentary: This is another example of a fraud scheme that is continually being modernized and is keeping up with the high technology and the vulnerabilities they present. Any successful anti-fraud program will continually be updated and will consider what "modernization vulnerabilities" come with the new high technology or processes now in place or those that will be in place in the future — including new services and products that your corporation may offer or use.

Does your corporation use prepaid telephone cards? If not, are you sure, or are you just taking someone's word for it who may or may not really know? If such cards are used, what controls are in place and how do you know they are working? Who monitors their usage and accompanying bills?

IDENTIFYING INTERNATIONAL CORRUPTION

> **U.S. spies on corruption overseas — Listening devices used to compile data on who is bribing who . . .** The U.S. intelligence community uses electronic eavesdropping to maintain and update a top secret database of international bribery cases, according to new reports by the State and Commerce departments and senior U.S. officials. The information is being used extensively as leverage to help American companies compete abroad and is being matched by similar efforts on the part of U.S. economic competitors. . . . THE DATABASE built by U.S. intelligence agencies contains the names of foreign companies that offer bribes to win international contracts and is reported to list hundreds of contracts worth hundreds of billions of dollars that over the past 14 years went to the biggest briber rather than the highest bidder.
>
> The database is developed mainly through electronic eavesdropping, say U.S. intelligence officials. Such eavesdropping, called communications intelligence or COMINT, is at the center of the "Echelon" controversy. European parliamentarians, among others, are accusing the United States of massive electronic spying for commercial purposes, using a worldwide network of spy sites linked by ferret software known as Echelon.
>
> Under a U.S. law known as the Foreign Corrupt Practices Act (FCPA), the U.S. Department of Justice can bring criminal charges against American companies making payments to foreign government officials in order to obtain or retain business. Companies, officers, and directors risk expensive and disruptive investigations, criminal and civil sanctions, and private lawsuits if they fail to take the steps necessary to avoid prohibited payments.[31]

[31] Reported by Robert Windrem, an investigative reporter for NBC News, 21 July 2000.

Commentary: It seems that the saying, "Hello, I am with the government and I am here to help you," comes to mind. It would behoove a CSO to contact his or her local FBI or other entity and determine how such a program might negatively and positively impact your corporation. Will such government representatives talk to you about it or even acknowledge that such a program exists? That may depend more on your personal than official relationship with the person or persons you contact.

This revelation may come as a surprise to some, but not all government employees are honest. Some even perpetrate frauds, as one earlier example shows. Perhaps the government person collecting such information may use it for personal gain. After all, the government is not the best payer in the world.

In the United States, you may be able to obtain at least some limited information if you discuss it as part of the corporation's responsibilities under the Economic Espionage Act. Of course, as the CSO with responsibility for the anti-fraud program, you may have a better chance of succeeding if you are a retired FBI agent — but not always.

CREDIT CARD INFORMATION THEFTS AND FRAUDS

> **MasterCard: Only 68,000 at "higher" risk in breach: . . .** Credit card users, don't fret. Only a small fraction of the 13.9 million credit card accounts at MasterCard that were exposed to possible fraud were considered at high risk, the company said Saturday. MasterCard International Inc. . . . said only about 68,000 of its card holders are at "higher levels of risk." And while those 68,000 should closely examine their credit or debit card accounts, customers do not have to worry about identity theft, . . . which processes credit card and other payments for banks and merchants. . . .
>
> The incident appears to be the largest yet involving financial data in a series of security breaches affecting valuable consumer data at major financial institutions and data brokers. Only about 13.9 million of the 40 million credit card accounts that may have been exposed to fraud were MasterCard accounts. It was not immediately clear how many of the other accounts were considered at high risk. Under federal law, credit card holders are liable for no more than $50 of unauthorized charges. Some card issuers, including MasterCard, offer zero liability to customers on unauthorized use of the card.[32]

Commentary: Only 13.9 million exposed out of 40 million. Wow! What were the other accounts? That sure makes us all feel better, doesn't it? The

[32] Associated Press, 17 June 2005. http://www.usatoday.com/money/perfi/credit/2005–06–17-mastercard-security-breach_x.htm

corporations involved always seem to rationalize such thefts as having little or no impact on consumers or others. I would ask them to prove it. Prove that it does not impact your financial situation or privacy instead of the consumer victims having to prove they have been harmed.

What can a fraud-threat agent do with "only" 13.9 million MasterCard accounts chock full of great information that can be used to help perpetrate multiple types of frauds?

The way to mitigate this terrible lack of protection is to hold the corporation responsible liable and to impose punitive damages based not on whether or not you as an individual were actually harmed but only on the fact that your personal information was not adequately protected. Furthermore, such damages should be very large to help deter such lack of assets protection. That is the only way to get the attention of corporations — by hurting their profit margins. For example, maybe for each account even exposed to compromise, each card holder gets a mandatory $5,000.

When that happens, profits will decline, and stockholders with declining stock value and dividends will demand action. If not, they will also continue to suffer as a result of the lackadaisical attitude of those responsible for protecting these assets — let's start with the CEO.

Will this happen? I doubt it. One just has to look at the massive lobbying campaigns now in effect between corporations and legislatures. Would this proposal for supporting legislation be met by an onslaught of corporate lobbying from many types of corporations? No doubt about it!

HACKERS, CRACKERS, PHISHERS, OH MY!

> **Crackers Snag Credit-Card Info . . .** Three teenagers claim to have stolen approximately 8,000 electronic invoices for online credit-card orders placed over the past two years through a Web electronics retailer. "This shows a disgusting lack of security on the Internet," said one of the crackers, who provided a sample of the data to Wired News this week to support the claim. "Thank God we aren't poor people, or con artists. . . . [We did this] purely for fun." . . . He said the group installed software that allowed them to pilfer 4.3 MB worth of archived credit-card orders and a 15 MB Microsoft Office inventory database. The cracker supplied Wired News with a file that contained copies of 583 credit-card orders for computer equipment purchased online. . . .
>
> The teenagers, all Americans, said they launched their attack by uploading a File Transfer Protocol server program known as *Serv-U* to the Dalco server. With the program's default directory set to the target machine's hard drive, and the program running in the background, the crackers said they were able to browse the directories and steal the data. "It was rather clever," boasted the cracker in an interview conducted over Internet Relay Chat, a global and largely anonymous text-based

> chat network. He said that what he called . . . poorly configured Windows NT 3.5 server allowed his team to gain high-level administrator access to the unencrypted databases. He said on Thursday that he had since erased all of the data from his own machine without passing it on to anyone, but could not speak for the others.[33]

Commentary: Maybe this is an "oldie" but it is still a "goodie." Yet, again we have a case of potential fraud-threat agents taking advantage of the vulnerabilities of high technology. Although the software may evolve, history has shown that, while programmers may close some security loopholes, they often open up new ones. So, it is just a matter of time before defrauders discover these new vulnerabilities and take advantage of them.

URBAN LEGENDS AND FRAUDS

> **You can look up anyone's driver's license for free on the Internet . . .** This is really scary. . . . Now you can see anyone's Drivers License on the Internet, including your own! I just searched for mine and there it was, picture and all.[34]

Commentary: Urban legends appear on the Internet all the time and people pass them around as if they were all true. It is also truly amazing how fast they travel. The author has on more than one occasion received the same urban legend from different people at least three times in one day.

It seems that no one cares to ever check out the information to determine if it is true. This can easily be done by using a search engine and then going to one of the several sites identified for discussing "urban legends." This example is not really a "fraud" per se but is provided just to show how fast information, bogus information, can travel around the world in an instant to probably millions of Internet users who may then take some action based on the bogus information. As noted earlier, such falsehoods can have major impacts on the stocks of corporations and support the perpetrations of various types of frauds.

MEDICAL RESEARCH FRAUD

> **School sorry over stem cell fraud:** Seoul University issues apology after panel findings. . . . One day after a panel investigating the work of

---

[33] http://www.wired.com/science/discoveries/news/1998/10/15665. 16 October 1998.

[34] Paraphrased from material on various urban legend Web sites.

> disgraced South Korean scientist . . . found that he faked claims of cloning human embryonic stem cells, the Seoul National University has issued a public apology. University president . . . said . . . fraud was "an unwashable blemish on the whole scientific community as well as our country" and a "criminal act in academia," according to the Associated Press. . . . resigned last December after colleagues accused him of deliberately fabricating data in his cloning research.[35]

Commentary: As general ethical conduct seems to continue to decline, it has an impact on the very fiber of our societies. One part of society that can least afford fraudulent conduct is in the area of medical research. Such research has a direct bearing on our health and therefore our lives. Millions of precious medical research dollars can be wasted due to fraudulent conduct by those involved in such research.

One wonders about the extent to which medical research frauds are perpetrated on an annual basis all over the world. One must assume that no country or corporation doing medical research is immune to these and other types of frauds.

Projecting such thinking into medical research identifying disease cures, one also wonders whether anyone with a medical condition has or will be crippled, suffer, or even die because some fraud delayed the cure. Many more examples could be cited here, but suffice it to say that a successful fraud may actually be a contributing factor in our deaths.

CORRUPTION AND THE WAR IN IRAQ

> **Rumsfeld: Corruption hurting Iraq:** Administration proposes $439 billion Pentagon budget. . . . Continued corruption in Iraq could damage efforts to create a democracy there, Defense Secretary Donald H. Rumsfeld said Tuesday, adding that it is up to the Iraqis to seize control and take more responsibility for their country. "It's true that violence, corruption and criminality continue to pose challenges in Iraq" and are "so corrosive of democracy," he told members of the Senate Armed Services Committee. "It's critically important that it be attacked and that the new leadership in that country be measured against their commitment to attack corruption," he added. Rumsfeld provided no specific examples. But there have been recent allegations that some revenue from Iraq's slowly rebuilding oil industry have been siphoned to help finance the insurgency there. Rumsfeld added that "our awareness of corruption is increasing," because coalition officials are doing more to investigate those problems within the government.[36]

---

[35] http://edition.cnn.com/2006/HEALTH/01/10/skorea.stemcell/index.html

[36] Associated Press, 7 February 2006.

Commentary: This is another example of and a sad commentary concerning the damage frauds can do. In this case, it may even be responsible for the deaths of innocent civilians and the allies' soldiers. Often, people look at fraud as just a white-collar crime in which big government and major corporations are the only victims, no people actually get hurt, and they (corporations) can afford it and have insurance, and on and on.

COMMENTS ON IDENTITY THEFTS AS A VEHICLE TO FRAUD

> **Identity theft is a part of today's digital landscape, and in today's environment individuals are nearly helpless to protect themselves** either from the theft and abuse of their identity or to repair the damage done by an identity theft. Identities are stolen by the hundreds of thousands, if not millions at a time and can be distributed over the Internet in a matter of hours and the information can be used for fraudulent purposes by a criminal with impunity. None of the currently deployed solutions including encryption, public key infrastructure, digital certificates, secure sockets, etc., are effective in preventing identity theft and abuse.[37]

Commentary: Identity theft and related frauds have exploded with the acceleration of high technology and as prices of high-tech goods have become lower and lower, resulting in increased vulnerabilities. Such successful attacks against employees may have an adverse impact on these employees' behavior and motivation, leading them to perpetrate a fraud to offset their financial losses as a fraud victim, where that motivation to commit a fraud did not exist before the theft.

LOBBYISTS AND CORRUPTION

> **Lobbyist to plead guilty to fraud**, other charges . . . agrees to cooperate with federal prosecutors, . . . Former high-powered lobbyist . . . guilty . . . to corruption, fraud and tax evasion charges in a deal with federal prosecutors, a source close to the negotiations. . . . the former lobbyist may have thousands of e-mails in which he describes influence-peddling and explains what lawmakers were doing in exchange for the money he was putting into their campaign coffers. . . . Prosecutors accused . . . of conspiring to "corruptly offer and provide things of value, including money, meals, trips and entertainment, to federal public officials in return for agreements to perform official acts" benefiting . . . and his lobbyist partner. . . . The government alleged that between January 2000

[37] news@infowar.com

> and April 2004, . . . and the lobbyist "would falsely represent to their clients that certain of the funds were being used for specific purposes.[38]

Commentary: Corrupt politicians — this should come as no surprise. How would such news impact your corporation and an anti-fraud program? What if your corporation's management was paying the lobbyists? How would you know? If you found out, what would you do? These are serious questions and bear serious consequences depending on the action or non-action that you take. As stated earlier, whistleblowers pay a price. Are you willing to pay that price?

INTERNET SCAMS ARE INTERNATIONAL

> **UK: Investors Warned About U.S.-Style Internet Scams:** UK investors have been told to watch out for American-style "pump and dump" Internet scams, in which false information is circulated with a view to forcing up share prices. . . . This particular electronic crime has two elements, international regulators believe. Having bought cheap shares in a lesser-known company, the fraudster generates false publicity as to its value in an effort to pump up the share price. He then dumps the shares and cashes in, leaving investors out of pocket.
>
> The Internet is a perfect medium for attracting potential investors. Perpetrators of such frauds require little more than a credible website, some links to fictitious articles concerning the company's prospects and false share tips disseminated via Internet news groups. The U.S. Securities and Exchange Commission (SEC) has a team of more than 200 people monitoring the Internet for signs of abuse. They carry out regular sweeps, working with the SEC's Office of Internet Enforcement.[39]

Commentary: This is another example, albeit on a more global scale, of the use of today's high technology to support a fraud scheme.

FAKING A MEDICAL CONDITION

> **Prosecutors: Man Faked Retardation for Nearly 20 Years to Scam Government Out of $111,000:** For nearly 20 years . . . his mother has collected disability benefits on his behalf. In meetings with Social Security officials and psychologists, he appeared mentally retarded and

---

[38] http://us.cnn.com/2006/POLITICS/01/03/abramoff.plea/index.html
[39] *The Times*, 11 May 1999.

> unable to communicate. His mother insisted he couldn't read or write, shower, take care of himself or drive a car. But now prosecutors say it was all a huge fraud, and they have video. . . . contesting a traffic ticket to prove it. "He's like any other person trying to get out of a traffic ticket," Assistant U.S. Attorney Norman Barbosa said Tuesday . . . indicted in September on charges of conspiracy to defraud the government and Social Security fraud, and the case was unsealed Tuesday. . . . The benefits cited in the indictment totaled $111,000.[40]

Commentary: This is another amazing example of defrauders using any opportunity to perpetrate a fraud. What if the mother was a corporate employee? Of course, if found guilty, she might be fired, but even before that, shouldn't some anti-fraud processes be in place to see what corporate assets she had access to and what controls are in place to protect them?

Are there any fraud indicators relative to her access and use of the corporate assets? Shouldn't your anti-fraud program have processes in place that allow a further check into this corporate employee's access to corporate assets?

INTERNET FRAUD SWEEP

> **New Jersey Charges Nine in Internet Fraud Sweep . . .** The New Jersey attorney general's office filed civil charges against nine people on Monday as part of an Internet fraud crackdown that uncovered bogus sales of company stocks, Beanie Baby toys and the impotence drug Viagra. "On the Internet, fraud is just a mouse-click away," Mark Herr, director of the New Jersey Attorney General's Consumer Affairs Division, said in announcing the charges. He said the cases were the first in the state involving "significant cyber-fraud." Five people were named in a nine-count complaint charging them with sales of 531,898 shares of unregistered stock in (a corporation) a phony e-commerce services company. . . . The complaint alleged more than 350 investors were bilked of $850,000 that the defendants took for personal use and which were not used for legitimate business purposes. None of the defendants was registered with the state's Bureau of Securities or the National Association of Securities Dealers.[41]

Commentary: High-technology tools combined with the innovation of fraud-threat agents continue to lead to new fraud schemes and more sophisticated use of old fraud schemes.

---

[40] http://www.foxnews.com/printer_friendly_story/0,3566,234657,00.html

[41] Reuters, 16 November 1999.

ATM FRAUD

> **Thieves net $100,000 in WaMu ATM scheme . . .** Group used fake keypads and bank-card slots in New York branches to steal from bank accounts. . . . A sophisticated group of thieves used technical trickery to steal ATM card information — and over $100,000 — from customers at two New York City Washington Mutual branches. The thieves rigged fake keypads and bank-card slots onto ATMs to gather card information and encoded the information on new cards, police say. They then used the new, fraudulent cards for withdrawals from approximately 50 Washington Mutual accounts at other ATM locations. . . . Images of the suspects were recorded on the bank's security cameras.[42]

Commentary: ATM frauds continue to occur; however, it is believed they are occurring at a slower rate than when the ATMs first came into use. It is probably still more likely that an ATM customer will be mugged at an ATM than a fraud-threat agent will take advantage of the vulnerabilities of ATMs.

Recently, some have said that the encrypted software used to facilitate ATM transactions may not be secure. This may be the case, but for all but the most sophisticated miscreants, they are probably secure. For those with a Ph.D. in computer science, can we consider any high-technology device secure?

We should never consider any high-technology device, any controls, or any portion of any anti-fraud program to be able to stop 100% of all fraud-threat agents or to thwart all fraud schemes. All we can ever expect is that the levels of risks will be made as low as possible and that for the remainder, we can hope for the best. As some movie dialogue once went: "Hope? We are hanging on hope?" The answer is that when all is said and done, "Yes, we are." Our hope is based on the philosophy of risk mitigation and not risk elimination.

SOCIAL SECURITY SCAM

> **The Social Security Administration (SSA) has warned of a new e-mail scam** in which recipients are asked to update their personal information or risk having their Social Security "account" suspended indefinitely. Recipients are then directed to click on a link in the e-mail that takes them to a Web site designed to look like the SSA's Web site. Among the pieces of information recipients are asked to give are: Name, Address, Date of Birth, Social Security Number, Credit Card Number, and/or Bank Account Number.[43]

---

[42] http://money.cnn.com/2006/01/06/news/atm_fraud/index.htm?cnn=yes

[43] *AFOSISA Global Alliance* magazine, Summer 2006.

Commentary: This is a typical scam, and one can tell by the detailed, personal information requested that the SSA, other government agencies, or private agencies for that matter would not ask for. When you go online to transact business and a credit card or other personal information is requested, you must always check the Web site address to be sure you are at the proper Web site address and not one that looks like the legitimate address. You may also want to use your search engine to find the Web site you are interested in. Never click on a Web site that is noted in an e-mail to you and then transact business. Yes, it may be legitimate, but why take the chance? Just search for that business's or government agency's Web site and then go to it. You still may end up on a bogus site, but your chance of going to the legitimate site is better.

STAMP FRAUD

> **Spanish Police Raid Auction Houses in Stamp Fraud Probe . . .** At least four people have been arrested in raids by Spanish police as part of an ongoing fraud investigation involving two prominent stamp collection companies. . . . The companies . . . are accused of defrauding nearly 200,000 mostly retired investors in a pyramid scheme involving overvalued stamps . . . subject of a Barron's magazine investigation, which found that its stamps were likely overvalued and that proceeds from sales to new investors were being used to pay returns to other investors. Barron's also reported that Lloyd's of London, insurer to the tune of $1.5 billion, might pull their backing over the allegations of improper practices.[44]

Commentary: There are probably as many different types of fraud targets and victims as there are pyramid–Ponzi schemes. The greed of the fraud victims is a major contributor to successful frauds. How will you try to deal with the human greed issue as part of your anti-fraud program? One view is that you discuss the potential negatives of perpetrating a fraud as part of the employees' awareness program, put controls in place to minimize the opportunities for frauds, and conduct aggressive fraud surveys looking for fraud indicators and employees who are not following procedures that impact the potential for frauds to occur.

The idea is to take away one or more of the following:

- *Opportunities* to perpetrate a successful fraud
- Employees' *motivation* to commit a fraud and/or
- Any *rationale* that an employee may use for committing the fraud — this is probably the most difficult task because humans can rationalize anything regardless of the facts.

[44] http://www.foxnews.com/printer_friendly_story/0,3566,194804,00.html

An interesting book about Ponzi who is "credited" with the Ponzi scheme is author Mitchell Zuckoff's book, *Ponzi's Scheme — The True Story of a Financial Legend*. It is an interesting read and helps one to understand how such a fraud can occur, even when one seems to have no real intention to perpetrate a fraud — at least at first.

BANKER AND IDENTITY THEFT

> **Russian bank chief jailed for identity theft . . .** A Russian bank chief, who coordinated an international identity theft operation, has been jailed for six years . . . helped run a criminal gang, which stole millions of pounds from British, American and Spanish account holders. The fraudsters used stolen credit card numbers to create false identities to purchase expensive electronic equipment and other goods, which they then resold on eBay. Police believe the global campaign could have spanned a decade.[45]

Commentary: Identity theft is a tempting fraud-related crime as one can commit this crime from other nations, often with impunity. Of course, all types of crime are rampant in Russia today, so the existence of identify theft there should not be surprising, even from a banker!

ACCOUNTING FIRM FRAUD

> **New York attorney general accuses accounting firm of fraudulent business practices by steering customers into IRA accounts. . . .** filed a lawsuit Wednesday against the accounting firm . . . sending the company's shares plunging. . . . stock tumbled nearly 8 percent in mid-morning trade on the New York Stock Exchange following the news.
>
> . . . accused the financial services firm of fraudulent business practices by steering approximately 500,000 customers into IRA accounts, that were "virtually guaranteed" to lose money. Those customers who opened the Express IRA accounts were often burdened by unadvertised account fees, making it difficult to grow their savings.[46]

Commentary: If you can't trust a major accounting firm to identify improper procedures in a corporation, within their own corporation and the like,

---

[45] SC Magazine, 19 December 2006. http://www.scmagazine.com/uk/news/article/610317/russian-bank-chief-jailed-identity-theft

[46] http://money.cnn.com/2006/03/15/news/companies/spitzer_hr/index.htm?cnn=yes

who can you trust to identify frauds? The answer is you can't trust anyone. Under the right circumstances, anyone will perpetrate a fraud — even you or me. You may say you would never do that and yes, you may be the exception. However, there may be circumstances that provide you with the opportunity, motive, and rationale to do so.

Have you ever in your lifetime taken something of value from another without reimbursing that person for what you took? Maybe you just didn't put the 50 cents in the coffee collection can when you took that cup of office coffee. Petty? Maybe. Wrong? Of course. So how did you rationalize that theft? No change? No money? The price is too high and you only pay for every third cup? Yes, rationalization is an interesting human phenomenon. Actually, you can see that it can work at all levels of thefts or frauds.

Never say never is good advice. After all, as we often find, we are surprised when we learn that the father or mother and pillar of the community or the little ole lady and grandmother is a major defrauder. We are astounded! How could he or she do that? I would never have suspected such a person.

You will find that each one of us may have what we consider to be a valid reason, a rationale as to why we would attempt to perpetrate a fraud, even if we are God-fearing, church-going, part-time Sunday School teachers. Human nature is interesting to study and important for you to try to understand as you go about developing a successful anti-fraud program. Remember: corporations don't commit frauds — people do.

What human beings are made of and what constitutes our ways of thinking are often neglected areas of consideration when we set about to protect corporate or other entities' assets from defrauders or other miscreants. However, it is probably our most important consideration when we are developing an anti-fraud program. We must also understand the thinking of fraud-threat agents. Too often we concentrate on controls almost in a vacuum; however, for controls to work, they must be based at least in part on the potential fraud-related thinking and actions of the employees.

> Ex-Tyco CEO was sentenced to 8⅓ to 25 years in prison Monday for his part in stealing hundreds of millions of dollars from the manufacturing conglomerate.[47]

[47] CNN Money, 19 September 2005

LAWYERS AND MEDICAL RIP-OFFS

Today's human beings are in general living longer and healthier lives than ever before. At the same time, we humans are messing up this earth with toxic chemicals and other man-made inventions. Although maybe not a fraud in all cases per se, the following provides the potential for fraud:

> **The $40 Billion Scam: How slick lawyers have turned a genuine health crisis into a ripoff you won't believe . . .** So far, at least 79 companies have filed for bankruptcy due to asbestos litigation alone, and 60,000 workers have lost their jobs. About 8,400 companies with facilities nationwide have faced lawsuits. Meanwhile, insurance companies are out $59 billion through 2005, with $34 billion paid out in cases and another $25 billion locked away in reserves. Those costs get passed along to consumers and companies as higher premiums and eventually prices for thousands of products and services.
>
> And what about those plaintiff lawyers behind the flood of lawsuits?
>
> "I would estimate their fees are north of $20 billion," says Brickman (A professor of law at the Cardozo School of Law at Yeshiva University in New York), who has exhaustively researched the scandal over 16 years. "The bottom line is that in mass torts, fraud works."[48]

These diagnoses were driven by neither health nor justice. They were manufactured for money. *U.S. District Judge Janis Jack*.

ANOTHER MENTION OF THE "NIGERIAN" SCAMS — VARIATIONS ON A THEME

Last but certainly not least is the topic of the Nigerian type of scams floating around the Internet. There are so many versions of this type of fraud that citing them all would double the size of this chapter!

The basic premise of this fraud scheme is that someone somewhere will reply to the e-mail and then be convinced either to send money or visit a certain place in order to collect money. As previously mentioned in Chapter 6, this is a dangerous fraud scam.

If you have not received any of these types of e-mails, you must not have any e-mail connections!

---

[48] "The Legal Scam You Pay For," *Reader's Digest*, January 2007, p. 74

CASE STUDY

You are beginning the development of your corporation's anti-fraud program. What processes would you consider integrating into your program based on the fraud cases cited in this chapter?

For this case study, no sample answer is given. All that information and hints of what to do are found throughout the commentaries associated with the cited cases.

Hacker attack at UCLA affects 800,000 people:

- UCLA says hacker invaded database for more than a year.
- Info exposed on about 800,000 students, faculty, staff.
- Data included Social Security numbers, birth dates, and addresses.
- UCLA: No evidence any data have been misused.[49]

SUMMARY

Thousands, if not millions, of frauds that have been perpetrated over the centuries. Ever since one human being wanted to have something of value belonging to another human being without providing just compensation and the owner's agreement, fraud schemes have been used to illegally gain that asset or assets.

With the ever-increasing role of high technology in our world many new frauds have sprung up, and many old ones have been identified, which have been brought into the twenty-first century through the use of the high-technology tools with all their vulnerabilities.

The examples provided do not even come close to identifying each type of fraud scheme that has been tried. Such an endeavor would take lifetimes and probably still not be completed. However, the examples do give some idea as to what the fraud fighter is up against, and they also help the fraud fighter develop a successful anti-fraud program based in part on the fraud schemes and identified types of frauds noted in this chapter.

[49] Associated Press via CNN, 12 December 2006.

This page intentionally left blank

II

ESTABLISHING AND MANAGING AN ANTI-FRAUD PROGRAM

Section I introduced you to the world in which businesses operate on a global scale; discussed the impact of high technology on businesses and frauds; and presented some fraud laws, schemes, and cases to help you gain a basic awareness of the fraud threats against your corporation's or other entity's assets.

Section II is the heart of this book. It provides you with a basic anti-fraud program guide on which you can build a program specific to your corporation's needs. It is not all-encompassing but is a guide to help get you started in defending your corporation's assets from fraud-threat agents.

This section begins with an introduction to the fictitious International Widget Corporation (IWC). This international corporation provides you with a model that you can use to build your anti-fraud program. It is especially useful for those of you who do not as of yet work for a corporation as a leader in establishing and managing a corporate anti-fraud program or have responsibility for assets protection.

This method has been used in the past, and readers have commented favorably on the usefulness of providing such a fictitious corporation.

The subsequent chapters explain how to begin to develop an anti-fraud program and manage it, including getting direct and indirect support of others within the corporation.

Section II's chapters are as follows:

Chapter 8 The International Widget Corporation
Chapter 9 Establishing an Anti-Fraud Program
Chapter 10 Managing an Anti-Fraud Program
Chapter 11 Winning through Teaming

Chapter 12 Anti-Fraud Functions
Chapter 13 Are We Winning the Battle? How Do We Know? Measure it!

The title of each chapter provides you with some idea as to what will be covered in this section.

As a reminder of what was stated in the Preface, the emphasis of this book is on *establishing* and *managing* an anti-fraud program in order to fight fraud. Therefore, you can expect this section to emphasize management techniques, teamwork, and liaison approaches that are useful when you begin to establish an anti-fraud methodology for your corporation (e.g., budget) and generally work with others within an international corporate environment.

8

The International Widget Corporation

INTRODUCTION

The International Widget Corporation (IWC) is a fictitious international corporation that you as the chief security officer (CSO), or another who has responsibility to lead an anti-fraud effort, can use to develop an anti-fraud program. It is also a model to help the fraud fighter think about how to defend corporate assets against global fraud-threat agents and their schemes.

This method (using a fictional corporation as a model) is used to assist the new CSO by providing a more practical model for a corporate anti-fraud program, as well as provide information that may also prove useful to experienced CSOs. In other words, it represents more of a "real-life" approach using real scenarios. The scenarios and the actions taken are based on actual situations that can be found in today's modern business environments.

You are encouraged to build an anti-fraud program based on IWC. One word of caution, however: the approach used is provided in a simplistic form. Even so, the basics provided will at least provide some assistance in your more complex environment — at least that is the goal.

IWC BACKGROUND INFORMATION

The IWC CSO must understand the business and processes of IWC if a quality, cost-effective, corporate anti-fraud program is to be developed for IWC. Part of that process requires the CSO to identify those key elements of IWC's history and business that must be considered in developing the IWC anti-fraud program, as well as consider IWC's organizational structure. (See Figure 8-1.)

The following is a summary of IWC's business environment (italics on page 168 are added to identify the key phrases that the CSO must take into consideration when building the anti-fraud program.):

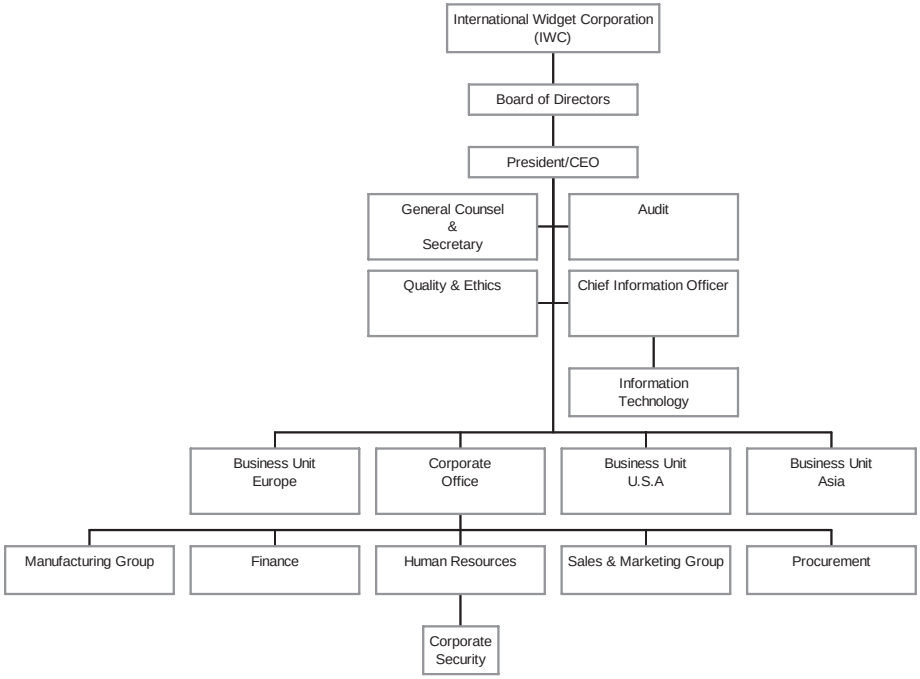


Figure 8-1. High-level organizational structure of IWC.

IWC is a high-technology corporation that makes high-technology widgets. In order to make these widgets, it uses a proprietary process that has evolved over the five years that IWC has been in business.

The proprietary process is the key to IWC's success as a leader in the manufacturing of high-technology widgets. The process had cost millions of dollars to develop. The protection of the high-technology widget process is vital to IWC's survival.

Computers are used to control the robots used in the manufacturing of widgets. Over the years, the use of robots has drastically reduced costs by eliminating many of the human manufacturing jobs. This automated manufacturing process is the pride of IWC and is considered one of its "crown jewels." Without this automation, IWC could literally no longer produce the widgets, not only because of the cost factors, but also because the manufacturing requires such small tolerances to make the products that humans could not manufacture today's widgets.

IWC is in an extremely competitive business environment. However, based on changes in technology that allow for a more efficient and effective operation through telecommunications and networks, it has found that it must network with its global customers and subcontractors. Furthermore, IWC continues to look for new ways to replace employees with robotics or

other ways of creating efficiencies to lower the number of employees that IWC must employ. It currently has low profit margins and any frauds will adversely impact that margin.

To provide for maximization of the high-technology widget process, IWC shares or interfaces its networks with its subcontractors, who must also use IWC's proprietary processes. The subcontractors, under contractual agreements, have promised not to use or share IWC's proprietary information with anyone. They have also agreed to protect that information in accordance with the security requirements (which include those defenses that assist in protecting the assets against threat agents) of their contract with IWC. (*Note*: All contracts that include the sharing of IWC assets should include asset protection specifications and address liability issues.)

Because of today's global marketplace, IWC has expanded its operations to include some manufacturing plants, coupled with small marketing and sales forces in Europe and Asia. This expansion took place in order to take advantage of the lower manufacturing and operational costs available outside the United States. In addition, this approach enables IWC to take advantage of political considerations; the corporation is looked upon as a local enterprise, thus gaining at least some political support to make marketing and selling easier in the countries where they are located.

Currently, a small manufacturing plant is located in the Dublin, Ireland, area and consideration is being given to opening up a plant outside of Prague, Czech Republic, within the next one to two years. Once that plant is operating as expected — with at least 25% lower operating costs than those in the Dublin plant — the plan is to close the Dublin plant and use Prague as the European home manufacturing base.

In order to take advantage of the Asian market and the cheap labor and overhead costs in China, IWC has decided to move its Asian plant from Taiwan to China (PRC) within a year. The China plant will be located outside of Guangzhou. The IWC executives hotly debated the decision to open the plant in China. In order to open the plant in China, the Chinese government requires IWC to share its technology and assets and to do so as a joint partner with a Chinese firm known as "Lucky Red Star."

The concern over this joint venture is that by sharing the "crown jewels," IWC's assets and proprietary processes could subsequently be used to compete against IWC on a global basis, and, moreover, with the Chinese government's support. The IWC executives were concerned that they might eventually be priced out of business. In the end, however, the executives decided that these business risks must be taken if IWC had any hopes of expanding its sales throughout Asia and leveraging the cheaper manufacturing costs in China and the Czech Republic. IWC will consider eliminating the manufacturing plant within the United States sometime within the next three to five years, after the European and Asian operations have proved successful.

Because of the many potential counterfeiting schemes, copyright violations, and such, IWC is also concerned about increased attacks against the corporate assets, especially its "crown jewels," as well as more fraud-threat agents' attacks.

KEY ELEMENTS FOR THE CSO TO CONSIDER

On the basis of this background information on IWC, the IWC CSO should keep the following key elements in mind:

1. IWC is a *high-technology, multibillion dollar, highly visible, global corporation*: IWC uses and is dependent on information and computer-based processes. Such technology is vulnerable to a multitude of different attacks, including those by fraud-threat agents. This makes the IWC assets protection and anti-fraud programs of vital importance. Its locations, visibility, and economic power make it a prime target for fraudsters.
2. IWC *uses a proprietary process:* Information relative to the proprietary process is one of the most valuable assets within IWC, and it must be protected at all costs from all threats, including the use of fraud schemes to gain access to this process.
3. *The proprietary process is the key to IWC's success and vital to company survival:* The number one priority of the assets protection and anti-fraud programs must be to ensure that this process receives the highest protection. It is therefore a priority for the CSO to ensure that the current anti-fraud mechanisms are in place and that they are adequate.
4. IWC is *in an extremely competitive business*: To the CSO, this means that the potential for use of fraud schemes is a factor to consider in establishing the anti-fraud program.
5. IWC is *networked with its customers and subcontractors; subcontractors must also use IWC's proprietary process*, *under contractual agreements:* When the CSO builds the IWC anti-fraud program, the customers' and subcontractors' interfaces to IWC entities must be a key anti-fraud concern.
6. Because of today's global marketplace, IWC has over the last several years expanded its operations to include some *manufacturing plants, coupled with a small marketing and sales force in Europe and Asia*. The European and Asian plants must also be considered when developing the IWC anti-fraud program. The program must be global in nature, but it must also consider the risks and fraud threats to its assets based on working in a foreign environment. For example, the amount and type of local frauds, as well as the society and culture of the foreign nations, must also be factored into the anti-fraud program.

7. Because of the foreign plants, *key executives will also be traveling extensively to the foreign locations*. Therefore, the threats posed by defrauders must be factored into any foreign travel briefings to these executives and to all other corporate employees who will be traveling overseas, even if for vacation.

GETTING TO KNOW IWC

Since the CSO is new to IWC and the widget industry, the CSO, in the first week of employment, will walk around the entire company, see how widgets are made, learn what processes are used to make the widgets, and watch the process from beginning to end.

The CSO will want to know as much as possible about the company. It is very important that the CSO understand the inner workings of the company. In fact, before being interviewed and finally hired as the CSO, the CSO applicant researched and studied all possible information about IWC and the widget industry. This knowledge proved very useful in the job interview process

Many new CSOs sit through the general in-briefing given to new employees, learn some general information about the company, and then go to their office. They start working and may not see how the company actually operates or makes widgets. They seldom see or meet the other people who participate in hands-on protection of the IWC's vital assets from fraud-threat agents and others. These people include users of automated systems on the factory floor, human resources personnel, quality control personnel, legal staff members, auditors, procurement personnel, contract personnel, financial specialists, purchasing and contract specialists, in-house subcontractors, and other non-IWC employees.

When asked why they don't walk around the plant or understand the company processes, the normal reply is: "I don't have the time. I'm too busy 'putting out fires'!" The answer to that dilemma is take a time management course; manage your time better; and make the time!

A CSO cannot provide a service and support-oriented anti-fraud program without an understanding of the company, its culture, and how its products are made. If you want to spend your time "putting out fires," do it right and join the fire department because you won't be a successful CSO.

The CSO should know how the manufacturing processes operate, how manufacturing is supported by other company elements, how employees use IWC assets, the problems they are having doing their jobs because of assets protection — security — constraints, and whether or not they are even following the IWC assets protection policies and procedures. As the CSO is acquiring this knowledge, he or she should be cognizant of the potential for various fraud attacks.

While the CSO is learning about the corporation and how things are done, employees should also be asked how well they think the assets they use are protected from fraud attacks and what they consider some of the processes' weaknesses.

All the IWC anti-fraud and related assets protection policies and procedures neatly typed and placed in binders will simply be ignored if they get in the way of employees doing their primary functions or do not help defend against fraud attacks.

The IWC CSO understands that one cannot see all these things from the office or cubicle. The CSO can only do the job well by walking around the areas where the people are working and actually using IWC assets, and by talking to all levels of employees from corporate management to the custodians. In addition, the new CSO should ensure that all members of the security staff, as well as all other corporate employees belonging to the anti-fraud team leadership group, take the same approach to their jobs.

IWC'S BUSINESS PLANS

The CSO must have an understanding of business and business competition on a global scale. Prior to developing an anti-fraud program, the CSO must also read and understand the IWC plans, which include the corporation's Strategic Business Plan, Tactical Business Plan, and Annual Business Plan. These plans are outlined at the executive management level and are passed down to all IWC departments. The management of the departments then makes input into the plan outline, after which this information is integrated at the executive management level. From there, the plans are passed down to the IWC departments, who will develop their own plans to support the overall IWC plans (see Figure 8-2).

STRATEGIC BUSINESS PLAN

IWC has developed a proprietary, Strategic Business Plan (IWC SBP), which describes IWC's strategy for maintaining its competitive edge in the design, manufacture, and sale of high-technology widgets. That plan sets the baseline and the direction that IWC will follow for the next seven years. It is considered IWC's long-range plan. It was decided that any plan longer than seven years was not feasible owing to the rapidly changing environment created by technology and IWC's competitive business environment.

The IWC SBP sets forth the following:

- The expected annual earnings for the next seven years.
- The market-share percentage goals on an annual basis.

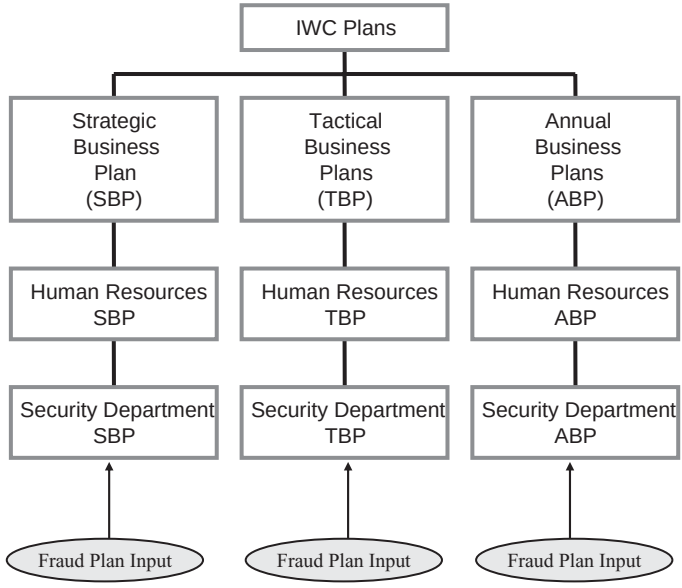


Figure 8-2. Structure of the IWC business plans.

- The future process modernization projects based on expected technology changes bringing faster, cheaper, and more powerful computers, telecommunications systems, and robotics.
- IWC expansion goals.
- IWC's acquisition of some current subcontractor and competitive companies.
- The requirement that a mature anti-fraud program can protect IWC's valuable assets, especially its proprietary information and processes, while allowing access to these assets by its international and national customers, subcontractors, and suppliers.

The CSO must understand the IWC SBP because the corporate security SBP must be integrated into the next level of SBP and provide the strategies necessary to support the IWC SBP. This includes the anti-fraud elements of such an effort.

TACTICAL BUSINESS PLAN

IWC's proprietary Tactical Business Plan (IWC TBP) is a three-year plan and sets more definitive goals, objectives, and tasks. The IWC TBP is the short-range plan that is used to support IWC's SBP. IWC's successful

implementation and completion of its projects is a critical element in meeting IWC's goals and objectives.

The IWC TBP also calls for the *completion* of an anti-fraud program that can protect IWC's proprietary and sensitive information and processes as well as other assets, while allowing access to them as needed under contractual agreements with national and international customers, subcontractors, and suppliers. In addition, it is expected to be able to integrate new, secure processes and the like, with *minimum* impact on schedules or costs.

Key Elements of IWC's TBP

The IWC TBP must itself also be protected from fraud-threat agents in a similar fashion as the IWC SBP.

The CSO must always remember that some of the IWC assets, such as its information, are time-sensitive and that the global marketplace is always dynamic. That is, its value to defrauders and others is time-dependent and changes as global market conditions change. Thus, its anti-fraud defense requirements may decrease over time and also be less costly. This is a key factor in protecting any information: *It should be protected using only those methods necessary, and only for the time period required, based on the value of that asset over time.*

> The CSO must consider that the IWC anti-fraud program must contain processes to reevaluate the anti-fraud defensive mechanisms used to protect IWC assets so that it is only protected for the period required.

As was true with the IWC SBP, the CSO must understand the IWC TBP because an IWC security TBP must be developed to integrate security services and support into the IWC TBP. The corporate security TBP should identify the goals, objectives, and tactics necessary to support the IWC TBP. These must include the establishment and maintenance of a proactive anti-fraud program.

A key point that should not be overlooked can be found by comparing portions of the IWC SBP and the IWC TBP. The IWC SBP states that "[i]n addition, it is expected that the anti-fraud program will be capable of supporting the integration of new customers, subcontractors, plants, processes, hardware, software, networks, etc. while maintaining the required level of threat agent defenses without impact to schedules or costs."

The IWC TBP includes a similar statement: "In addition, it is expected that the anti-fraud program will be capable of supporting the integration of new customers, subcontractors, plants, processes, hardware, software,

networks, etc. while maintaining the required level of anti-fraud defenses with minimal impact to schedules or costs."

The interpretation can be made that the CSO has three years to establish a viable anti-fraud program with minimal impact on schedules and costs. After that three-year period, it is expected that the anti-fraud program will *not* impact schedules or costs. As the new CSO, you must determine if that goal of zero impact is possible. (*Hint*: There will always be some impact. The goal should be to minimize that impact.)

As the new CSO, this potential conflict should be immediately brought to the attention of upper management for clarification and interpretation. The apparent conflict may have been caused by the selection of a poor choice of words. However, it may be that the IWC management meant what they said. It is then up to you as the IWC CSO to meet that objective or have the sentence clarified and changed.

IWC'S ANNUAL BUSINESS PLAN

IWC also has a proprietary Annual Business Plan (IWC ABP) that sets forth its goals and objectives for the year. The IWC ABP defines the specific projects to be implemented and completed by the end of the year. The successful completion of these projects will contribute to the success of IWC's Tactical Business Plan and Strategic Business Plan.

IWC's ABP called for the hiring of a CSO to establish an anti-fraud program that would provide for the protection of IWC's valuable assets from fraud-threat agents, while allowing access to the assets by its customers, subcontractors, and suppliers. This obviously seems like an impossible challenge, but it is not one that is unusual for corporate executives to demand or require.

The CSO will also be responsible for managing the corporate security organization. The CSO will report to the executive vice president of Human Resources (HR). The executive vice president of HR reports directly to IWC's chief executive officer (CEO).

IWC AND THE HISTORY OF ITS CSO

At one time, IWC had only a professional physical security program made up of alarm systems, badge readers, and a guard force. Its program was accomplished under a guard force, outsourcing contract as overseen by the IWC Contracts and Procurement Office. This office also oversees its separate access badge reader contract and its alarm system contract. Ultimately, however, the IWC executives determined that they needed a professional CSO and organization to meet their ever-increasing security requirements as they expand worldwide and mature as a corporation.

IWC's executive management agreed that a CSO position should be established and that the CSO hired should lead the IWC's assets protection program. Because IWC had previously been a victim of fraud attacks, the CSO was also charged with establishing an anti-fraud program and managing the corporate security organization. However, no consensus was reached as to where in IWC the CSO reported. The new CSO did understand, however, that no assets protection program could be successful unless it included an anti-fraud program as part of the overall assets protection program.

Some members of executive management recommended that the CSO report to the director of auditing. However, the director of auditing advised that the auditing department was strictly responsible for determining IWC's compliance with applicable state, federal, and international laws and company policies and procedures. The director felt that the auditors' limited scope and functions would adversely limit the CSO in establishing and managing an assets protection program as well as the anti-fraud program.

The director of auditing also argued that a conflict of interest might present itself if the CSO were to establish corporate anti-fraud policies and procedures — albeit with management support and approval — while at the same time having another part of that organization (the audit group) determine not only compliance with those policies and procedures, but also if they were adequate.

The CSO and the corporate security department were also considered for inclusion in the Information Technology Department (IT) since IWC was an information-based and high technology-supported corporation whose major assets were computer-based. The reasoning was that the majority of assets that required protection were IT supported, regardless of whether they were protected from defrauders, thieves, or other miscreants.

Since the information systems security (InfoSec) organization was under IT, it made sense to place all of security under IT. However, the executive vice president of IT strongly objected. That offer was tabled pending the hiring of the CSO. They reasoned that the CSO and the vice president of IT could meet later, discuss relevant anti-fraud defensive issues, and decide the best approach to be used by the IT Department.

Also considered as the "home" of the CSO and the corporate security organization was the Finance Department, which also reported directly to the CEO. Both of these were not considered "practical" by the vice president of finance and the CEO.

Following a survey taken of other corporations similar to IWC, it was determined that the majority of the corporate security departments in those corporations were part of the Human Resources departments. Thus, it was finally decided that the CSO position and organization should be established within the HR Department. Apparently, no one else seemed to want

to be responsible for the function, but also it seemed a logical positioning based on the survey.

A CSO was hired; however, due to the lack of progress in developing an anti-fraud program and the loss of some valuable corporate assets as a result of successful fraud attacks, the other CSO was fired and the new CSO (you, the reader) was hired. During the interview process and again after being hired, the new CSO determined why the CSO position was formed and why it reported where it did in the IWC organizational structure.

During the interview process, the new CSO applicant laid out an anti-fraud program baseline that helped the executive management team select you as the new CSO as no other applicant or past CSO ever discussed providing an anti-fraud program and for making the case as to why one would be necessary, but as a subset of the assets protection program. Such an IWE anti-fraud program made a great deal of sense to the management team, especially after the CSO (when an applicant for the position) provided examples of the types of fraud threats, schemes, and fraud successes that had taken place against other corporations and other entities.

The new CSO's understanding of how this position ended up where it did provides some clues as to the feeling and inner workings of IWC's management vis-à-vis the CSO and the anti-fraud program. This information will be useful both when the CSO begins to establish IWC's anti-fraud program and when the CSO requests support from these corporate executives. It also provides the CSO with some insight into what type of support the CSO's organization may receive from these executives. The circumstances surrounding the firing of the previous CSO also helped the new CSO understand what must now be considered the number one priority: the establishment of the IWC anti-fraud program.

Here is an example of the use of this information: Knowing that no major, logical department within IWC wanted the corporate security, responsibility could be leveraged. That means that those department heads might not mind supporting corporate security and the anti-fraud program, but they did not want to have too much responsibility for that effort. This provided the CSO the possibility of being a strong leader without concerns that the departments identified would want to absorb some of the security functions into their departments. Thus, a more centralized, CSO-directed anti-fraud program could probably be established. As with any position within a corporation, office politics played a major role in this endeavor, as did informal information channels, such as the flow of gossip. To be successful, the CSO must understand the "game" of office politics, power, and "back-channel" information flows.

Furthermore, it is clear that the director of auditing would support the anti-fraud program but had some concern as to how well the auditors would support the CSO leading the anti-fraud program. The CSO assumed that from the auditing standpoint, the audit manager would probably agree to be part of an anti-fraud team but would not want any responsibility for

writing the assets protection and the anti-fraud program policies and procedures.

When the CSO decides how to establish assets protection and anti-fraud policies and procedures, he or she must keep in mind what departments should be involved in a particular part of that development and "buy-in" process.

KEY ELEMENTS OF IWC'S ANNUAL BUSINESS PLAN

The CSO must also develop a corporate anti-fraud program annual business plan. That plan must include goals, objectives, and projects that will support the goals and objectives of IWC's ABP and include those associated with defending the corporate assets against defrauders and other miscreants.

ANTI-FRAUD PROGRAM PLANNING

The main philosophy running through this chapter should be obvious: As a service and support organization, the IWC security department and the IWC anti-fraud program must include plans that support the corporation's business plans.

The CSO should be able to map each major business goal and the objective of each plan to key anti-fraud program projects and functions. When writing the applicable anti-fraud program plan, the CSO will also be able to see which functions are not being supported. That may or may not be a problem. However, the mapping will allow the CSO to identify areas where required support to the plans has not been identified in the CSO's plans.

The CSO can then add tasks where increased anti-fraud support is needed. Following this procedure will show management how the anti-fraud program is supporting the business. When mapping the anti-fraud program plan probably through the assets protection plan to the business plans, the CSO should summarize the goals because they will be easier to map.

IWC'S DEPARTMENTS OF PRIMARY IMPORTANCE TO THE CSO

Since the IWC Security Department is a service and support organization, all the IWC departments and personnel are important to the CSO. However, the CSO must work closely with several departments and rely on them to successfully provide anti-fraud program service and support. In addition, several are an integral part of helping to ensure that the anti-fraud

program is successfully implemented and managed. At IWC, these departments are:

- *Ethics Department*: This small organization reports to the CEO and is managed by a director. This organization is responsible for working with the training department to provide ethics training to the employees. In addition, it manages the IWC Ethics Hotline. The Ethics Hotline was established to receive complaints and conduct inquiries into allegations of wrongdoings by the employees or others who may be associated with IWC. The complainants may remain anonymous if they so choose. If they provide their names, that information is kept IWC-Private.

  If an allegation is received that requires more detailed inquiry possibly involving evidence, more in-depth interviews, and interrogations, the ethics director provides that information to the CSO's manager of investigations. The manager of investigations works directly for the CSO, conducts the inquiries, and reports the results back to the director of ethics, who is defined as the internal customer for such matters. The director of ethics chairs a monthly ethics meeting whose members include the CSO's representative (manager of investigations), legal representative, Human Resources representative, and the manager of audits
- *Audit Department*: IWC's Audit Department is similar to other corporate audit departments. The auditors in this department have the primary responsibility for conducting audits to ensure that IWC is operating and that its employees are performing their duties, in accordance with applicable federal, state, and local laws, as well as corporate policies and procedures. The audit manager and the CSO share information of mutual interest.
- *Legal Department*: This department is responsible for performing all common duties associated with any corporation's legal department, including providing advice and assistance to the CSO as requested or deemed appropriate.
- *Employee Relations*, *Human Resources Department*: This organization within the Human Resources Department, as the name implies, deals with employee issues such as employee complaints about their managers, providing guidance to managers relating to employee discipline.

The structure of IWC is no different from that of most other corporations. The corporate environment (or corporate office) differs from that of a business unit. The corporate environment has a strategic outlook, managing the overall business performance and strategy of the company. The focus is on the strategic direction of the enterprise, making the company profitable and producing shareholder value. The IWC corporate office generally does not

develop and deliver products and services. That is done by its business units, although they maybe co-located, as they are at IWC.

In support of its vision, a corporate office will establish the overall strategy for the company determining the type and scope of business. The corporate office will also develop policy, provide performance and compliance oversight, and exercise its fiduciary obligations to the board of directors and the shareholders. The corporate office usually does not get involved in the daily operations of a business unit. However, there are exceptions or conditions such as poor performance, at which time the corporate office will intervene in the operation of a business unit.

A business unit functions much differently from a corporate office. It operates in an environment where goods and services are designed, developed, produced, and delivered. It is a tactical operation in support of the company business strategy, and its day-to-day focus is on getting the product out. Typically, many different business units operate independently of each other and report to a corporate office (see Figure 8-1). Each business unit has different strategic objectives that fit into the overall company strategy.

IWC, like every company, regardless of size, has its own special culture. Some companies encourage competition between business units. Here rivalries as well as aggressive behavior are encouraged and rewarded. In other companies, teamwork is advocated. "Social scientists tell us that cultures are built upon behavioral 'norms' which are defined as a set of expectations on how people will behave in a given situation."[1] The culture of a company can differ between the corporate environment and the operations environment just as much as it differs between companies. Subcultures within an organization exist, which may differ significantly from the larger organization. Understanding the company culture is essential for a successful anti-fraud program.

IWC VISION, MISSION, AND QUALITY STATEMENTS

IWC requires that all those in IWC management perform certain management, albeit sometimes bureaucratic, tasks. Like many of today's modern corporations, IWC has developed vision, mission, and quality statements using a hierarchical process. IWC directed that the statements should link all levels in the management and organizational chain. The statements of the lower levels should be written and used to support the upper levels and vice versa.

---

[1] Golin, Mark, et al, "Secrets of Executive Success" (Emmaus, PA: Rodale Press), 1991.

Most employees seem to regard such "statements" as part of just another management task that is somehow supposed to help all employees understand their jobs — or whatever. However, these statements are often developed in "employee team meetings," get printed, are placed on walls, and are soon forgotten. Confidentially, many managers feel the same way, and that is probably why managers present them as just another task to be performed by or with employees.

This is unfortunate, for these statements are a good idea inasmuch as they set a direction and philosophy for everyone at IWC, at all organizational levels. When presented with the right attitude, they can be used to focus the employees on objectives and give them a better understanding of why they are there doing what they are doing. IWC's vision, mission, and quality statements are as follows:

Vision Statement

In many of today's businesses, management develops a vision statement. The vision statement is usually a short paragraph that attempts to set the strategic goal, objective, or direction of the company. IWC has a vision statement and requires all organizations to have statements based on the IWC corporate statements.

What Is a Vision? A vision statement is a short statement that is:

- is clear, concise, and understandable by the employees;
- is connected to ethics, values and behaviors;
- states where IWC wants to be (long term);
- sets the tone; and
- sets the direction for IWC

IWC's Vision Statement: *IWC's vision is to maintain its competitive advantage in the global marketplace by providing widgets to our customers when they want them, where they want them, and at a fair price.*

Mission Statement

Mission statements are declarations as to the purpose of a business or government agency.

IWC's Mission Statement: *Design, manufacture, and sell high-quality widgets, thereby expanding our global market shares while continuing to improve processes in order to meet customers' expectations.*

Quality Statement

Quality is what adds value to a corporation's products and services. It is what your internal and external customers expect from you.

IWC Quality Statement: *To provide quality widgets to our customers with zero defects by building it right the first time.*

PLANS

Plans are generally thought of as a logical series of tasks, functions, and thoughts written down in order to accomplish some future objective. In the case of IWC, it is like any small, medium, or large corporation. It has business plans, hiring plans, marketing plans, and the list goes on. The CSO also must develop plans to ensure that an IWC assets protection program and anti-fraud program can be successfully established and managed as part of its service and support to the corporation.

Since the SBP is a seven-year plan, the specifics of how to get there are not defined in sufficient detail to assist the CSO in also stating generalities. Keeping in mind the service and support functions and the "parasite on the profits" philosophy, the CSO's SBP statement related to this particular goal is as follows:

- *Establish and manage a cost-effective IWC Anti-Fraud Program that will provide the minimum amount of anti-fraud defenses conducive to an acceptable level of risk and thus contributing to the IWC goal of IWC 7% average annual profit increase for the next seven years.*

Remember that the Corporate Security Department goals must integrate into the Human Resources Department goals and SBP and then to IWC. This is part of the "balancing act" that a CSO must do as the IWC Security Department is under the Human Resources Department. Therefore, the goals must support the Human Resources goals. At the same time, the CSO is responsible for the IWC anti-fraud program for the entire corporation that is broader in scope than just Human Resources goals.

The CSO works in a world of office politics where often security is given a bad name. These goals help show that the CSO and the Corporate Security Department are "team players" and doing their part to support the IWC goals. As the CSO, also remember that if you do not agree with someone, they often say that you are not a "team player." This should be a warning to you to conform to someone's beliefs or be considered a possible adversary. If this comes from a peer, be wary. If it comes from your boss, be very concerned, and in fact, it is imperative that a one-on-one meeting be held to discuss the matter.

The real beauty of these two supporting IWC SBP goals is this: You come across, as you should, like a team player ready to sacrifice and do your part to meet the IWC goal.

Based on the minimum amount of anti-fraud defenses conducive to an acceptable level of risk is a key term. What is considered the acceptable level of risk is an *executive management decision* and should be based on risk analyses conducted by members of the Corporate Security Department in conjunction with various other IWC staff members who can contribute to the individual analyses.

The executive management's decisions relative to risk will include deciding which of the various options presented along with the value of the assets and their anti-fraud defensive costs versus risk should be implemented. Thus, the executive management's decisions are a factor in the cost of protection. Therefore, the CSO can fall back on the position that the executive management decisions assisted in whether or not the CSO met this SBP goal. In other words — "It's not my fault!" This approach is sometimes necessary in dealing in the world of office politics. It is sad but also a matter of survival. You must weigh the risks of using such a position if it becomes necessary. As the saying goes, "Damned if you do and damned if you don't."

The CSO should try to have the minimal amount of budget and staff conducive to getting the job done. The CSO should try to get performance and thus raises and bonuses tied more to successfully getting the job done at least cost consistent with the protection of the assets. The job of the CSO is challenging, but it can also be a fun job.

OTHER IWC PLANS AND CSO SUPPORT

Using the approach as discussed above, the CSO must integrate anti-fraud program SBP, TBP, and ABP goals into the CSO's assets protection goals, HR goals, and the IWC overall goals.

CASE STUDY

As the new CSO, how would you go about developing anti-fraud-related vision, mission, and quality statements?

One approach would be to:

- Identify the IWC statements.
- Identify the HR statements.

- Identify the previous Security Department statements.
- Develop anti-fraud-related statements that support the above statements.
  - Discuss the development of statements with your boss.
  - Establish a project team with selected members of the security department representing all the security department organizations to draft statements and coordinate them with all security department personnel for input.
  - Have the project team finalize statements.
  - Have the CSO modify as appropriate and approve the statements.
  - Submit the statements to the CSO's boss for approval.

SUMMARY

The reader can use the fictitious global corporation, IWC, to build an anti-fraud program.

Many corporations set their goals and objectives in planning documents such as strategic, tactical, and annual business plans. These plans are key documents for the CSO to read and use to determine the corporation's future directions.

These plans are also key documents that the CSO may be able to use to determine what is expected from the CSO and the anti-fraud program. The plans should also be used as the basis for writing service and support anti-fraud plans, as separate documents or as sections that are integrated into the identified corporate planning documents.

The decision process of the IWC executive management in determining which department the CSO and the corporate security organization belong to provides some key information that the CSO should use in establishing the anti-fraud program and related security organization. It helps identify potential "power plays" by managers and provides a glimpse at the corporate political environment.

The CSO must look at IWC from a global perspective and consider political, technological, economic, and global competitive factors, fraud-threat agents, and similar topics around the world. This broad scope is required when developing an anti-fraud program for IWC that will meet the worldwide needs of the IWC, now and into the future.

9

Establishing an Anti-Fraud Program

INTRODUCTION

With this chapter we begin what is the heart of this book: establishing and managing an anti-fraud program. The International Widget Corporation (IWC) will be used as the corporation for which an anti-fraud program is to be established and managed. If you are working for a corporation, you can of course substitute your corporation for IWC so that you can build a realistic model that works in your environment.

IWC's assets (i.e., people, facilities, information, and equipment) are valuable and must be consistently protected by all IWC employees, contracted personnel, associate companies, subcontractors — in fact, everyone who has authorized access to these assets. They must be protected regardless of the environment in which they are located, for example, in IWC facilities in foreign countries.

A corporate chief security officer (CSO) is responsible for ensuring that these assets are protected and does so by establishing and managing a formal assets protection program. Such a program must protect the corporate assets from the various threats, both national and international. As a subset of that program or as a standalone program, depending on the corporate culture and needs, is the anti-fraud program. For our purposes, such a program is a subset of the corporate assets protection program at IWC. (See Figure 9-1.)

In order to provide anti-fraud defenses and related protection measures, those individuals who have authorized access to the IWC assets must:

- Be aware of the details of the IWC anti-fraud program, at least as it applies to them.

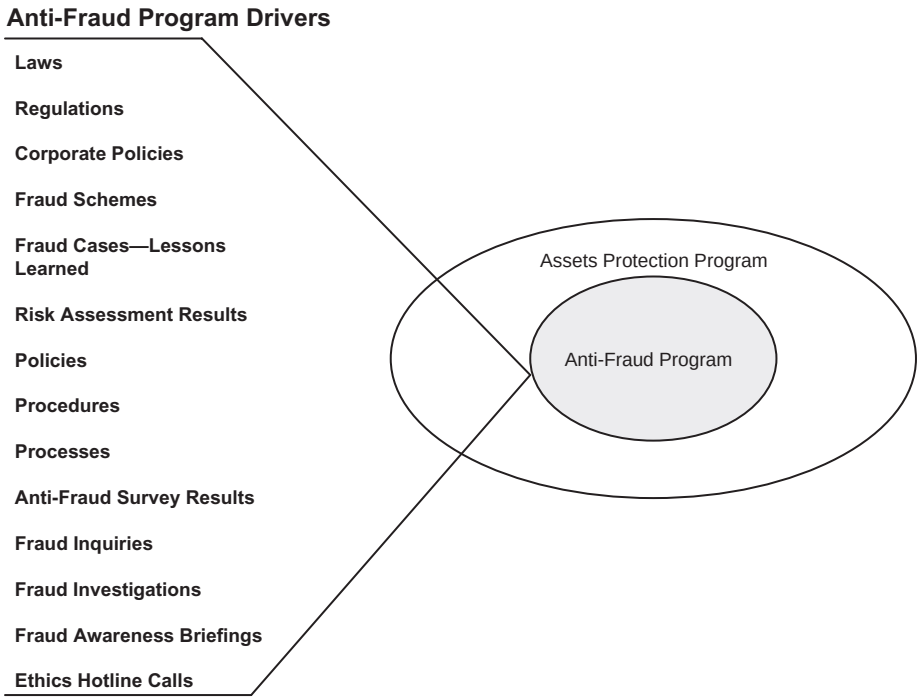


Figure 9-1. IWC assets protection and anti-fraud programs and what goes into them.

- Receive guidance as to the policies, procedures, processes, and plans relating to the anti-fraud program.
- Understand how to apply anti-fraud defensive measures.
- Understand why such anti-fraud measures are required.
- Understand at least basic fraud schemes.
- Know how to rapidly report potential fraud threat agent attacks and vulnerabilities.

When IWC's CSO decided that a policy document was needed, the IWC CSO drafted one for the IWC CEO to sign, after coordinating it with the VP of HR, for subsequent distribution to IWC employees and all others with access to IWC assets. It was also done to fulfill that requirement as stated in the IWC plans (e.g. IWC Strategic Business Plan).

The type of policy document that you as the CSO draft will depend on your corporate culture and the type of format that the CEO prefers to use. This format and "wording" can be found in other CEO-signed documents that were sent out to the IWC employees and also by discussing the draft with your boss and the CEO's secretary, who will know how the policy document should be worded for the CEO's signature.

It is imperative that the CEO state his or her support for the anti-fraud program and does so in writing. The difficulty is to have such a policy approved and made available to all employees, associates, and others without it seeming that such a program was necessary owing to the perception of "massive frauds" taking place within the corporation. As is true of most policy documents, office politics plays a very important role.

IWC'S ANTI-FRAUD PROGRAM

The CSO knew that, to successfully protect IWC's assets from fraud-threat agents, formal guidelines and directions had to be provided to the IWC employees. There also had to be some formal processes for ensuring that the IWC assets are protected from fraud-threat agents in an effective and efficient manner — in other words, "good and cheap."

It was obvious to IWC's management and the CSO that to do otherwise would cause employees to protect assets as they saw fit, or not protect them at all. Such was almost the case now at IWC, and the CSO knew that there was an urgent need to quickly establish an anti-fraud program based on the history at IWC of successful and unsuccessful attacks by fraud-threat agents.

The IWC anti-fraud program would be developed taking into consideration and/or incorporating:

- Reasons for the anti-fraud program, including its drivers such as laws and regulations.
- IWC vision, mission, and quality statements.
- Legal, ethical, and best business practices.
- IWC's strategic, tactical, and annual business plans.
- IWC's assets protection program to include its related strategic, tactical, and annual security plans, policies, and procedures as directed by the IWC CSO.
- The corporate security department's vision, mission, and quality statements.
- Current anti-fraud related policies, procedures, and processes.
- Other anti-fraud related documents.

The IWC anti-fraud program cannot be developed in a vacuum if it is to work. The input of others is a necessity as the program, if not done correctly, may adversely impact IWC's business. Remember that the CSO's security department and functions must be service and support driven. Furthermore, they are an overhead function; thus they take away from IWC's profit base.

As part of that endeavor, the anti-fraud program must be integrated into the IWC assets protection program and must support the IWC business

plans. It then follows that the plans call for certain actions to protect IWC's vital assets.

Remember what is being discussed here are the plans, processes, policies, and procedures that are established, implemented, and maintained (kept current) as they apply to all IWC departments. This should not be confused with the security department's internal plans, policies, and procedures (e.g., work instructions, processes, and such that apply strictly within the IWC security department).

As the CSO, one of your first tasks is to obtain a copy of the IWC assets protection program document (hopefully there is one). If none is available, should one be developed prior to developing an anti-fraud program as a subprogram to that assets protection program? At IWC, a formal assets protection program does exist.

Within your corporation, you may find that:

1. There is no such document.
2. The one now in use is not really current and needs updating.
3. To your shock and amazement, the IWC assets protection program documents are current and excellent.

Of the three options, which would you prefer and why? Actually, there are benefits to all the options. The one you choose will probably be based on where you are coming from and where you are going (e.g., your education, experience, and what you would like to see in such a plan).

Option number one has some benefits. If there is no such document as the IWC assets protection program by any name, one can "do it right the first time" and develop one that meets IWC's needs using your own tried and true methods. However, the less experience you have, the more difficult it will be to do it right the first time.

If you are new to the corporate CSO position, it may be doubly difficult and a real problem. No, not a problem, because you are now in a management position; therefore, these are not called problems. They are called "challenges."

Having an assets protection plan that has been approved by executive management has some benefits, of course. "Approve it?" you say. "Why does anyone have to approve it? I am the CSO, the security professional, the expert in the business. I know what I am doing. I don't need any non-security people out there playing amateur assets protection expert." That may have worked in the past, maybe in the times of the hunter-gatherer period, but not now. Teaming is now the latest approach in corporate management. One reason for that is of course so that no one is responsible and yet everyone is in it together and, therefore, all our responsible. "It's not my fault!", "We all agreed," and "It's not my responsibility!" are what generally follows when something goes wrong.

Here's the issue: as the CSO, you are going to establish an anti-fraud program that will impact everyone and everything in IWC in one form or

another, since the IWC assets permeate all levels of IWC and IWC cannot function without them. You are the new CSO at IWC and really don't have a good handle on how anti-fraud assets protection policies and procedures impact the IWC business of making widgets.

You may have a great way to protect a certain type or types of assets, but find that if it were implemented it would slow down production. That is not a good idea in the competitive, fast-paced, global marketplace in which IWC competes for business. That may get you a warning first but then fired (as was the case of the last CSO?), or it may increase costs in other ways (impeding employees' productivity is a cost matter also).

The second option also has some good advantages, especially for the CSO who has less experience in the profession and/or less experience at IWC. The advantage is that you have a framework on which to build. But as with option number one, some caution is advised, especially when building on that framework, basically changing it to how you envision the final assets protection program and anti-fraud program baselines.

Option number two allows you, as the new CSO, the opportunity to see what executive management has authorized to date. In other words, you know how much "protection" the executive management of IWC will allow at what expense to productivity, costs, and so forth. This will help you decide how to structure your anti-fraud program: you will not likely receive any additional budget to incorporate an anti-fraud program into the overall IWC assets protection program since IWC is continually looking for ways to save money and increase productivity.

If you increase assets protection defenses by adding a more formal and aggressive anti-fraud program, it must provide sound, convincing business reasons why that should happen. In this cause, you have an edge because of the previous loss of IWC assets to fraud-threat agents, which led in part to the firing of the former CSO. In addition, the CEO is supportive in that both the Strategic Business Plan (SBP) and Tactical Business Plan (TBP) have assets protection/anti-fraud goals, and those plans had to be approved by the CEO prior to implementation.

The CSO can make a case for the anti-fraud program as part of the "new and improved" assets protection program. Thus, the assets protection program already has high visibility and at least some executive management support. However, that "honeymoon" may not last long if you require protection mechanisms that are not backed by sound business sense.

Option number three is great if you are new to the CSO position and/or lack confidence or experience in assets protection and anti-fraud program development. However, caution is also needed here because IWC assets were lost and the former CSO was fired. The questions you must get answered are as follows:

- Did the assets protection processes — and for our purposes those specifically related to an anti-fraud program or lack thereof as set forth in the IWC assets protection program — leave a vulnerability or

vulnerabilities that allowed the fraud threat agents to take advantage of it?
- Was the assets protection or anti-fraud aspects of it not the issue but someone or a group failed to follow proper procedures?
- Was the CSO just not the right person for the job at IWC? (If this is the case, find out why so that you don't make the same mistake, assuming you want to work for IWC for more than a year or two.)

As the new CSO, you should get the answers to these questions and then determine the best way to integrate an anti-fraud program into the overall assets protection program for IWC. You of course want to determine whether the assets protection program can be modified and enhanced to mitigate future fraud-threat agent attacks. The benefit of a current assets protection program is that it has received the concurrence of executive management — but remember that it may be a bad plan. After all, what does executive management know of assets protection and anti-fraud matters except what the CSO tells them, aside from "common-sense" knowledge?

Let us assume that there is an IWC assets protection program but none of it addresses fraud-related matters such as fraud-threat agents and defending the assets against their schemes. Furthermore, it is not up to date.

So, the IWC must start from the beginning to build an anti-fraud program. Actually, that may not be entirely true. If you are an experienced CSO, you have brought knowledge and experience to the IWC CSO position, and that includes fighting frauds.

> There generally are some assets protection plans, policies, procedures, and processes that can be used to support an anti-fraud program or be modified to fit into an anti-fraud program.

It would be cost-effective if assets protection plans, policies, and processes can be used in part in building the anti-fraud program. It would be a more effective and efficient method to implement since the employees and others are already aware of how, at least in general, to protect IWC assets from general threats. It may just be a matter of gathering applicable plans, policies, procedures, projects, and processes together for analysis as part of establishing the anti-fraud program baseline.

In addition, over the years the IWC CSO has swapped and collected assets protection and anti-fraud plans from other security professionals that may prove useful. Several words of caution are in order:

- Never take another's assets protection program documents (or any documents) without approval of the appropriate corporate authority

because such plans may be considered and marked as corporate-confidential, corporate-private, corporate-proprietary, and the like. There is an ethics issue here.

- Remember that the other assets protection and anti-fraud plans may be outdated and/or not meet the needs of IWC (e.g., different corporate culture or environment).

ANTI-FRAUD PROGRAM PROJECT PLANNING

Using formal project management techniques, the CSO decided to establish an anti-fraud program project team. The CSO must either select a project lead, lead the team, or have the group select its own project lead. If the CSO's security organization has one or more staff members experienced in anti-fraud matters (e.g., Certified Fraud Examiner [CFE]), one of those specialists may be the natural one to head up the project team.

Other team members should include members within the IWC security organization who are responsible for each of the assets protection functions of the security organization — for example, investigator, assets protection education, and awareness specialist. Although someone who was a CFE may appear to be the best person to lead the project team, that also depends on the individual's leadership abilities, project management skills, interpersonal relations skills, knowledge of IWC office politics and culture, and the like. These qualities hold a higher priority in the project lead selection process than the credentials of just a CFE.

> One should not automatically assign the anti-fraud program project's leadership role to anyone who does not also have project management and leadership skills, which include the skills related to teaming with others to meet specified goals.

These team members would not be used full time on the project but represent the various security — assets protection — functions and provide input as deemed appropriate by the project team leader. If no one met the criteria for such an important position as the project leader, then the CSO may have to take on that responsibility.

Generally speaking, the CSO should not be taking on such jobs as the project will take time away from the overall duties of the CSO position. However, both the CSO and the entire security department's reputation will be positively or negatively affected by the results of this project and the eventual establishment and management of the IWC anti-fraud program. The IWC CSO, being new to the job, is especially busy with the normal CSO activities; however, the CSO may not have a choice, even though the

use of micro-management techniques should be avoided in all but under the most vital and necessary circumstances.

The IWC CSO decided to use only specialists from the security department at this time to speed up the draft of the baseline anti-fraud program's primary document — the document that contains the requirements, processes, plans, policies, and procedures. To do otherwise, for example, adding auditors, IT staff, human relations specialists, ethics specialists, legal staff, and so on, would invariably cause so much time in discussions and arguments over the relative restrictiveness of policies that the outcome could be a slowdown or committee analysis-paralysis. The CSO determined that coordination would be done upon security's finalization of the draft document.

Let's now assume that there is an overall IWC assets protection plan in place with outdated portions. The CSO, who has already read the document and does not agree with some of the requirements in it and sees other requirements that are obviously lacking, should first meet with the security specialists currently responsible for the assets protection program and the maintenance of the assets protection document and that person's manager. The assumption is that someone in the current security organization has responsibility for the assets protection program — or equivalent plan or program.

The main purpose of the meeting would be to determine why it is not current and discuss the rationale for all the requirements stated in the document. It may be that some portions were deleted due to executive management objections. These must be identified because it is of little use to update the plan and program if it is to meet resistance and rejection when it is briefed to and coordinated with executive management, unless the CSO strongly believes that some requirements should be added and makes a case for such changes to executive management.

The CSO must decide whether or not to:

- Update the overall IWC assets protection program to include its plans, policies, procedures, and processes and set the anti-fraud program aside until that is completed.
- Update the assets protection program and the anti-fraud program in parallel.
- Update the anti-fraud program as the highest priority while maintaining the overall assets protection program's status quo.

If you were the IWC CSO, what would you do?

If you decide to hold the anti-fraud program project in abeyance pending completion of the update of the assets protection program, you may find that the anti-fraud program may be delayed a year or more, or worse yet, you may never get to it due to the need to constantly update the overall assets protection program and related plans, policies, procedures, and processes.

Would this be prudent knowing that IWC has been the target and victim of fraud threat agents in the past and may still be a target of fraud-threat agents?

If you decide to do both as projects in parallel, would there be:

- Some chaos as a result of changes being made to the overall assets protection program which may impact the anti-fraud program while the anti-fraud program project team is working with outdated assets protection plan information?
- How much rework of the anti-fraud program would then be required later — for example, the anti-fraud program would be out of date as the assets protection program plans, policies, procedures, and processes were updated?

If you want to maintain the status quo of the assets protection program and develop the anti-fraud program, remember that vital aspects of the assets protection program would also apply to the anti-fraud program and such aspects may be outdated. Therefore, you would be building the initial anti-fraud program baseline on outdated assets protection program. Thus, the anti-fraud program would have to be updated as soon as the assets protection program was brought up to date. This may not only cause some confusion among those who have to comply with both programs, but may also incur additional costs. If nothing else, employees will incur costs in lost productivity as they learn the new policies, procedures, processes, and such that apply to how they protect the IWC assets from all miscreants, including the fraud-threat agents and their schemes.

The CSO has decided to establish two project teams and to work both projects in parallel. The other two options were considered as leaving the assets at too great a risk to all the various miscreants who may target one or more assets of IWC. Furthermore, since some of the assets protection criteria will also be used in the anti-fraud program, or at least have some influence on it, they both must be expedited and thus must be developed together.

If two project leaders and the team members have been identified, the CSO must be actively involved since there must be constant communication between the two project leads if both projects are to be successful. The CSO would do this by receiving periodic status reports from both project team leaders.

> The CSO must ensure that neither project leader operates in a "project vacuum," and they must share information on a regular basis — at least weekly. Neither can view their project as more important than the other's.

To begin the project, the CSO will explain the objectives of both projects at one of the CSO's regular security managers' meetings and again at one of the expanded staff meetings. The IWC CSO will also require that both project team leaders and project team staff members' managers brief the CSO on a weekly basis as to their progress, issues, and such.

Once the projects are well under way and appear to be going smoothly, at least as they relate to communications between the two project teams, the CSO may want to be briefed only every other week and then maybe once a month. It will all depend on the progress and lack of conflicts between the two project teams.

IWC ANTI-FRAUD PROGRAM PROJECT MANAGEMENT AND PLANNING

It is important to have a formal project plan to manage such a vital program. At IWC, the CSO and staff perform two basic types of work: (1) level of effort (LOE) and (2) projects. LOE is the day-to-day routine operations such as physical access control, awareness briefings, guard patrols, and investigations.

Projects are established in which some tasks related to the assets protection plan initial updates; in addition, the anti-fraud program project must be completed, but they are not ongoing tasks. It is imperative that the CSO, the CSO's managers, and the project leads be intimately familiar with and experienced in both project management and time management.

The IWC CSO has established a criterion as to whether or not some task or tasks should be a project. Projects must have:

- A stated objective (generally in one clear, concise, and complete sentence)
- A beginning date
- An ending date
- Specific tasks to be performed to successfully meet the objective
- A project leader
- Specific personnel to complete each task
- The stated date as to when each task will be completed

The IWC CSO has directed that a project plan be used to manage the anti-fraud program development, as well as the update assets project plan and program. Using Figure 9-2 as an example, let's develop a project and fill-in-the-blanks for major portions of the chart for an anti-fraud program:

> SUBJECT: The project name — for example, Anti-Fraud Program Development

SUBJECT: _____
RESPONSIBILITY: _____

ACTION ITEM: _____
REFERENCES : _____

● **OBJECTIVE(S)**

● **RISK/STATUS:**

	ACTIVITY/EVENT	RESPONSIBILITY	2002 Feb	Mar	Apr	May	Jun	Jul	RISK LVL	RISK DESCRIPTION
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Legend: Milestone ○ =Major Activity; Deviation Span; Scheduled; Complete

Risk Level: HIGH H; MEDIUM M; LOW L

PAGE 1 of 1

ISSUE DATE xxxxxxxx

STATUS DATE _____

Figure 9-2. Basic project management chart that can be used to track the anti-fraud development program tasks.

RESPONSIBILITY: The name of the project leader — John Doe, security specialist

ACTION ITEM: What is to be accomplished? — for example, A baseline IWC anti-fraud program is to be developed and integrated into the IWC assets protection program with processes in place to periodically update it.

REFERENCES: What caused this project to be initiated? For example: "See CSO memo, dated June 2, 2007."

OBJECTIVE(S): State the objective of the project: Develop an anti-fraud program that will effectively and efficiently protect IWC assets from fraud-threat agents and their schemes.

RISK/STATUS: State the risk of not meeting the objective(s) of this project: Due to limited staffing and multiple customer projects being supported, this project may experience delays as higher priority LOE and other projects take precedence.

ACTIVITY/EVENT: State the tasks to be performed — for example, meet weekly with project team members, review IWC policies.

RESPONSIBILITY: Identify the person responsible for each task. In this case, each team member's tasks would be identified.

CALENDAR: The calendar could be a year long, monthly, quarterly, or a six-month calendar with vertical lines identifying individual weeks. Using the six-month calendar, the Project Lead and assigned project team members would decide what tasks had to be accomplished to meet the objective and, using the "arrows" and "diamonds" identified in the legend, mark the beginning and ending dates of each task. The arrows are filled in when the task is started and when the task is completed, and the diamonds are used to show deviations from the original dates.

RISK — LVL: In this space, each task is associated with the potential risk that it may be delayed or cost more than allocated in the budget for the task. Using "High," "Medium," or "Low" or "H," "M," or "L," the Project Lead, in concert with the person responsible for the task, assigns a level of risk.

RISK — DESCRIPTION: A short description of the risk is stated in this block. If it requires a detailed explanation, that explanation is attached to the project plan. In this block the Project Lead, who is also responsible for ensuring that the project plan is updated weekly, states "See Attachment 1."

ISSUE DATE: The date the project began and the chart was initiated goes in this block.

STATUS DATE: The most current project chart date is placed here. This detail is important because anyone looking at the project chart will know how current it is and can compare it with the ISSUE DATE to determine how long the project has been in existence.

Other types of charts can also be developed to show project costs in terms of labor, materials, and the like. A good, automated project plan software program is well worth the costs for managing projects. As the CSO, you should check within IWC to see if an approved project management software product is available. If so, use it as it will meet IWC standards.

In the case of project charts, the CSO also uses them to brief management as part of the briefing to management relative to the ongoing work of the security organization. The CSO receives weekly updates on Friday mornings in meetings with all the CSO's project leaders where each project leader is given five minutes to explain the status of the projects. Basically, all the CSO requires is that the project leaders state the status of their projects. For example, "The Project is still on schedule" or "Task #2 will be delayed because the person assigned the task is out sick for a week; however, it is expected that the project completion date will not be delayed because of it."

The CSO holds an expanded staff meeting the last Friday of each month. (The CSO should be sure to have coffee and donuts available.) All assigned security personnel attend these meetings, which last two to three hours. At these meetings, one hour is taken for all project and security functional leads to brief the status of their LOE and projects to the entire staff. The CSO does this so that everyone in the organization knows what is going on — a vital communications tool. Also during this time, other matters are briefed and discussed, matters such as the latest risk management techniques, conferences, and training courses available.

ANTI-FRAUD PROGRAM PROJECT TEAM

The next step in developing an anti-fraud program is for the project leader to identify:

- Security staff members who should be on the project team
- Every major action that is to be taken, documented as individual tasks
- Individuals responsible for each task
- When each task will begin and end
- Any budgetary needs

The project leaders must get the CSO's approval prior to beginning the projects. The CSO requires this okay to ensure that all tasks are identified and that the CSO and security managers concur in the use of labor hours and other resources needed for the projects.

ANTI-FRAUD DRIVERS — THE FIRST MAJOR TASK IN ANTI-FRAUD PROGRAM DEVELOPMENT

An anti-fraud program, whether as part of an assets protection program or as a standalone program, is needed because of many factors or security drivers (see Figure 9-1). Security drivers are those factors that cause certain levels of assets protection, anti-fraud defensive measures, to be put in place at certain times. One of the major security drivers is, of course, threats to assets that try to "take advantage" of a security weakness or vulnerability to perpetrate a fraud, other crime, or IWC policy infraction.

The chance that an attack by a fraud-threat agent can take advantage of a security weakness or vulnerability is called a risk. The amount of anti-fraud defenses and related protective measures to be applied to specific corporate assets is determined. If it is determined correctly, it will be based on the amount of money, people, time, and other factors it would take to adequately protect the assets from these fraud miscreants, based on the assets' values.

Other security drivers include various laws, regulations, policies, frauds, fraud schemes, and the like that mandate that anti-fraud assets protection mechanisms be instituted. In other words, these factors are the primary reasons that an anti-fraud program is being developed.

So, a major task is to identify, in detail, all the drivers that cause the need for an anti-fraud program. Each driver should be linked to each anti-fraud defensive measure. This task should be performed graphically and also with supporting text as part of the anti-fraud program document or documents, to be included as part of any fraud awareness briefings and training. Such linkages make it easier for executive management and all employees to see the need for certain anti-fraud defensive measures. It also helps if the CSO is trying to justify additional budget that can be linked to required, specific defensive measures (e.g. Mandated by law or SEC regulation).

IWC ANTI-FRAUD PROGRAM REQUIREMENTS — POLICIES

In developing an anti-fraud program, one must first look at drivers and identify requirements that drive the formation of policies that lead to procedures, which turn into processes to be followed by all those having authorized access to the IWC assets.

> Remember that requirements are derived from "drivers," that is, those laws, regulations, common business practices, ethics, and the like on which the anti-fraud policies are based.

Anti-fraud policies are based not only on drivers but also on IWC policies, which is another type of anti-fraud requirements' driver. The policies are needed to comply with the requirements. The procedures are required to implement the policy, and the processes are steps that are followed to make up the procedures.

RISK ASSESSMENT — THE SECOND MAJOR TASK IN DEVELOPING AN ANTI-FRAUD PROGRAM

After the anti-fraud assets protection drivers and requirements are identified, and an overall anti-fraud IWC policy document is implemented, the next step is to answer the following questions:

- Are the assets being protected from fraud-threat agents as required by one or more drivers (e.g., laws and regulations)?

- How much risk is being incurred, for example, risk is low, high, moderate, or may a statistical measurement be used based on the anti-fraud defenses?
- How much does each of the anti-fraud defensive measures cost to implement and maintain?
- Are the protective measures adequate, more than adequate, or nonexistent?
- What project tasks are needed to provide adequate anti-fraud defenses?

These questions can be answered through the implementation of risk assessment tasks.

As is true for all assets protection needs, a risk assessment should be taken periodically to determine the specific requirements for protecting corporate assets from fraud-threat agents, to measure how well the assets are being protected, and to decide what must be done if they are not adequately protected. This step should be taken in order to provide the most objective look at the threats, vulnerabilities, and risks to corporate assets, as well as to depict the anti-fraud defenses (e.g., protection of these assets) as they relate to their value, cost of protection, and required anti-fraud protection specifications.

The approach that the anti-fraud program project team will use is to develop a risk assessment process to determine the threats, vulnerabilities, and risks to IWC assets posed by fraud-threat agents. Does this make sense? Actually, it may or may not.

We discussed the importance of the two project team leaders, assets protection plan update the assets protection program project, and the anti-fraud program project to communicate on a regular basis and share information. For example, the anti-fraud program project team may be spending valuable time (and time is money in the business world) developing and then conducting an anti-fraud program-related risk assessment. However, as part of the IWC assets protection program, that had already been done. The risk assessment methodology, processes, and so on have been standardized throughout the security department. Therefore, in the case of IWC, there is no need to waste valuable time and other resources by reinventing the "risk assessment wheel."

BASICS OF IWC'S RISK ASSESSMENT PROCESS

Remember that you as the IWC CSO and your security staff are responsible for leading an anti-fraud/assets protective effort, that is, protecting things and people that need protecting according to the requirements set forth by the government agencies and owners of the assets who are willing to pay for that protection. That is, of course, delegated by the owners to

management, who in turn delegate the work to the CSO. However, responsibility cannot be delegated away from management. They have final responsibility for safeguarding corporate assets, something that the CSOs often do not make management aware of, or at least not often enough.

as·set [á sèt] noun (plural as·sets)

1. somebody or something useful: somebody or something that is useful and contributes to the success of something
2. valuable thing: a property to which a value can be assigned

plural noun as·sets

1. owned items: the property that is owned by a particular person or organization
2. LAW seizable property: the property of a person that can be taken by law for the settlement of debts or that forms part of a dead person's estate
3. FINANCE balance sheet items: the items on a balance sheet that constitute the total value of an organization [mid-sixteenth century. Via Anglo-Norman assetz "sufficient goods" (to settle an estate) from, ultimately, Latin ad satis, literally "to sufficiency."][1]

The policies, procedures, and processes used to defend IWC assets against fraud threat agents are based on the amount of risk the owner or corporate management, having been delegated that responsibility, is willing to assume, which itself is usually based on the value the owner or management assigns to the assets and the adverse impact to the business if they were not available.

Fraud Threats + Vulnerabilities = Risk

To understand the fraud threats to corporate assets, it is important to view these threats as they relate to the entire process of risk management. Risk management is a much-maligned process that has been improperly used, not used at all, or, in some cases, the wrong methodology or input has been used under the wrong circumstances.

The CSO must understand the basic concepts related to fraud threats, for example, as discussed in Section I of this book, and their associated

[1] *Encarta® World English Dictionary* © & (P) 1999 Microsoft Corporation. All rights reserved. Developed for Microsoft by Bloomsbury Publishing Plc.

assets protection risks based on the weaknesses in the current protection systems or processes. The first thing the CSO must understand (relative to assets protection from fraud-threat agents[2]) is the specific threats against the assets of the corporation. Some threats may lead to fraud-threat agent attacks, and others to other forms of attacks. The threats in general will vary for a number of reasons, notably:

- *Corporate environment*: A corporate office in an urban setting in a run-down part of town inhabited by drug dealers, addicts, and prostitutes will be prone to experience more crime that may spill over to the corporate grounds. A corporation may want a "campus" setting and thus will have less physical security than is required.
- *Corporate culture*: The corporate culture may be one that considers every employee trustworthy and loyal, so no need is seen for "excessive" controls that smack of a "police state." This attitude, though admirable, is not realistic in most of today's societies. In this atmosphere there is little control on corporate assets.
- *Products*: Threats against corporations that cut down trees would be more at risk from environmentalists than a corporation that produces baby clothes.
- *Global visibility*: A corporation that is a major force in a nation-state and/or foreign nation-states tends to be the target of attack if the corporation's home nation-state is having political difficulties with the nation-state where the corporation has offices. For example, U.S. corporations in Indonesia may be at risk because of the United States' "war on terrorism," which Muslims in Indonesia may consider as anti-Islam.
- *Vulnerability of assets*: If the assets are perceived to be vulnerable or in fact are vulnerable, there may be more attacks against them. Whereas, if the assets are perceived to be very well protected, and in fact are very well protected, there will be fewer attacks, at least over time. Therefore, the risks to these assets posed by fraud-threat agent attacks may be reduced.

THREATS

As we discussed in Section I, fraud threats can take many forms, and the type of fraud-threat agents' attacks that occur is limited only by the attacker's imagination. The two basic types of threats that the CSO deals with can be categorized as either natural or man-made.

---

[2] This of course applies to all types of threats to corporate assets; however, for our purposes, we are focusing on the fraud-related aspects of assets protection.

> One ought never to turn one's back on a threatened danger and try to run away from it. If you do that, you will double the danger. But if you meet it promptly and without flinching, you will reduce the danger by half. — *Sir Winston Churchill*

NATURAL THREATS

Natural threats are those threats that are not man-made. They are called acts of God, acts of nature, and the like and include:

- Fires, such as those caused by lightning
- Floods, such as those caused by excessive rain
- Earthquakes, caused by movements of earth's plates
- Winds, as when they are caused by typhoons/hurricanes

Natural threats apply to assets protection in general. However, when it comes to frauds, they do not apply, for only humans can perpetrate frauds; nature cannot. One must also be aware, however, that in some instances a fraud is "supported" by nature; for example, as when one falsifies damage caused by a hurricane when filing an insurance claim. If the natural act (hurricane) did not occur, the opportunity to perpetrate this fraud does not exist.

> An act of nature can provide the environment that allows fraud-threat agents to take advantage of a disaster. For instance, consider the allegations of fraud after Hurricane Katrina in the United States.

MAN-MADE THREATS

Man-made threats are defined as all threats that were not caused by nature — therefore, by humans. Historical data and changes in the working environment may assist in foretelling future threat events. Crime, specifically fraud statistics from local law enforcement for the area where the corporation is located, may assist in determining the potential fraud threats to the corporate assets in that area.

The many Web sites on the Internet can also provide useful fraud-threat agent information, fraud schemes, and fraud cases. Remember that

due to technology fraud has gone global as never before, and a fraud-threat agent has the ability to attack your corporation at any place where there are corporate assets and from anywhere.

Frauds, like other crimes, can be accomplished either internally or externally. When the corporation is preparing to "downsize" the workforce, there is a better chance that disgruntled employees may want to "get even" with the corporation and therefore perpetrate frauds. These frauds can take many forms, as noted in our discussion of fraud schemes and fraud cases.

> Man-made threats are only limited by the imagination of the fraud threat agent (attacker).

As with most applications of assets protection, in developing your anti-fraud program, start with a common-sense approach and get more sophisticated after the basic anti-fraud defensive policies, procedures, plans, and processes have been installed, maintained in a current state of readiness, and periodically tested.

> **threat [thret] noun (plural threats)**
>
> 1. declaration of intent to cause harm: the expression of a deliberate intention to cause harm or pain
> 2. indication of something bad: a sign or danger that something undesirable is going to happen
>   • a threat of severe thunderstorms
> 3. somebody or something likely to cause harm: a person, animal, or thing likely to cause harm or pain
>   • The dog is no threat.
>
> [Old English þrēat "crowd, menace." Ultimately from an Indo-European word meaning "to press in," which is also the ancestor of English thrust and protrude.][3]

VULNERABILITIES

Remember that for purposes of our discussion, vulnerabilities are weaknesses in the anti-fraud policies, procedures, plans, or program that allow

[3] Ibid.

a fraud-threat agent to successfully perpetrate a fraud that adversely impacts the corporate assets.

> vulnerable [vúlnərəb'l] adjective
>
> 1. without adequate protection: open to emotional or physical danger or harm
> 2. MILITARY open to attack: exposed to an attack or possible damage
> 3. extremely susceptible: easily persuadable or liable to give in to temptation
> 4. physically or psychologically weak: unable to resist illness, debility, or failure
> 5. BRIDGE liable to increased stakes: liable to higher penalties as well as bonuses, having won one game of a rubber -[Early seventeenth century. From late Latin vulnerabilis, from vulnerare "to wound," from vulnus "wound, injury."][4]

One thing is certain, though: there will always — always — be vulnerabilities that allow a fraud agent to be successful. Although your goal is to eliminate all of them, your only hope is to mitigate the risks they pose.

There are no exceptions to this principle. If you believe otherwise, for example, that you have a fool-proof anti-fraud program in place, we have a nice palace in Iraq with a water view we would like to sell you.

RISKS

Risk management is a key part of both management's and CSO's responsibilities. Since there is no such thing as a perfect anti-fraud program, the CSO must look at assets protection, which incorporate anti-fraud defense mechanisms that provide filters and "security rings" around corporate assets. These filters and rings make it increasingly difficult for a fraud-threat agent to successfully use any fraud scheme to penetrate the anti-fraud defenses and successfully realize the fraud-threat agent's goals. The less sophisticated the fraud-threat agent is, the sooner the defrauder will be defeated by one of the anti-fraud defensive filters or rings.

ASSETS PROTECTION RISK ASSESSMENTS

The process of identifying risks to corporate assets, determining their magnitude, and identifying areas needing safeguards at IWC is called Assets

[4] *Encarta® World English Dictionary* © & (P) 1999 Microsoft Corporation. All rights reserved. Developed for Microsoft by Bloomsbury Publishing Plc.

Protection Risk Assessment (APRA). In other words, you are assessing the risk to a particular asset or group of assets, which can also be called the "target" since fraud-threat agents may consider them targets.

risk [risk] noun (plural risks)

1. chance of something going wrong: the danger that injury, damage, or loss will occur
2. somebody or something hazardous: somebody or something likely to cause injury, damage, or loss
3. INSURANCE chance of loss to insurer: the probability, amount, or type of possible loss incurred and covered by an insurer
4. FINANCE possibility of investment loss: the possibility of loss in an investment or speculation
5. statistical odds of danger: the statistical chance of danger from something, especially from the failure of an engineered system

transitive verb (past risked, past participle risked, present participle risk·ing, 3rd person present singular risks): (1) put something in danger: to place something valued in a position or situation where it could be damaged or lost, or exposed to damage or loss; (2) do something despite danger: to incur the chance of harm or loss by taking an action — [mid-seventeenth century. Via French risque from Italian rischo, from rischiare "to run into danger," of uncertain origin.][5]

APRA is a formal IWC security department process that evaluates the threats and vulnerabilities to determine the level of risk to corporate assets due to attacks by fraud-threat agents. Assessments are usually done through a qualitative or quantitative analysis, or a combination of the two. It is the measurement of risks.

- *Qualitative* analyses usually use the three categories of risk as high, medium, and low. It is an "educated best guess" based primarily on opinions of knowledgeable others gathered through interviews, review of historical records, conducting of tests, and the experiences of the people doing the assessment.
- *Quantitative* analyses usually use statistical sampling based on mathematical computations determining the probability of an adverse occurrence based primarily on historical data. It is still an "educated best guess" but is based primarily on statistical results.

[5] Ibid.

ASSETS PROTECTION RISK ANALYSES

Analyses of the risks, the countermeasures to mitigate those risks, and the cost-benefits associated with those risks make up the risk analyses process. Basically, it is risk assessment with the costs and benefits factors added.

> Vulnerabilities must be eliminated or mitigated or the risk of their exploitation must be knowingly accepted by management. The risks may be mitigated by application of additional protection measures, or management may choose to accept a risk for a limited duration or for a limited population of assets if there is some compelling reason.

DEVELOPING ANTI-FRAUD DEFENSES

Once the drivers and requirements are identified, anti-fraud policies are in place, and the appropriate levels of risk assessments are conducted, you can add to your "to do" list the task of developing the anti-fraud defenses.

The approach is often called "Defense-in-Depth" and is required for the adequate protection of corporate assets. The most common misconception is that protective devices and countermeasures once installed do not require additional steps to adequately protect the assets from fraud-threat agent attacks.

Any protective measures require constant maintenance and testing and are just a component of an effective anti-fraud defensive model. Additional components or layers should be considered as additions to provide an effective protection model within your corporation.

Using multiple layers in an anti-fraud defensive model or system is the most effective method of deterring attackers (fraud-threat agents). Every layer provides some protection, and the defeat of one layer may not lead to the compromise of your entire corporation's assets to fraud-threat agents. Each layer has some interdependence with other layers.

Can you identify cost-effective, anti-fraud mitigating factors relating to the various fraud schemes and threats? This identification is critical since the cost of protecting assets might be more than the value of the assets. Remember that the overprotection of corporate assets also adversely impacts the financial "bottom line" — the profits — as does underprotection.

Remember, too, that the corporate security department is usually an overhead cost to the corporation. It can be a "parasite on the profits" of the corporation. Therefore, it behooves the CSO to keep costs to the minimum

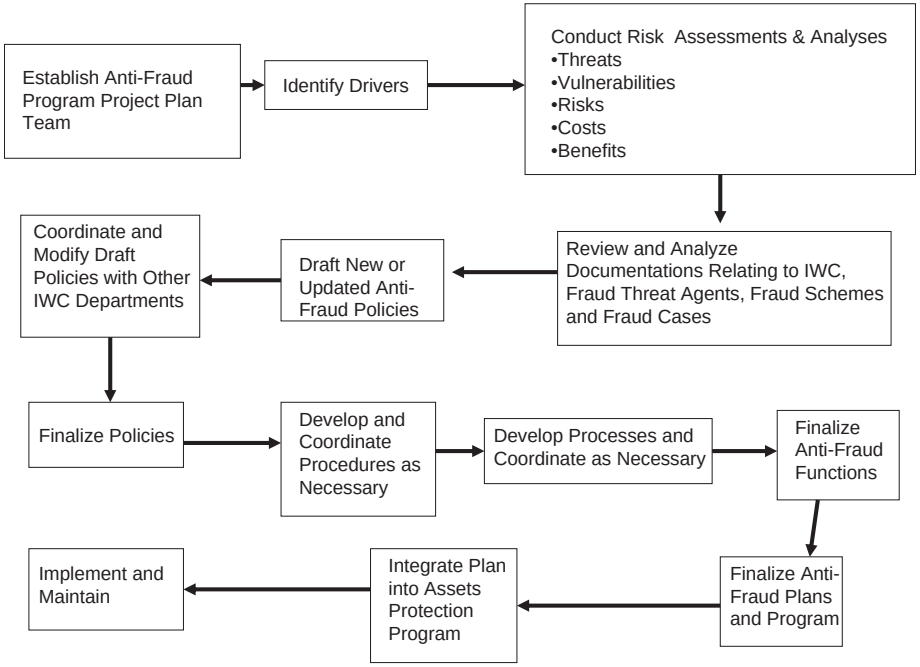


Figure 9-3. One example of the flow of tasks that go into developing an anti-fraud program for IWC.

required to meet the level of risk deemed appropriate by the corporation, thus contributing to the bottom line. If the anti-fraud defenses are properly applied as part of a well-thought-out anti-fraud program, they add value to the corporation because they protect the corporation's valuable assets. Not having some valuable assets available may reduce IWC's competitiveness in the global marketplace.

The anti-fraud or security drivers and requirements are used as part of an anti-fraud risk assessment program, which is then used to mitigate risks. The next step in the process is to use all that information to formulate new or updated anti-fraud policies, then procedures, then processes as part of the overall anti-fraud program for a corporation. (See Figure 9-3.)

THREE KEY INGREDIENTS IN AN ANTI-FRAUD PROGRAM'S DEFENSES

When developing an anti-fraud program, the CSO must remember that attacks against corporate assets by people require that three things must be in place, as often stated by the Association of Certified Fraud Examiners (ACFE) and criminologists. They are:

- Motive: If one is not motivated to violate rules, regulations, or laws relative to corporate assets, one would not do so even if the opportunity and rationalization to do so were present.
- Opportunity: If one did not have an opportunity, even though motivated and able to easily rationalize defrauding the corporation, one would not be able to perpetrate the crime.
- Rationalization: If one were to have the motive (being fired) and the opportunity (lack of verification processes and other controls on travel expense vouchers), one would commit the fraud, if the fraud-threat agent could rationalize it. Rationalization is important. Without rationalization how would one ever commit a crime? For example, we often see those who are loving family members and devoutly religious people perpetrate crimes. They would have been unable to do so without rationalizing it as not being a sin or a violation of their religious beliefs. In other words, one needs an "excuse" to perpetrate the act, such as: "After being loyal for over 20 years I am losing my job so that the corporation can save money, while the CEO gets a $100 million bonus."

Think about it and remember it. When you are developing your anti-fraud program, remember that your defenses (e.g., controls) should take away one, two, or all of the triad's "legs."

Fraud = Motive + Opportunity + Rationalization

IWC'S ANTI-FRAUD POLICIES

When discussing information assets protection policy, we define it as:

A codified set of principles that are directive in nature and that provide the baseline for the protection of corporate assets.

It is always the best policy to speak the truth, unless, of course, you are an exceptionally good liar. — *Jerome K. Jerome*

The corporate anti-fraud policies may be one document or a series of documents, depending on your corporate culture. To keep it simple, at IWC the CSO may want to have only one anti-fraud policy document, and from that all else, such as plans, programs, procedures, and processes, will be driven.

This policy makes up the most important portion of the anti-fraud program as it incorporates the anti-fraud "rules." It is the foundation of the IWC anti-fraud program. It is crucial that it:

- Cover all assets that must be protected from fraud threat agents.
- Cover all aspects of those assets' protection.
- Does not have any loopholes that could contribute to vulnerabilities.
- Be clearly written.
- Be concise.
- Take into account the costs of protection.
- Take into account the benefits of protection.
- Take into account the associated risks to the assets.
- Be coordinated with executive management and others as applicable.
- Be concurred with by executive management and others as applicable.
- Be *actively* supported by executive management and all employees.
- Include a statement relative to the process of maintaining its currency at all times.

One cannot state these requirements too strongly. They are the key to a successful anti-fraud program. If it is not stated in writing, it does not exist. After the assets protection and anti-fraud policy is established and approved in accordance with IWC requirements (executive management approval for all policies that affect the entire corporation), the information contained in the policy must be given to all corporate employees. This will be done through the IWC Security Education Awareness and Training Program (SEATP) and its communications process. (See Figure 9-4.)

A key process that the CSO must establish is one that will maintain all anti-fraud assets protection documents in a current state. Because this is a crucial function, the IWC CSO has assigned one staff member full-time to ensure that the policy and the entire anti-fraud program as documented are current at all times and ensure that when changes are considered, they are properly coordinated and the information is dispensed to all employees as soon as possible. The changes may just be procedural, or they may mitigate a fraud risk to some valuable IWC assets.

The CSO's focal point for the anti-fraud policy is informed of all actions, decisions, and other information that are gathered by the security organization staff and others, such as auditors. That information is analyzed and compared against this and other policies. When conflicts arise between events and the anti-fraud policy, they are analyzed to determine whether the policy must be updated. If so, then a process is implemented to do so.

If an event occurs that does not violate policy but obviously weakens the protection of an asset, a change in policy, procedure, or process is given

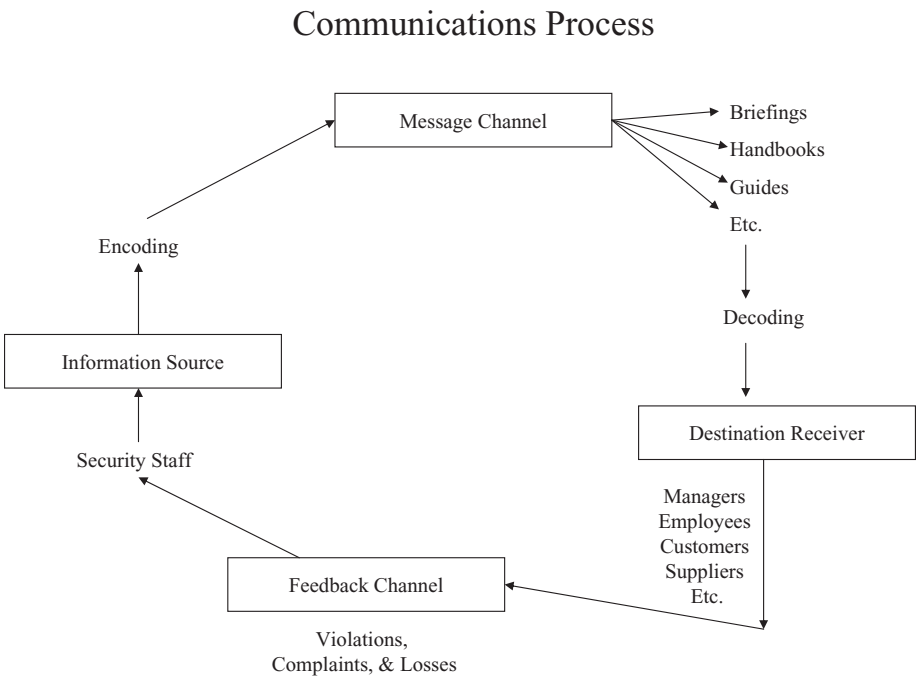


Figure 9-4. IWC SEATP communication loop process to be used for the anti-fraud program SEATP.

priority to eliminate that identified vulnerability based on costs, benefits, and risk. This would of course apply not only to the anti-fraud program but to the assets protection program as well.

An anti-fraud policy letter was issued to the IWC employees to begin setting the stage of the anti-fraud program. The letter, signed by the CSO, was as follows:

> *To: All IWC Employees*
>
> *Subject: Protecting IWC's Information Assets from Fraud-Threat Agents and Others in Order to Maintain Our Competitive Edge*
>
> *We are a leading international corporation in the manufacturing and sales of widgets. Today, we compete around the world in the global marketplace of fierce competition. In order to maintain a leadership position and grow, we depend first and foremost on all of you and provide you the resources to help you do your jobs to the best of your ability. You are vital to our success.*
>
> *It is the policy of IWC to protect all our vital assets that are the key to our success. You and these other vital IWC assets must be able to*

operate in a safe environment, and our other resources must be protected from loss, compromise, or other adverse effects that impact our ability to compete in the marketplace.

It is also IWC policy to depend on all of you to do your part to protect these valuable information-related assets in these volatile times.

The protection of our assets can only be accomplished through an effective and efficient assets protection program which incorporates an anti-fraud program. We have begun an aggressive effort to build such programs.

In order for the program to be successful, you must give it your full support. Your support is vital to ensure that IWC continues to grow and maintain its leadership role in the widget industry.

(Signed by the IWC President and CEO)

It is crucial that the CEO lead the way in the support of the IWC anti-fraud program. To get the above statement published is a major step in that process.

ANTI-FRAUD REQUIREMENTS AND POLICY DIRECTIVE

The IWC anti-fraud policy document will follow the standard format for IWC policies and include the following:

1. Introduction Section, which includes some history as to the need for an anti-fraud program at IWC.
2. Purpose Section, which describes why the document exists.
3. Scope Section, which defines the breadth of the Directive.
4. Responsibilities Section, which defines and identifies the responsibilities at all levels to include executive management, organizational managers, security staff, employees, associates, subcontractors, and suppliers.
5. Requirements Section, which includes the requirements for:
   A. Identification of the assets
   B. Access to the assets
   C. Applicable controls
   D. Audit trails and their review
   E. Reporting of responsibilities and action to be taken in the event of an indication of a possible violation
   F. Minimum anti-fraud defensive/protection requirements

G. Requirements for anti-fraud procedures to be written by all IWC departments based on complying with the anti-fraud policy

ANTI-FRAUD PROCEDURES

Over the years, the CSO has had experience in several corporations. The CSO learned that the best way to provide an updated anti-fraud program is to begin at the highest level and work down. This form of anti-fraud protection evaluation, analysis, and improvements is based on the fact that assets protection is driven and must be supported from the top down. Therefore, the CSO began with the overall IWC asset protection drivers and requirements, followed by the information assets protection policies. Once they were in place and the IWC employees were made aware of them, those related procedures already in place had to be analyzed, and project tasks had to be established to update them and develop new ones where needed.

Each anti-fraud procedure requires that it be written using the IWC standard method that supports the implemented anti-fraud policy, to include its spirit and intent. Some procedures may be written for everyone in IWC to follow, while various departments may write others based on their unique assets environment. Those procedures for everyone should be drafted by the anti-fraud project team and coordinated through the security department and all applicable IWC departments.

Various opinions have been voiced as to the best way to develop procedures because one continues to get to a more detailed level as one goes from drivers, requirements, and policies to procedures. The main issue is this: If the CSO establishes a specific procedure to comply with a specific policy, which in turn assists in meeting the IWC goals as stated in the SBP, TBP and ABP, the procedures may not be practical in one or another of the IWC departments. Thus, the department head may so state and ask for a waiver and state that they can still comply if they have a different procedure that takes into account their unique working environment. More than one department may have similar complaints. So, how does the CSO ensure that people are following proper anti-fraud policy and that the procedures to be written to comply with that policy are adequate?

The CSO has found that the best way to do this at IWC is to require that the individual departments establish, implement, and maintain their own set of anti-fraud and assets protection procedures that comply with the anti-fraud policy. This approach has several benefits:

- Each department's decision to write its own procedures helps enforce the philosophy that anti-fraud defenses, as well as assets protection, is everyone's responsibility.

- There will be fewer complaints and requests for waivers because one or more of the IWC departments cannot comply with the procedures as written by the CSO's staff. This benefits the CSO as tracking waivers may turn into a nightmare; for example, who has what waivers, why, and for how long?
- The departments can develop procedures that meet their unique conditions, and as a result, the procedures should be more cost-effective.
- The CSO and staff will save time and effort by not having to write and maintain anti-fraud procedures for all IWC departments. To be blunt — it's the department's problem. However, the CSO has offered to make security staff's anti-fraud specialists available to answer questions and to provide advice as to what should be in the procedures' documents. This was done in the spirit of providing service and support to the IWC employees.

The question then arises as to how will the CSO be sure that the procedures written by each department meet the spirit and intent of the anti-fraud policy? Two methods were identified:

- The security staff as part of their risk assessment and analyses processes will conduct limited fraud risk surveys and as part of those surveys, the procedures will be reviewed. The limited risk assessments and subsequent analyses will provide an indication has to how well the procedures in place help protect IWC assets under the control of each department and/or suborganization from fraud-threat agents.
- IWC's audit staff will compare the procedures with the policies during their routine audits. The director of audits agreed to conduct such reviews since they are responsible for auditing for compliance with federal, state, and local laws and regulations and IWC policies and procedures anyway. It also helped that after the CSO's arrival, the CSO and director met and agreed to monthly meetings to share information of mutual concern. The CSO learned long ago that security personnel have very few true supporters in helping them to get the job done, but auditors were one of them.

Procedures, along with their related processes, are the heart of an anti-fraud program because they provide the step-by-step approach showing employees how to do their work and they also ensure the protection of corporate assets from fraud-threat agents. And if it can be done by the departments writing their own anti-fraud and assets protection procedures, it gets them actively involved as valuable team members in the process of protecting IWC's valuable assets.

THE CSO AND SECURITY DEPARTMENT'S ANTI-FRAUD ACCOUNTABILITIES

The CSO and the anti-fraud project team have come up with a set of responsibilities to which the CSO and security department staff will be held accountable vis-à-vis anti-fraud matters. They are as follows:

1. Identify all anti-fraud requirements needed and develop IWC policies and applicable procedures necessary to ensure conformance to those requirements.
2. Evaluate all anti-fraud defensive measures through risk assessments, analyses, and fraud surveys; cause changes to be made when and where applicable.
3. Establish and administer an anti-fraud program to protect IWC assets from fraud-threat agents.
4. Establish, implement, and maintain a process to identify fraud threats and mitigate those threats to IWC assets in a cost-effective manner as part of the anti-fraud program maintenance efforts.
5. Establish and maintain an anti-fraud awareness program, supported by policy, procedures, and processes to ensure that IWC management, employees, and others who have access to IWC assets are aware of the IWC anti-fraud program requirements for the protection of IWC assets, the fraud-threat agents schemes, how to defend the IWC assets against them, and such.

OFF-SITE CORPORATE FACILITIES

The IWC CSO is also the acting manager of the off-site anti-fraud program subordinate organizations. However, the CSO has also determined that it will be necessary to appoint a person as a supervisor to manage the day-to-day operations of the off-site anti-fraud program. At the same time, there were not enough personnel, as stated by HR, to appoint a manager at the off-site locations. However, the supervisor has authority to make decisions related to that activity, with several exceptions. The supervisor cannot counsel the security staff, evaluate their performance (except to provide input to the anti-fraud manager), make new anti-fraud policy, or manage budgets.

RECRUITING ANTI-FRAUD PROFESSIONALS

Once the CSO has gotten the anti-fraud project team started, the CSO adds another task to the project plan, which is to develop criteria for one or more fraud specialists to be subsequently identified and hired as the secu-

rity department's focal point for all fraud-related matters. The CSO viewed this position as the "in-house fraud consultant" to the security department and IWC in general as part of the CSO's view of the security department as being service and support driven.

The CSO's anti-fraud project team must determine the following:

- How many anti-fraud professionals are needed?
- What functions will they perform?
- How many are needed in each function?
- How many are needed in which pay grades?
- How many should be recruited for the off-site locations?
- Does the off-site locations or main plant have the highest priority?

Once these questions are answered with supporting documentation and approved by the CSO, the CSO should then work with the CSO's boss. If approved by the boss, the CSO should then contact the IWC Human Resources staff to justify the additional staffing and budget and advertise for the hiring to fill that position.

The first choice should be to hire from within IWC, but only if the person meets the requirements. If not, then someone from outside IWC, who of course meets the criteria, would be hired. The advantage of hiring from within is that the employee already knows IWC culture, how things operate, and the like. Furthermore, it may even be a promotion for the applicant, which is always good for morale since other employees can see that they can advance within IWC and have new challenges, expand or change their careers, and so forth.

While all this seems really great, the main problem is that the boss will probably say that the CSO must work within the security department's budget because no additional budget or resources will be made available owing to budget constraints and ongoing layoffs of employees.

What would you as the IWC CSO do under these circumstances?

CASE STUDY

Based on the lack of budget and inability to hire even one additional staff member to be the focal point for anti-fraud matters within IWC's security department, the CSO decided to:

- Compare the fraud specialist criteria developed by the anti-fraud project team as approved by the CSO with the personnel files of each member of the security staff.
- Choose the security staff members who best meet the criteria for the anti-fraud specialist position.

- Contact the candidates' security manager and discuss the candidates' suitability for such a position based on the candidates' individual personality, education, experience, attitude, and such.
- Contact the top potential candidates to determine whether or not they would be interested in such a position.
- If more than one candidate is interested and only one position is available, convene a security managers' board to interview the candidates one at a time, posing a series of fraud-related questions.
- Choose the best candidate for the position.
- If more than one position is available, use the same approach as for one position.
- In coordination with the new anti-fraud specialist and the specialist's manager, the CSO should then develop a training program for the specialist and begin the process of getting the specialist totally qualified as a fraud specialist.
- The new specialist is also added to the anti-fraud project team, or based on the project lead position criteria, is made the anti-fraud program project team leader.

SUMMARY

In today's global marketplace where many corporations conduct business, corporate assets are bombarded by fraud threats to these assets from inside and outside the corporation. The workplace of the modern corporation in today's "what's in it for me" environment has changed over the years, as have the societies in which the corporations operate. With the ever-increasing role and dependency on technology, the threats to corporate assets have never been greater.

The information related to threats, vulnerabilities, and risks as presented in this chapter has been presented in various ways, but a central theme has been used: that all successful anti-fraud programs focus on the drivers, management of risks, policies, procedures, plans, processes, and fraud awareness briefings and training material.

This new era offers increased challenges to the CSO who must develop and manage a cost-effective anti-fraud program. To successfully accomplish that objective, the CSO must understand the threats, vulnerabilities, and risks to the corporate assets presented by fraud schemes, and the CSO must be familiar with fraud cases. These risks must be managed in a cost-effective manner that provides the minimal amount of anti-fraud defenses needed based on the assessed and acceptable risks.

10

Managing an Anti-Fraud Program

INTRODUCTION

No matter what job the CSO has with regard to protecting corporate assets, there are some elements of the CSO position that permeate all aspects of that job, as well as the job of any corporate manager. It is important that the CSO management and leadership aspects be discussed because they are an integral part of the CSO's responsibilities vis-à-vis protecting corporate assets and leading the anti-fraud program efforts.[1]

As the new IWC CSO, you have an identifiable management style. Over the years, hopefully you have honed your skills and CSO "personality" so that you can provide success and professional security leadership and management to IWC and your security staff. Some of the areas that a CSO should concentrate on and continue to learn more about are the following:

- Leadership
- Management
- Customer expectations
- Dealing with executive management
- Dealing with peers
- Dealing with office politics
- Representing IWC in the community
- Managing an effective and efficient security department
- Focusing on an industry model of security duties and responsibilities
- Dealing with the news media

[1] Some portions of this chapter were excerpted from the book *The Manager's Handbook for Corporate Security* (Kovacich and Halibozek), published by Butterworth-Heinemann, Elsevier (2003), and used here with permission.

CSO LEADERSHIP

As the CSO, you are the senior security executive within IWC. It is your responsibility to align the security organization to support the corporate objectives, concentrating on those objectives identified in the IWC business plans. In essence, you should create a professional security organization that follows and supports the established corporate objectives while providing protection to the corporate assets (e.g., people, information, equipment, and facilities). One of your goals is to create a vision for the security organization that is congruent with IWC's vision. Remember that the CSO, as the functional leader, also sets the security organization's direction.

> Lead, follow, or get out of the way.[2]

As a service organization, security must find ways to deliver assets protection, that is, anti-fraud services, that least interfere with or impact daily business. Simply stated, one should act as an enabler, work toward achieving company goals and objectives, and find ways to say "yes." This is not always easy to accomplish. Sometimes principles of good security practices will conflict with how people want to conduct business.

Security is sometimes seen as getting in the way of doing business. What executive management expects from a security organization is to integrate its assets protection services into company operations in such a way as to not interfere with operations while providing a sufficient level of assets protection. What executive management does not need or want is a security function that says "no" or "you can't do that."

Always remember that there is always more than one way to accomplish anti-fraud, assets protection functions, with some requiring accepting more risks than others. A successful CSO is one who finds ways to integrate protective measures as seamlessly as possible into the corporation's operation and who can add value to the security department and corporation. Also remember: *where there is a need, there is a waiver.* That is, sometimes there are valid and logical exceptions to the rules.

As the CSO, you must set the tone for the anti-fraud program and your security organization. You lead in part by establishing the nature of the anti-fraud program and the security organization by defining what is important and how they will operate. You are the link between the anti-fraud program and executive management. You must ensure that the anti-fraud functions operate in alignment with corporate norms and values.

---

[2] Author unknown.

MANAGEMENT VERSUS LEADERSHIP

> Effective leadership is putting first things first. Effective management is discipline, carrying it out. — *Stephen Covey*
>
> The very essence of leadership is that you have to have a vision. — *Theodore Hesburgh*

Management focuses on getting today's work done today while leaders look to tomorrow. The focus of management is much shorter than the focus of leaders. Having a clear and communicated vision is essential for any leader. If you expect people to follow, you must offer them a sense of direction. Followers need to know where they are going. As a leader, your vision must be clear, easily and regularly communicated, and shared. Leaders with followers sharing their vision stand a much greater chance of success than leaders with followers who do not share their vision.

Getting employees to share your vision will require you to develop their trust. The first task of leadership is to convince followers of your credibility. They must trust you. Developing their trust will require you to do what you say you will do. Be consistent in what you do, and do not stray from your values.

Without followers, no one is a leader. These management and leadership methods must be incorporated into your anti-fraud program if it is to be a success.

As part of a series of executive seminars conducted at Santa Clara University in California by the Tom Peters Group, more than 5,200 senior managers were asked to identify the characteristics they most admire in a leader.[3] These are the qualities they listed:

- Honest
- Competent
- Forward-looking
- Inspiring
- Intelligent
- Fair-minded
- Broad-minded
- Courageous
- Straightforward
- Imaginative

---

[3] Golin, Mark, et al, "Secrets of Executive Success" (Emmaus, PA: Rodale Press), 1991

As important as it is for employees to know and trust their leader, it is just as important for a leader to know and trust their employees. Knowing them and the organization will better enable you as the CSO to develop a connection. Being connected with your employees increases the chance they will share your vision. It also allows you to challenge them to perform beyond their own expectations.

> When developing and implementing the IWC anti-fraud program, it is imperative that some level of employee trust be considered while at the same time balancing that philosophy with incorporating anti-fraud defenses where you actually consider that people within IWC or associated with IWC cannot be trusted.

Why is good leadership important for a security department and the anti-fraud program? As is true of any other function within IWC, to perform well security must have an effective leader. This leader must know and understand the mission, objectives, and values of the company. You as the CSO are that leader, and you must be able to effectively communicate with your security staff the direction and vision for the security organization and the anti-fraud program in such a way as to best support the IWC's mission and objectives. Furthermore, you must lead the effort to develop security organizational goals that incorporate anti-fraud program objectives and that are designed and implemented to support IWC business goals.

MEETING CUSTOMERS' EXPECTATIONS

Security is a service and support organization, as well as a compliance organization. The service and support aspect of security has a set of customers that differ from the compliance customers. Yet, there is some overlap and commonality. Compliance customers expect the security organization to maintain an environment that is compliant with all applicable laws, regulations, contract provisions, and company policy, including those related to the anti-fraud program.

The service and support aspects of security involve those tasks performed in support of other employees and functions but are not required by policy and procedure, code, regulation, and law. Service customers expect the delivery of security services to be timely and efficient. They also expect their needs to be met promptly and to their satisfaction. These customers can be further defined as internal and external.

IWC INTERNAL CUSTOMERS

As the IWC CSO, IWC management is your primary customer for the compliance aspects of an anti-fraud program. Employees are your primary service customers, and they have varying expectations. Management looks to security to ensure that programs and processes are in place that will enable the organization to achieve and maintain compliance with regulation, contracts, laws, and policy. In a way, this is the fiduciary responsibility of security. Furthermore, management expects compliance to be achieved and maintained in a cost-effective manner. Management also expects security to create and sustain a secure environment. The workplace must be an environment where people, physical assets, and information are appropriately protected from fraud-threat agents and other threat agents — a safe and secure place to work.

IWC employees expect security services to be delivered efficiently and seamlessly, causing minimal impact or disruption to their daily work. For example, in the process of accounting, anti-fraud defenses must be in place. However, your customers expect to be able to do their accounting tasks efficiently and effectively with no loss of productivity due to the anti-fraud defenses integrated into their work processes. Delays due to such defenses will be met with resistance and frustration. Furthermore, any time lost as a result of an inefficient anti-fraud process is time not available for other productive activities. Remember the old adage, "time is money."

Other customers may be people who permanently reside on your facility but are representatives of the companies or people who purchase the products and/or services IWC produces and buys, or they may have a long-term business relationship with IWC.

By virtue of their location on IWC property, you should provide some type of anti-fraud service and support for these customers. IWC management must decide how to treat these internal or external customers, and it is up to you to classify them and treat them as IWC looks at them and would like them treated.

IWC EXTERNAL CUSTOMERS

These customers fall into many categories. Although they are not IWC employees, they do have a relationship with, or an interest in, IWC. They may be customers who purchase products and services; they may be suppliers who provide goods and services to IWC; or they may be vendors or contract labor personnel who perform work for IWC but are not IWC employees.

External customers may also be regulatory agencies responsible for ensuring compliance with anti-fraud regulations and laws. An example of

a regulatory agency customer is the U.S. Securities and Exchange Commission (SEC).

Depending on their relationship with IWC, the type and degree of customer interests in your anti-fraud program vary. For example, contract labor personnel are interested in working in a safe and secure environment; the SEC is interested in ensuring that IWC is compliant with all applicable federal laws and regulations.

IWC EXECUTIVE MANAGEMENT EXPECTATIONS OF A CSO

Executive management is responsible for assets protection. Like every other aspect of the business, executive management holds the ultimate accountability and responsibility for security. Consequently, they have a vested interest in a successful anti-fraud program — or they should. However, sometimes the CSO must "gently" remind them of that fact. How executive management defines a successful anti-fraud program may differ significantly from how a security professional defines one.

As security professionals, we tend to want to have the best program we can. After all, this is our area of expertise. We want to be compliant in all aspects of our compliance obligations. We also tend to employ as many controls as practical to ensure that the risk to corporate people, physical assets, and information is minimal. In essence, it is important to create an environment that is more risk-averse than risk management. Therefore, as a CSO you may generally be willing to accept fewer security risks than executive management.

Executive management is interested in having a cost-effective anti-fraud program, seeking to achieve an acceptable level of compliance cost-effectively.

Security at IWC, like security at most corporations, is a cost center; it generally is not a revenue-producing organization. That is not to say security does not add value to IWC. Security does add value to IWC. The challenge for you as the IWC CSO is to apply the appropriate levels of anti-fraud defenses and "prove" to executive management and others at IWC that the IWC anti-fraud program does add value to IWC products and services.

A very senior executive in a Fortune 500 company once characterized a successful security program by using a scale of red, yellow, green, and blue (blue being the very best and red being unsatisfactory); the successful program was one that operated in a light green environment. What he meant was that he wanted a program that kept the corporation compliant with laws and regulations; maintained a secure environment for the protection of people, physical assets, and information; and did so at

minimal cost. In this executive's opinion, monies spent on obtaining and maintaining a security condition that was green or better was bad for business.

Based on this acceptable level of security risk, any monies spent on security taking the assets protection program beyond that "light green" condition could have been better spent in other areas of the business such as engineering, product development, or marketing. Obtaining and maintaining this condition is a challenge that virtually all security professionals face, and that is the battle for funding.

As the CSO, you must ask and answer many questions relating to anti-fraud programs, including:

- How many anti-fraud defenses are enough?
- When are the physical assets, people, and information of the company effectively protected from fraud-threat agents?
- What are the fraud risks and defensive vulnerabilities for the IWC operating environment?
- How are resources best employed to achieve an acceptable level of risk?
- What tools and processes are needed to ensure an appropriately anti-fraud defensive environment?

Executive management may ask you these and similar questions. You must anticipate their questions and be prepared to offer specific, well-thought-out answers. The more you can respond immediately, not only with answers but also answers from a business application point of view, the more confidence they will instill in you and the more support you will be able to receive from them. In other words, talk their language when addressing their anti-fraud program concerns and always consider business impacts.

Of course, there may be some that you can never convince or win over; however, as long as they are the small minority, you can expect to receive support and understanding from executive management. As you progress in developing the IWC anti-fraud program, you should make it your personal goal to understand those who oppose you and what you are trying to accomplish. Furthermore, instead of avoiding them, thus building up more animosity, you should spend more time with them.

You will find that if they do begin to agree with what you are doing, they will become some of your staunchest supporters. There is nothing more rewarding than winning over an "adversary." As a leader and professional security manager, this offers some of the best personal rewards and demonstrates that you are perfecting your craft. Keep a "win and lost" record and view these efforts as an enjoyable game. If you are "batting" at or less than 50%, it is suggested that you change that record or be sure to keep a resume updated.

A CSO does not welcome adversity but cannot shy away from it either. Adversity and the challenges that come with it are a major part of what a CSO deals with everyday. If you can't handle it, and in fact don't enjoy the opportunities it brings, change careers.

Remember that, as a CSO, you are responsible for leading and managing the security department and the anti-fraud program. One of your objectives is to achieve and maintain a secure and compliant environment. For this, you are accountable to executive management. It is your responsibility to work with executive management to define an acceptable level of risk, a risk level that you should establish only after fraud threats and vulnerabilities to fraud-threat agent attacks have been identified, validated, and analyzed.

For this process, you must rely on your security staff and other anti-fraud team members such as auditors. (More information on teaming is presented in Chapter 11.) Don't forget that what your staff does reflects directly on you and that they also have occasions to interface with all levels of IWC management. Therefore, you must ensure that they are professionals in their conduct and apply anti-fraud defensive principles consistent with the philosophy of the IWC anti-fraud program. Remember, too, that there are many informal and formal communication channels available to executive management. Thus, what they hear from others about you and your staff has a direct bearing on the support and confidence they have in you.

MANAGING RISK

The *minimum* amount of anti-fraud defensive measures conducive to an *acceptable level of risk* are key terms. The acceptable level of risk is an *executive management decision* and should be based on risk analyses conducted by members of your security department in conjunction with various other IWC staff members who can contribute to the individual analyses.

The executive management's decisions relative to risk will include deciding which of the various options presented, along with the value of the assets and their protection costs versus risks, should be implemented. Thus, the executive management's decisions are a factor in the cost of protection. As their "in-house, anti-fraud consultant," you of course should guide them and make recommendations to help them in their decision-making function.

The CSO should always look at how the job can be done more efficiently. In many corporations, promotions and the amount of salary with

benefits that are provided the CSO has to do with the amount of the security staff, the size of the budget, and where in the bureaucracy the CSO reports. The CSO should try to have the minimal amount of budget and staff conducive to getting the job done as stated by executive management, even though you are adding a major anti-fraud program to the integrated assets protection program. Try to get your performance and position grade based on results and impact on IWC rather than on the amount of budget or the number of staff you have.

SECURITY'S VISION, MISSION, AND QUALITY STATEMENTS

As the CSO you are required, as part of the IWC management team, to develop vision, mission, and quality statements that help set the direction for the security department. The statements must support the vision, mission, and quality statements of the Human Resources Department, which in turn support the IWC statements. The CSO, in concert with the security staff, came up with the following statements relative to the anti-fraud program:

- IWC's Security Department Vision Statement: *In partnership with our customers, provide a competitive advantage for the IWC widget business by continuous protection of all IWC's assets from fraud-threat agents and other miscreants without hindering productivity and cost-effectively support increased production of IWC widgets.*
- IWC's Security Department's Mission Statement: *The mission of IWC's Security Department is to provide low-cost, productivity-enhanced assets protection services and support that will assist in defending IWC from fraud-threat agents and other miscreants while helping IWC to maintain its competitive advantage in the global marketplace.*
- IWC's Security Department's Quality Statement: *To provide quality anti-fraud support and services while enhancing the productivity opportunities of the IWC workforce.*

MANAGING THE IWC ANTI-FRAUD PROGRAM

Let's look at the CSO as a manager of the various aspects of the job, including planning, controlling, and budgeting.

PLANNING

Security serves the corporation. An effective IWC security organization that meets the protection, compliance, and service needs of employees,

management, and customers cannot be established and maintained independently of the rest of the company. Security is a key component of the IWC business and must be part of the planning process. Beginning with company goals, which are usually identified in multiyear plans or annual business plans, the CSM and security staff must be part of the planning process. The plans and objectives of IWC identify the path that IWC will take to achieve its goals and mission and to satisfy its shareholders and stakeholders. Obviously, IWC's anti-fraud program is incorporated into the planning function.

In the process, the IWE CSO must determine what management intended to achieve when they wanted to be made safe from fraud-threat agents:

- Are there specific fraud issues and concerns?
- What fraud incidents occurred in the past?
- What are the vulnerabilities of, and fraud threats to, IWC?
- What anti-fraud plans, policies, procedures, processes, and projects should be implemented?
- What level of risk is management willing to accept?
- How do you know when you have achieved your anti-fraud goals?

These are just some of the questions that the CSO should ask to be able to effectively plan, and then execute, that plan in support of corporate goals.

Since IWC is in business to make a profit for shareholders, a great amount of planning is focused on directing and growing the IWC widget business. Strategic planning groups conduct market, product, economic, and competitive assessments with the intent of finding opportunities for business growth and understanding customers, competition, and threats. Security needs to be part of this process in order to plan for supporting it.

Establishing and managing an anti-fraud program for IWC is part of those service and support duties and responsibilities. For example: if the strategic planning group identifies a high potential market opportunity for a joint manufacturing venture in a foreign country where fraud runs rampant, are there any issues that should be of concern? Clearly, the answer is yes, and some issues are quite fundamental:

- What is the crime or fraud rate in that country?
- Are there risks due to political instability?
- What fraud-threat agents are unique to that country?
- How much will you be able to rely on that country's law enforcement and security agencies to support IWC's anti-fraud program?

These questions are best addressed during the anti-fraud program planning stage. Waiting until after the operation is up and running may very well be too late.

The cost of correcting a problem is generally more expensive than the cost of preventing one.

SOME ASPECTS TO INCORPORATE INTO AN ANTI-FRAUD PROGRAM PLAN

Establishing an effective and efficient anti-fraud function within the IWC security department will require some analysis. Furthermore, it may require selling the need for a staff to perform that function, as was discussed in the previous chapter.

Even if you have been specifically hired to establish an IWC anti-fraud program, you will still be expected to define to management the size and scope of such a program and its related functions, including its costs and impacts on employee productivity. As part of your analysis, you should consider the following:

- *Define your Statement of Work (SOW).* Determine what needs to be protected from fraud-threat agents, for now in general terms or groupings and later in specific detail. You must also determine the amount of protection needed. To do so, you need to understand executive management's general expectations of the IWC anti-fraud program:
  - What does executive management believe needs to be protected?
  - Does it have special fraud-related requirements or concerns?
- *Determine if your customers have any anti-fraud and related assets protection requirements.*
  - Are you contractually bound to provide specific types of anti-fraud defenses?
  - If so, what is the scope of those requirements?
  - What, if anything, do your internal and external customers expect from you, the anti-fraud program, and your related services and support?

You may also want the opinion of an outside anti-fraud specialist — someone who has no vested interest in IWC so that he or she may make a more independent assessment of your overall anti-fraud program needs.

If you decide you may want to hire an outsider, be very careful. *Select a specialist with proven experience in your particular industry, and use caution as there are many who are good at talking but short on actual experience in what you are asking their opinion and recommendations about.*

> Anyone can read a book and say what needs to be done, but there are few who are *experienced* enough in the anti-fraud program consulting field to actually *know how to do it* and have *done it successfully* before.

If you do think a security consultant would be a good idea:

- Be sure to interview previous clients of the consultant for their nonattribution input.
- Verify the consultant's background.
- Contact several anti-fraud consultant specialists to receive bids on statements of work, but remember that the lowest bidder is not always the best one to select.

In addition, consider this: Executive management may wonder why you need an anti-fraud program consultant's help. If so, why did they hire you? Are you the right person for the job?

A specific type of anti-fraud program-related consultant may be needed in the future; however, as you build the anti-fraud program according to IWC's needs as you see them, you may decide that the use of a consultant is premature. After you establish a list of projects that are to be accomplished, you may find you do not have the experienced staff needed to successfully complete the anti-fraud project. In that case, a consultant may prove useful.

An advantage of hiring an outside anti-fraud program consultant is that with limited staff and/or the staff's fraud experience, a consultant may be able to complete some of the related anti-fraud program tasks or projects faster. You may also have at least one of your staff to assist the consultant, thus providing needed training for at least one member of your security staff. That person may then have the basic knowledge required to be able to conduct future anti-fraud-related projects or functions that you need a consultant to do for you now.

Another disadvantage of hiring a consultant is that it may create a morale issue for your staff, who may believe they can do the task themselves and should be given the opportunity to try, However, you want an experienced person to do it now, and this position does not endear you to your new staff. Nor is it the right thing to do. You should offer them the challenge: you might be surprised by the results.

Three major components of a corporation require some type or degree of anti-fraud defenses that you must assess. This point is again stressed so that you as a CSO do not lose focus on the basics. Often, CSOs are so inundated with crises and day-to-day operations that they forget why they are employed in the first place. You are employed to protect IWC assets:

- *People*: Virtually all companies identify people as their most important resource. This is particularly true in this, the Information Age and in a knowledge environment. It is people who use assets such as information and knowledge to create and deliver products and services. Skilled people are the critical component of wealth creation for a company. The category of people generally refers to employees; however, a company has an interest in protecting many other groups of people as well. While on company premises, security is also concerned with protecting customers, suppliers, and visitors.

  Executive management knows that people are important, but it also knows that more often than not, people are the most expensive assets and the first to go when business is bad. Furthermore, in some environments, especially manufacturing environments like IWC, executive management continues to try to find ways of automating processes and taking people out of the processing loop. Remember: robots can work 24 hours a day without stopping for a rest; they don't get sick, they don't take vacations — and they don't usually make mistakes.
- *Physical Assets*: Although physical assets come in many forms, for the purpose of our discussion, they are considered the physical items of value that the company uses in its production of goods and/or services. Capital assets such as plant and equipment are the most visible and costly physical assets. Buildings, computers, vehicles, and other like items represent a substantial investment for the company and are essential for the operation of the business. Protecting them is critical.
- *Information*: Some argue that all information has value and therefore requires protection. Others maintain that only sensitive information, proprietary or private in nature, requires protection. Working with management and those identified as owners of information, the CSO can determine what types of information require anti-fraud protection and to what degree it must be protected. In our age of information, the ability to share ideas and have a free flow of information is essential to the development of products and services. Being faster to market with products and services impacts the performance and ultimate survivability of a company. Also remember that information is time-sensitive and that as a result its protection will vary over time. Protecting information is the most difficult of all assets to protect and also the most difficult to evaluate.

BUDGETING

Once you have determined your anti-fraud program's statement of work and have identified the needed people, equipment, and facility space, you

must develop an anti-fraud budget to incorporate into your overall assets protection and security department budget. Failure to develop a quality budget may inhibit your ability to develop and manage an effective organization and anti-fraud program.

> An ineffective security organization can only lead to an inadequate anti-fraud program.

Let's assume you will be asking for additional budget in order to establish and manage an IWC anti-fraud program. Please do not play the budget "game" and ask for more than you need. If you as the IWC CSO can show specific justification for your needs and what will not happen with no additional budget or worse yet, a budget decrease, you have a better chance of getting what you need. If you end up getting a reputation for inflating your budget requests, the next time around you may get a budget far less than what you may actually need.

> Merriam-Webster defines budget as a plan *for the coordination of resources and expenditures*.[4] It is used to assist in the proper and prudent allocation of resources.

The budgeting processes you will encounter may vary considerably. Different businesses or companies choose to use the budgeting approach that best fits their needs. Even within companies, you may encounter different processes for budgeting. Below is a description of two different approaches you as the IWC CSO may find:

- *Zero-based budget:* This budget process requires the CSO to assess the complete security statement of work (SOW), which includes the anti-fraud program SOW, and to identify the resources needed to fulfill that SOW. A critical component of this process is ensuring that the SOW is valid. With the zero-based budget process, it is necessary to first identify the drivers to that SOW. Drivers are the specific regulation, laws, contractual requirements, company policy, customer expectations, or executive management needs and requirements that cause the IWC security department to take a protective action (e.g., those related to the anti-fraud program).

[4] Merriam Webster, Webster's Ninth New Collegiate Dictionary (Springfield, MA: Merriam-Webster Inc.), 1987

Resources cost money and must be planned for, budgeted, and acquired. The resources may be in the form of labor, material, capital assets, or services provided from a supplier. Regardless of their form, they cost money and must be planned for within the budget process.

- *Affordability-based budgets:* This budget process differs significantly from the zero-based budget process. With this budget process the security SOW is shaped by the available budget. Here the CSO works to form the security SOW to fit into the available budget. Generally, this process provides less available budget than what is necessary to maintain a fully compliant and fully serviced SOW. Therefore, the CSO must identify areas of the anti-fraud program in which a risk of noncompliance or borderline compliance will be accepted or a degradation of services will occur. Usually, this means imposing less timely or less efficient processes on your customers — which may in fact increase costs. Simply stated, customers may have to wait longer to receive the services they need in order to offset the lack of available resources needed to deliver them more expediently. This can be dangerous in that the corporation's work may continue but at an unacceptable level of risk because security does not have the time or resources to provide the needed anti-fraud defensive service or support and business cannot wait.

Through this process, all SOW requirements must be identified. Once identified, an assessment of the necessary anti-fraud program resources to perform the anti-fraud SOW must be made. In an ideal world, the necessary resources (budget) would be provided to the security department for the implementation of processes supporting the SOW. In the real world, the SOW is often aligned with "available" resources causing a risk acceptance evaluation.

If enough resources are not available to fulfill the SOW, then some degree of risk must be accepted for the portion of the SOW that will not be fulfilled. Often the choice of what does not get accomplished or is only marginally accomplished is left to you as the CSO. Nevertheless, executive management should be aware of and accept or acknowledge this condition.

Whatever process is employed to establish the anti-fraud budget, the following categories of resources must be addressed:

- *People*: The human resource (security professionals) needed to execute the statement of work.
- *Equipment*: The tools needed by security which do not fit into the capital asset category.
- *Capital Assets*: The fixed or permanent assets, or those employed in conducting business.

- *Training and Development for the security professionals*: In order to maintain a skilled and effective anti-fraud-trained workforce, periodic education and training is necessary. Keeping up with fraud developments in the security or management field is just one example of the type of training an anti-fraud specialist or specialists need.

For the budget process to be successful there must be an identifiable relationship to available resources (expressed in the form of monies budgeted) and the SOW. Questions that must be considered when developing a budget include:

- What must be done?
- For whom must it be done?
- What results are expected?
- What will it take to do it?
- How much will it cost?
- What are the recurring costs?
- What are the one-time costs?
- What is the return on investments?
- What happens if you don't develop a budget?

CONTROLLING

The CSO develops action plans to facilitate achieving the anti-fraud program and its related quality, vision, and mission statements, goals, and objectives. Controlling means that the anti-fraud action plans are implemented in accordance with defined and documented expectations.

Performance of the action plans is monitored, compared to expectations, and adjusted or improved accordingly. Simply put, when you as the CSO implement your anti-fraud action project plan, ask yourself:

- Did you accomplish what you expected to accomplish?
- If you did, how do you know?
- If you did not, how do you know, why not, and how do you improve?
- How much did it cost you?

When establishing an anti-fraud program consider the following:

- *Organization design*: The security organization and security job structures are designed to match the organization's assets protection program that includes the anti-fraud program SOW, that is to say, the anti-fraud program work your organization must perform. Plans are developed to align your resources in part with the requirements of the anti-fraud program SOW. Procedures and processes are written

and mapped to define and describe how the work gets done and what expectations will be met.

- *Expectations:* The security organization is expected to deliver an IWC anti-fraud program that operates effectively and efficiently. It may be a called a "security product" incorporating aspects of service or support functions. In any event, targets of performance levels or delivery of specific anti-fraud related products, services, or support must be defined. It is necessary to determine just how fast, how frequent, how many, or how effective are the anti-fraud products and services produced and delivered.

  Boundaries must be set and balanced in accordance with customer expectations and available resources. Boundaries provide a standard to measure against to determine effectiveness of performance and achievement of anti-fraud program goals. Key success factors should also be identified. Anti-fraud success factors are activities, events, or milestones that must occur for you to be successful. Knowing what key success factors are, and monitoring them, will assist in periodic determinations and assessment of progress.
- *Monitoring:* Monitoring the IWC anti-fraud program performances in relationship to alignment with plans will provide you with early and periodic assessments of progress. Measuring results with performance metrics (additional information on metrics is available in Chapter 13) and measuring customer satisfaction with customer surveys should provide sufficient feedback to compare performance with expectations. Perhaps the most important benefit from measurement is that it provides for early feedback on performance.

  Knowing if you are on or off track early in the process allows for performance adjustments and improvement before things get out of control. Periodic measurement is essential for problem identification. By monitoring performance, you develop an understanding of how well you are performing. Through measurement, you may validate performance to determine if it is as expected, or you may identify systemic and individual problems, causing corrective action to be taken.
- *Improvement:* When problems with one or more aspects of the anti-fraud program are identified, corrective actions must be taken. Failure to take corrective action can either cause you to operate at a reduced level of efficiency or allow problems to get out of control. Thus, the fraud-threat agents' attacks may be successful and the protection of assets will suffer.

  When problems are identified, include your security staff in the problem-solving process. Use tools such as process and workflow diagrams to map all steps of a process. This will enable identification of non–value-added steps and even the root causes of any systemic anti-fraud defensive mechanisms and related problems. When beginning the problem-solving process, consider the following steps:

- Clearly identify the problem.
- Involve employees in developing potential solutions.
- Assess cost and impact of changes.
- Rank all potential solutions.
- Develop strategies to implement the best solution.
- Change process, command media, or work instruction.
- Train employees on the new standard.
- Monitor performance of the new standard.

- *Reward:* It is important to offer positive recognition for improvements made by employees. Any time employees correct a problem or improve an anti-fraud program process, a positive response from you and your appropriate manager is in order. When employees use measurement data to identify and solve problems, that behavior should be reinforced.

  Reinforcement will encourage them to continue to make decisions and changes based on data. The amount of recognition or reward should vary depending on the magnitude of the problem solved. In some cases, the mere acknowledgment of their efforts will suffice; in other cases, more significant rewards such as monetary incentives and promotions may be necessary. Examples of rewards include certificates of appreciation and attendance at security conferences.

QUALITY, PROCESS IMPROVEMENT, AND ASSESSMENT OF ORGANIZATION PERFORMANCE

Once you, the IWC CSO, have all anti-fraud related functions up and running, you need to assess how well they are performing:

- Has the goal of "doing it right the first time" been met?
- Can processes be improved and efficiency gains made?
- Are workload, process performance, and costs effectively measured?

The following section provides an overview of these important concepts.

PROCESS MANAGEMENT

To determine the effectiveness of any single anti-fraud process it is necessary to measure that process. What gets measured will depend on how the process works. For example, a transactional process may require measuring the cycle time of each transaction. In some cases, the amount of what is being delivered is most important. In other cases, the frequency of delivery matters most. In any event, determining what gets measured is a product of what the process is intended to do. In other words, the process is

designed to do something. Does that something get done? If so, how efficient, effective, frequent, or cost is the process of getting it done?

> A process is a series of steps or actions taken to produce products or services.

To measure an anti-fraud-related process first requires an understanding of the process itself:

- What are the requirements that drive the process? In other words, why do it at all?
- What is the final product or service delivered?
- Who are the customers?
- Are their needs and expectations being met?
- How does the process itself work?
- Are there dependent subprocesses?
- Who are the process owners?

You will need to know the answers to these questions in order to successfully assess the anti-fraud program's processes and their effectiveness.

A tool used by the IWC CSO to assist in developing an understanding of how a process works is the process flow diagram. In this diagram, each step in any process is identified and examined in regards to how that step fits into the whole process. Furthermore, the value of each step itself is assessed. In other words, is it necessary to perform that step and does it bring value to the customer? By placing each step of the process in a flow diagram form, each step can be assessed individually. Unnecessary or non–value-added steps should be eliminated or redesigned into value-added steps.

Once a process is diagrammed and refined, measuring the actual performance of the process against the desired outcome is essential. This will tell just how effective the process is. Comparison of the actual cost and production or process time to the desired cost and production or process time will tell the CSO whether they are effective and efficient.

PERFORMANCE MANAGEMENT

The IWC CSO understands that determining the success of the IWC anti-fraud program can be, and usually is, measured in many ways. Some processes, like those related to compliance with anti-fraud-related laws and

regulations, are usually measured through the government or regulatory agency inspection process. Here a government organization with oversight responsibilities will conduct an inspection at a site or facility to assess the level of compliance. Any areas found noncompliant will require corrective action and may lead to the issuance of a citation.

Compliance with IWC anti-fraud program policy and procedures can also be measured through the internal audit process. In addition, IWC's anti-fraud program should include a self-inspection process. Self-inspections should be conducted periodically by the security organization and used as a tool to help understand the organization's level of anti-fraud performance and help prepare for external agency reviews. Furthermore, such tools can be offered to department managers for their own self-inspections.

USING TECHNOLOGY TO DELIVER ANTI-FRAUD PROGRAM SUPPORT AND SERVICES

There are many reasons to deploy technology in the effort to protect assets through an anti-fraud program. However, technology can also be used to improve the efficiency of how anti-fraud processes, services, support, and products are delivered. Some available technologies are quite obvious to the IWC CSO and have been in use for some time; others may even reside within IWC and are just waiting to be tapped into. Many information technology tools and capabilities already exist, which, if deployed properly for the delivery of anti-fraud program support and services, could reduce anti-fraud program costs, perhaps significantly. As a responsible CSO, the IWC CSO is continually looking for ways to achieve more cost-effective delivery of anti-fraud program support and services.

In today's IWC with its tight resource environment, efficiency and timeliness are not the only motivation to seek alternative means of providing services and support. The lack of budget to explore other options or add staff may drive you to seek help from technology. Furthermore, if you cannot get more budget allocations for additional anti-fraud resources that you have determined to be necessary to improve or enhance the anti-fraud program, then the use of technology to free already committed resources may be a possibility. This should allow you to re-deploy those freed resources to other areas — for example, enhance the anti-fraud program personnel resources where they may be needed.

Again, remember that at IWC security is a cost center and not a revenue-producing entity; therefore, it is in competition with other organizations for budget. How that budget is obtained varies and is often dependent on the demonstrated added value of the anti-fraud program and the assets protection program. As an example, if a security risk assessment or fraud survey shows that an anti-fraud program is out of compliance and that this noncompliant condition could adversely impact sales or a

contractual obligation, management will divert resources to correct this problem.

The only concern you may have as the CSO is that someone other than you may be the person who receives the additional resources to fix the problem. This of course assumes that the noncompliant condition was a result of something you did or did not do. It is not necessary to be completely dependent on the budgetary discretion of management. The solutions may rest within your own creativity as a CSO and willingness to explore other options. You should take the initiative to do this and not wait for a budget or compliance crisis.

MANAGING QUALITY AND MANAGEMENT OVERSIGHT

It is a mixed blessing that the IWC anti-fraud program is often subject to very close oversight. Although it is good to have an external (outside of the security organization) perspective and assessment, dealing with these activities and entities (SEC) is time consuming and can be difficult. Internal audit programs, government inspections, or customer reviews are some of the various methods employed to determine the effectiveness of an anti-fraud program.

Dealing with audits and inspections takes much time and effort. However, they provide a CSO with periodic feedback on the condition of the anti-fraud program. The other down side is that more often than not the focus is on compliance and not on efficiency. Efficiency needs to be measured, and the good news is that the CSO can take care of this task.

Perhaps the most important method for measuring the efficiency and effectiveness of an anti-fraud program is to have solid metrics in place measuring all key processes for delivering products and services and to conduct self-assessments (or self inspections).

Conducting self-inspections helps a security organization understand where it stands in relationship to all anti-fraud compliance obligations (i.e., policy, procedures, regulations, and contractual obligations). Self-inspections also allow the IWC CSO to tailor the inspection or assessment process to focus on issues of efficiency. During a self-inspection or self-assessment, special emphasis can be placed on assessing the efficiency or effectiveness of processes and the delivery of anti-fraud program support, products, and services.

WHAT IS RISK MANAGEMENT AS IT RELATES TO IWC'S ANTI-FRAUD PROGRAM?

The risk assessment and risk analysis topics were discussed in the last chapter. Here, we will discuss the management of risks as part of an IWC

anti-fraud program. The reason for doing so is to separate the actual "technical" aspects of risk assessment and related methodologies from the management of risks.

In order to understand the anti-fraud risk management methodology, one must first understand what risk management means. Risk management is defined as the *total process of identifying, controlling, and eliminating or minimizing uncertain fraud attacks or events that may affect the protection of the corporate assets*.

Risk management incorporates some aspects of risk assessments; risk analyses (to include cost-benefit analyses); target selection; implementation and tests; security evaluations of safeguards; fraud surveys; and overall reviews.

Many corporations also have risk management staff to deal with various aspects of business risks (e.g., insurance coverage as part of a risk mitigation strategy). CSOs should contact these specialists and coordinate activities related to the management of risks to corporate assets caused by fraud-threat agents. You may be surprised to learn how much they may be able to help you with techniques, data, and the like.

The goal of the assets protection risk management process is to allow the CSO, in coordination with executive management, to be able to manage the risks posed by fraud-threat agents to IWC assets. Risk management emphasis should be placed on management decision-making processes incorporated into the IWC anti-fraud program.

Although the ideal goal is to eliminate all risks, it is not a goal that can usually be achieved. The CSO and IWC managers deal with the uncertainty that arises in the course of daily activities associated with the threats posed by fraud-threat agents.

MANAGING AND REDUCING RISKS TO CORPORATE ASSETS

The starting point in managing and reducing risks to enterprise assets is assumed to be a basic anti-fraud program that uses integrated protection measures. An ongoing monitoring and surveillance program augments this baseline program and addresses both internal aspects, coupled with attention to external factors that could drive the threat. The risk of a fraud attack is not static; it is a dynamic variable that will fluctuate in part based on business cycle elements and in part on the ripeness of new products and new technologies for exploitation. Varying the degree of watchfulness, in effect adopting a process of heightened alert for periods of increased risk to fraud attacks and of basic vigilance at other times based on the inputs received from the monitoring and surveillance systems, helps protect assets at lower costs.

The response element should include a combination of internal and external assets capable of determining the facts in a legal and expeditious manner. Whereas investigations in the physical world may precede at a deliberate pace (hours, days, weeks, or longer), today we increasingly do business and work in cyberspace where the response to asset fraud attacks and subsequent inquiries must move at Internet speed, which means nanoseconds, minutes, hours, and days at most. Such speed is necessary because some key information may well be perishable.

The best possible resolution of a fraud incident or of known or suspected fraud attacks against corporate assets is the arrest and conviction of the perpetrator(s). In some circumstances, however, it may be preferable to turn the matter over to a counterintelligence operation. An attempt that is detected early enough may misdirect or mislead in a way that will feed the opponent inaccurate, incomplete, or misleading information (misinformation) to confound their analysts. After all, if the intrusion is detected quickly and is done properly, then the intruders might believe that they had avoided detection by the anti-fraud defenses of the target. Playing to this belief, the fraud attackers may be subtly deflected.

As global competition increases and the global power of a nation-state is measured in terms of economic power, such attacks are expected to continue to increase, and to increase exponentially, as the global marketplace competition becomes more of a global economic battleground where one cannot be neutral. You are either a player or a victim.

Regardless of the outcome, it is vital that every case of known or suspected fraud attacks against the corporate assets be carefully analyzed and that weaknesses in anti-fraud defenses, operations, and procedures that facilitated the breach should be addressed. This leads once again to the beginning of the cycle where enhanced anti-fraud defenses are implemented and await the next onslaught of attacks.

PROGRAM FOR MANAGING ANTI-FRAUD DEFENSIVE RISKS

The following points should be considered in building a framework for managing risks arising from fraud-threat agents: in many ways the operational and procedural anti-fraud defensive measures are as important as or more important than purely technical measures. This is true because some of your automated anti-fraud defensive systems, such as those related to computer and network systems, are vulnerable to compromise and breakdown. Therefore, there should always be a backup plan that includes a human in the loop.

Anti-fraud defenses must be managed with a combination of technical, procedural, and operational safeguards.

> Risk management: analysis of possible loss: the profession or technique of determining, minimizing, and preventing accidental loss in a business, for example, by taking safety measures and buying insurance.[5]

Remember: preventing, detecting, and responding to fraud threats is a dynamic process that will grow and change as rapidly as new technologies and processes are developed. Keeping up with the rapid pace of these changes is essential if the CSO is to defend key corporate assets against pernicious fraud threats.

> Risk-benefit: studying risks and benefits: studying or testing whether the benefits of a procedure, process, or treatment outweigh the risks involved.[6]

Remember that the most fundamental and essential step is to provide management leadership, direction, and support in conducting an anti-fraud risk assessment that considers all logical types of fraud-threat agents' attacks and vulnerabilities to those attacks.

The purpose of such an assessment is threefold:

1. To identify the full range of the corporation's important assets, including property, personnel, and sensitive proprietary information, especially assets that are unique to the corporation. Determine where they are physically located and how they are protected.
2. To create a value matrix of the assets and determine their relative contribution to the corporation's business. Stratify them to identify the top tier, the assets of greatest significance. We generally refer to the most important ones by the term *the crown jewels*. Although there is no precise formula for determining when a specific asset qualifies for such status, most senior managers and executives of a corporation can reach a rough consensus as to the items they can all agree are "crown jewels." Subsequent steps in the anti-fraud risk assessment should focus on managing and reducing the risks to these, the most significant assets.
3. Review the existing framework for safeguarding the corporation's most valuable assets using an interdisciplinary team that can evaluate

[5] Ibid.
[6] Ibid.

technical, operational, procedural, and legal protective measures. Consider how well the existing array of anti-fraud defensive measures will defend the most critical resources against the multiple technologies and techniques that will be used by fraud-threat agents if they are assigned the task of obtaining them.

The primary objective of the review called for in (3) is to ensure that the corporation has invested sufficiently in the integrated technical and operational anti-fraud defensive measures as well as a complete legal and procedural foundation to prevent, detect, deter, and respond to known or suspected incidents of fraud attacks.

In those corporations, such as IWC, which have had known or suspected incidents where fraud attacks have resulted in loss of assets, a two-pronged response is necessary.

- First, management must ensure that it makes a serious effort to determine all the discernible facts concerning the incident. Too often the tendency is to either write off an incident as an isolated event or as simple "bad luck." Although both may be true, the opportunity also exists to gain valuable insights regarding the strengths and weaknesses of the existing assets protection program. The insights gleaned from such a detailed analysis may help prevent future, and perhaps even more serious, incidents.
- Second, management will be better prepared to make informed decisions concerning steps to actively enforce the corporation's rights through litigation or prosecution, if it is armed with a complete report of the incident. Of course such an analytical process presupposes that the corporation has anti-fraud mechanisms to identify and report known and suspected fraud incidents in a timely manner such that an investigative response is possible.

Management must also consider that in order to get assistance from law enforcement to investigate an incident of known or suspected fraud attacks (where applicable), several key hurdles must be overcome.

- How does the corporation know a fraud incident (crime) has happened?
- Was the asset protected consistent with its status (did the corporation take reasonable steps commensurate with the value of the asset)?
- Have they calculated the value of the asset and any associated losses?

Although an ability to answer these questions is not a prerequisite for contacting the local or federal law enforcement agency, the investigators will likely ask for these and other details early in any official discussion concerning a fraud incident.

RESPONDING TO FRAUD INCIDENTS

The topic of how to respond to incidents, including proper investigation protocol in detail, goes well beyond the focus of this book. Suffice to say at this point that, although the corporation has many options when it knows or suspects an incident, one should not expect any public agency to come in and act as the internal security team for the corporation. The corporation must be prepared to conduct its own inquiries and should only approach law enforcement when management believes there is a reasonable basis for suspicion that an incident requiring law enforcement support has actually occurred. This can be done through an inquiry or perhaps through an inquiry in conjunction with a limited risk assessment or fraud survey.

The anti-fraud risk assessment is limited to the specific objective in determining the risks of a successful fraud-threat agent attack against a specific asset and the costs of mitigating that risk — for example, the cost of anti-fraud policies, procedures, processes, and the like, including the cost of compliance by all IWC employees, and/or the rationale for the requirement.

The assessment is also limited in time. For each of these issues where different assets and departments were involved, such as manufacturing or marketing, a separate, limited risk assessment will be conducted.

The approach can also be used for anti-fraud assessments and includes developing baseline anti-fraud policies, procedures, and processes while at the same time identifying specific anti-fraud requirements for each different work environment of the IWC, the Human Resources Department, the Manufacturing Department, and the like.

The results of the limited risk assessments will then be provided as part of a formal briefing by the CSO to the vice president of that particular department. A copy of the report to the vice president of Human Resources, the CSO's boss, will be given just to ensure that the boss was in the communications loop and because a copy will be available for use when briefing the CEO and the executive management team on the new anti-fraud program. The limited assessment would be part of the backup documentation for the briefing. The CSO could reason that a copy to the CEO would not be a good idea at that time because then the CSO would have to explain what it was and why the CEO had it.

The limited risk assessment will state the risks, mitigation factors, and estimated costs of the increased anti-fraud protection of that particular asset or set of assets. If the vice president of that department, who is also the person immediately responsible for the protection of that asset or assets, does not concur in the anti-fraud protection requirements, then the vice president must formally accept the risks in writing on the last page of the report and send it back to the CSO.

The acceptance of risk statement reads as follows: *I have reviewed the findings of the limited risk assessment conducted by members of the IWC*

anti-fraud program project team. I understand the potential loss of, or damage to, IWC assets under my care that may occur if additional protective processes are not put in place. I accept that risk.

Another approach may be that management is not authorized to accept such risks because these risks are not acceptable to the welfare of IWC. This decision must be coordinated by the CSO with the CSO's boss and executive management. Their decision on how to proceed on this vital issue should be required because management has overall responsibility for the protection of IWC assets and the CSO is the "in-house" consultant and assets protection specialist. The overall assets protection responsibility lies with the CEO and executive management.

Most people will be unwilling to sign such a document or will try to delay signing, hoping that the issue will be forgotten. The CSO can never let that happen. To resolve that issue, a reply of concurrence or nonconcurrence will be set forth in the document with a suspense date. If no reply is forthcoming by that date, the report states that additional safeguards will be put into effect no later than a specific date because of the action person's failure to sign the document. A nonreply is taken as concurrence.

Often the executive will try to find a way out of the dilemma, and "negotiations" will take place during which various options will be examined, other than those already stated in the report. The CSO cannot turn down such a request, for to do so would give the executive the ammunition needed to conclude that the CSO was not being cooperative, was not a team player, or had a "take it or leave it" attitude. At the same time, negotiations cannot go on indefinitely. If a roadblock is reached, then the executive and the CSO should agree that the matter will be discussed at a meeting with the CSO's boss or possibly even the CEO.

MANAGING FRAUD THREATS

It is extremely important to understand as many fraud threats against corporate assets as possible. Remember that if it were not for threats, there would be no need for an anti-fraud program. That should be understood as obvious, but it is stated here because sometimes a CSO loses sight of the objective of an anti-fraud program, which is designed to achieve the following:

- Protect corporate assets from fraud in a cost-effective manner from all applicable attacks by fraud-threat agents, and since there is no such thing as perfect, impenetrable security, the CSO must also have an anti-fraud program that:
  - Minimizes the probability of a successful fraud attack by a fraud miscreant.

- Minimizes the damage if an attack by a fraud-threat agent occurs.
- Provides a method to quickly recover in the event of a successful attack.
- Provides a process to quickly mitigate the fraud threats and eliminate or reduce the vulnerabilities that allowed the fraud attack to succeed.
- Provides for a rapid inquiry or investigative response, the collection of evidence, the conducting of interviews as documented in the event IWC wants to pursue legal action against the identified fraud-threat agents.

CASE STUDY

As IWC's CSO, you must find some efficiency gains in order to properly establish and manage an IWC anti-fraud program. You are technology literate and believe that the use of technology to support efficiency gains is worth studying.

As the IWC CSO, how would you proceed?

Some thoughts on that question are as follows:

When looking for ways to use information technology to enhance the delivery of anti-fraud program support and services you may want to focus on those services only. However, the best way is to look at all security functions and to ascertain where any gains realized efficiently in the security department can be allocated to the anti-fraud program functions.

First the CSO may want to start with examining transactional services. It is the transactional services and not the consultative or oversight services where information technology can be deployed most cost effectively. At IWC, the CSO first examined the security education and awareness training program process, which also includes anti-fraud aspects, and determined it to be an ideal candidate for the use of information technology as a means of delivering this service.

It was determined that in many ways, security education is a transactional process. At IWC, security education is accomplished by a department that has responsibility for the implementation of a training and awareness program for the "rank and file." How they manage to accomplish their task is through a labor-intensive process, yet much of the work is reccurring and repetitive (transactional process), covering subjects such as the following:

- Workplace violence prevention training
- Protection of company information
- Automated information systems user security training
- New employee indoctrination
- International/foreign travel security and safety briefings

- Protection of classified information for IWC's government customers
- Anti-fraud defenses and what employees must know and do

Traditionally, these products were delivered through standard briefing packages designed for all company employees. Each addressed the areas where particular employee awareness is needed or even mandated (company policy or government regulation). On some sort of a scheduled basis, employees are identified as requiring awareness training and are notified to attend a formal presentation. These presentations are delivered to a group of employees who attend together. In this case the following steps take place:

1. The requirement(s) is/are identified.
2. The briefing is designed and developed.
3. A target audience is identified and scheduled.
4. An IWC security professional conducts a formal presentation (to a group or to an individual).
5. Each employee security/personnel record is annotated to indicate requirement fulfilled.

Steps 1 and 2 are one-time events. First, a requirement is identified. It may be in the form of a government regulation or a company policy or, it may be a management desire to have employee awareness increased in a particular area of concern. Once the requirement is established, training materials are developed. They may be delivered as a briefing or presentation, brochure, pamphlet, videotape, or computer program. This process, excluding revisions and updates, is a one-time creative process and is the process most dependent on the expertise of the security professional. Steps 3, 4, and 5 are reoccurring transactional steps and could be more efficiently executed with the help of information technology.

Using technologies such as computer-based training, one can build a Web-based security education and awareness program into the IWC intranet. Feeding from, and connected to, the human resources employee database, a security information system can be established where the criterion is developed by security and compared against the HR database. Those employees who require a particular type of awareness training could receive an electronic notification directing them to a Web site to complete their mandated training. At their leisure, and in lieu of taking scheduled time to attend a group presentation, the identified employee can visit the specified Web site and complete the training course. This process usually takes significantly less time to complete than the process of attending briefings. Upon completion of training, the computer system can generate a notification updating the personnel/security record for that employee. A security professional can create custom reports allowing for the review of this process to ensure that it works as designed. Overall, this process would

save time for the employee (someone else's costs) and for the security professional (your costs) preparing and conducting these briefings.

SUMMARY

The CSO in IWC has a dual role of being the *leader* of the anti-fraud program and corporate security efforts and a *manager* of the security department. The CSO should treat those who are provided assets protection and security service and support as the customers of the CSO and security staff. They can be grouped as internal and external customers.

The CSO expects certain things from executive management and vice versa. The CSO expects support for the anti-fraud program and the security staff functions. The executive management expects the CSO to develop and maintain a cost-effective anti-fraud program.

Establishing and managing the IWC anti-fraud program requires the development of a statement of work and an understanding of the internal and external customers' assets protection requirements that are additional to the basic assets protection requirements of any publicly owned corporation. The anti-fraud defensive requirements are based on people, information, and physical assets. When you as the new IWC CSO come to work, you should come to work with a plan and then work the plan.

CSO responsibilities include the normal management responsibilities of planning, budgeting, controlling, staffing, and counseling. It also requires working in a team-emphasized environment where the CSO encourages everyone to work in a cooperative manner, as well as to communicate extensively throughout the security department and IWC.

Because IWC is an international corporation, it has offices in the United States, Europe, and Asia. Consequently, the CSO must establish and manage an anti-fraud program and security department that includes the foreign locations.

11

Winning Through Teaming

INTRODUCTION

In today's business world, the use of teaming techniques is almost mandatory. Sometimes, a strong leader who can quickly get things done is preferred; however, it seems that today's managers do not want to take chances, jeopardizing their careers and bonuses, so they use teaming as a way of building a consensus so that if anything goes wrong, they are not personally to blame.

> Finagle's Eighth Rule: Teamwork is essential. It allows you to blame someone else. — *Proverb*

ANTI-FRAUD PROGRAM TEAM BUILDING

Teams work toward common goals that are understood and accepted by all team members: to achieve long-term goals and objectives. Team members must work openly and honestly with each other toward developing and maintaining a successful anti-fraud program. They must collaborate with each other, and the various anti-fraud teams are no exception. Some disagreement is expected. Both listening to others and offering ideas are essential skills.

To build an effective anti-fraud team, the CSO must operate in a collaborative way. Working with team members, the CSO working with the security managers must first identify the purpose of the teams and their objectives. The teams themselves, such as the anti-fraud program development project team, should identify issues and problems and work together

to develop and implement short-term and long-term strategies. Effective teams will improve the performance of your organization — at least these are the formalized methods and goals. Sometimes they work and sometimes they don't work so well.

Teaming has its advantages. In today's budget-conscious corporate environment, teaming allows the CSO to be able to call on other resources to assist in meeting the security department's goals such as establishing and managing an anti-fraud program. In addition, teaming with other IWC departments allows the CSO to rely on the anti-fraud related expertise of others such as auditors, legal staff, ethics staff, and such.

As part of teaming, there are expectations on many fronts. These expectations positively or negatively impact teaming in order to successfully meet the CSO's goals such as an effective and efficient anti-fraud program.

EXECUTIVE MANAGEMENT AS TEAM MEMBERS

The most important thing vis-à-vis an anti-fraud program that IWC executive management can provide to a CSO is overt support for the anti-fraud program. By providing that support, executive management is actually part of the team responsible for the success of the anti-fraud program.

> Executive support for the anti-fraud program is essential to its success.

The chairman of the board, CEO/president, and all others in executive management must make it known throughout IWC that they are supporters of the anti-fraud program. Of course, executive management providing an increased budget does not hurt either.

Those in executive management should recognize the criticality of a successful anti-fraud program and their relationship as team members to that goal. They must communicate their support for consistent applicability of anti-fraud defenses to all employees, from other senior executives through management to the rank-and-file employees. Without executive support and commitment to a sound anti-fraud program, it will fail. Without senior executive support, managers and employees will find reasons, usually cost driven, to circumvent and even avoid anti-fraud policies and procedures. This condition leads down one path, and that is a failed anti-fraud program and damage to IWC through successful fraud attacks targeting IWC's valuable assets.

As part of that teaming, the CSO should have access to IWC's executive management. Although access is generally not required on a regular basis, when a CSO needs access to the most senior executive managers, it

is usually for issues that can directly affect the IWC's welfare, that is, the anti-fraud program. Sometimes this is a difficult matter with the CSO reporting to the vice president of Human Resources who reports to the CEO. The vice president, as your boss, will more than likely have some serious concerns about any one-on-one meetings with the CEO and other members of IWC's executive management team.

As the CSO, you must establish a criterion with your boss for direct contact to the executives. Furthermore, you must ensure that you truly require any requested meeting. Based on the established criterion, you should expect that the CEO or others whom you want to contact are receptive to such meetings and not have them delegated to a lower level of management. Of course, most issues can be handled, and should be handled, at the lowest level of management deemed appropriate where effective decisions can be made. However, as the CSO, you should make it known, diplomatically of course, that you require this type of support. So, when you ask for a meeting, executive management knows that it is important enough for them not to put it off or delegate down to a lower level of management.

> The CSO must ensure that executive management knows that they are an integral part of the anti-fraud program and are valuable team members.

TEAMING WITH IWC EXECUTIVE MANAGEMENT THROUGH A BUSINESS APPROACH

Members of executive management in any business generally speak the same language, the language of business, that is, profits, losses, cost-benefits, return on investments. Establishing and selling an anti-fraud program to IWC's executive management will not require the CSO to justify such a program. After all, that is one of the reasons they hired the new CSO. What will be required is for you as the IWC CSO to take a business approach if you are to convince them that the methods, processes, approach, and philosophy you want to use in developing an anti-fraud program makes good business sense.

It is imperative that you remember that executive management is accustomed to approaching business decisions in the context of requirements, resources, cost, return on investment, and associated risks. For example, when working to convince an executive to support the requirements and budget of an anti-fraud program, that executive will expect you to present a business case. The executive may look for answers to the following:

- Why is a formal anti-fraud program even needed?
- What will it cost?
- Will the anti-fraud program really eliminate or reduce successful fraud attacks?
- How long before one can expect a return on the initial investment?
- What is the risk of establishing a formal anti-fraud program versus not establishing one?
- What makes this program different from the assets protection program?
- Isn't this program the same as the assets protection program and, therefore, wasting resources?
- What are similar companies doing to defend their assets against fraud-threat agents?
- More specifically, have you benchmarked with similar corporations? In other words, have you compared your anti-fraud program concepts and proposal with a security organization and corporation of similar sizes and within a similar industry?

Understanding the business perspectives of executives is a must if you are to be successful in developing an anti-fraud program and getting them to be active team members. Different executives take different approaches and have different priorities. When working with IWC's chief financial officer (CFO), you can reasonably expect the CFO to place a high priority on cost, risks, and return on investment.

When working with the vice president of Human Resources, your boss, you can expect employee welfare and workplace environment issues to have a high priority. This is not to say that either perspective is, or should be, more important or weighed with greater value. It is to say that understanding each will enable you as the CSO to better support your anti-fraud program business case or gain their support in this or other related matters.

TEAMING WITH CORPORATE PEERS

Understanding the culture of an international company like IWC and the various subcultures, as well as cultures in foreign countries, of different business units, and functional organizations, is critical to your success as a CSO. Working with heads of different departments, you will encounter cultural similarities and cultural differences. Some organizations will have a risk-taking approach, whereas others will not; some will be more creative, whereas others will be less creative. Remember that you are dealing with people and not nonlife forms. They have needs, feelings, problems, goals, and individual personalities. That is why it is so very important that as a CSO you are a "people person" and genuinely enjoy interaction with your peers and others at IWC.

Understanding their needs, desires, and agendas is absolutely necessary if you want their support. Remember President John F. Kennedy's now famous phrase spoken at his inaugural: "Ask not what your country can do for you but ask what you can do for your country"? Well, that same approach, modified of course, is a good attitude for you to take in dealing with management, in fact with anyone at IWC. Keep in mind that you lead a *service and support department*.

> Ask not what you need from others but what you can do to help others succeed.

It is important for you to understand how and perhaps even why corporate peers are different and how you should interact with them and gain their support to meet the anti-fraud program objectives. In dealing with your peers and others, your goal should also be to help them succeed while building an anti-fraud program. If you can do that, the IWC anti-fraud program will meet the needs of everyone at IWC with the least impact on productivity and costs, and you will have a better chance that management and employees will support it.

When dealing with creative and more open organizations, you can probably be very straightforward in sharing your views and seeking theirs. The managers and staff of these organizations encourage open and frank communications. They generally treat everyone with respect and encourage exploration of new ways to do things.

When working with risk-averse or more closed and traditional IWC departments, you may have to be circumspect in your approach and more conscious of their signals and indicators. They may not always say what they are thinking. The personnel of these organizations tend to be more conservative in their approach in conducting business. "Rocking the boat," expressing disagreement, or not sharing information is usually inappropriate behavior, and you will probably encounter resistance in getting support for the anti-fraud program.

You should understand the duties, responsibilities, overall processes, and limitations of each IWC department. Generally, we humans like to talk about our work and ourselves. As the CSO, use this opportunity to listen to what everyone is saying. Be sincere in your interest in their activities as there is no doubt what you do will impact them in one way or another. Also remember the old saying, "You were born with one mouth but two ears for a reason."

Since security in general and the anti-fraud program are generally compliance-related functions, you may find common ground with other compliance organizations. Audits, Environmental Health and Safety, Ethics

specialists, and the Legal Department all deal with compliance-related issues. Each works to ensure that the policies, procedures, and processes developed and implemented facilitate compliance with contractual requirements, regulations, and laws. As such, their approach to conducting business may provide insight into how you should proceed.

> Take the time to learn how other functional organizations interact with each other and how they conduct daily business, for that will give you insight into your efforts to effectively deal with them and build a successful anti-fraud program.

The CSO must be able to work with peers and others in order to get the job done. If the CSO can get an understanding of the needs of the IWC managers and employees and help meet those needs, it will also help the CSO in meeting the anti-fraud program goals and gain their support for that effort.

TEAMING AND DEALING WITH OFFICE POLITICS

Office politics is a fact of life in today's business world. It is imperative that the CSO understand that and ensure that office politics does not adversely impact the CSO's objective of establishing and managing an efficient and effective anti-fraud program for IWC.

Much of what you as a CSO do to achieve success in any company, and IWC is no exception, depends on your skills and willingness to work hard — in other words, how well you perform your duties. However, some of what you do to be successful depends on your understanding of and participation in what is called office politics; IWC politics cannot be ignored. Individual success and departmental success require that you become engaged in some manner in office politics.

You cannot isolate yourself from office politics without limiting your ability to succeed. If you do isolate yourself, you cut off a valuable means of understanding IWC and facilitating success for you and your department. Furthermore, your opportunity to form successful anti-fraud teammates will be significantly reduced.

Not all information within IWC flows through formal channels. Much important information is distributed and shared informally. Having access to that information, in essence being part of the informal information flow process, will contribute to your understanding of the corporation and your overall success.

Understanding who has power and influence is also important. Aligning yourself with decision makers and with those who influence and serve

the decision makers will offer you an advantage. If it is too difficult to align yourself with the decision makers, then focus on alliances with those who influence decision makers. Influencing them will ultimately have an impact on the decision makers. If you find this distasteful, get over it.

Alliances are a part of organizational behavior. Without them your influence will be limited, as will your success. That being said, remember that this does no mean compromising your personal values, honesty, or integrity. In other words, it does not mean having to "kiss butt" or "bend over and take one for the good of the corporation." However, life is full of compromises, and as long as your personal and corporate values are intact, then proceed.

Look at it this way: as nasty and distasteful as it is to admit it, we humans use others to get what we want. Isn't that what management is all about? That is a fact of life whether one likes it or not. It is how one goes about doing it that makes the difference. For example, as mentioned earlier, if you can help others succeed and by doing so help the anti-fraud program succeed, what is wrong with that? That is what is called a "win-win" situation. In this case, you are using people to meet your objective, but they may also be using you in return.

One may even want to plan on how to get others to support the anti-fraud program based on their individual needs and personalities. You, as the CSO, may want to target them and exploit their personality strengths and weaknesses. This approach may sound "cold and impersonal," but in fact if done right and for the right reasons, why not use this tactic as part of your toolbox of methods for dealing with people?

As a CSO, you must get things accomplished through others, and it is much more effective and efficient if you can work with them instead of pulling or pushing them into supporting an IWC anti-fraud program, such as by threats of disciplinary action. It takes less energy, and it almost always proves to be more successful.

Understanding your own political tendencies, behavior, and personality will help you in the political environment and further your goals to establish a teaming environment relative to gaining support for the anti-fraud program. Be observant and listen. Knowing how people react to you allows you to focus on your positive characteristics and to control or change your negative characteristics. Although it is difficult, you must try to be objective if you are to succeed in this endeavor.

Controlling your behavior will help you in relationship building, which is essential in developing alliances. In any event, never lose focus on your primary role and responsibilities. It is important to be aware of and to understand office politics. It is also important to participate. Company politics can be a nightmare, or it can be a vehicle that helps you accomplish your objectives. Recognize that and learn to manage within the political environment without it getting in the way of fulfilling your obligations.

The CSO works in a world of office politics where security is often given a bad name. These positive office politics tactics help show that you the CSO and the corporate security department staff are "team players" and are doing their part to support the IWC goals.

You may be thinking, "Why do I have to do all this work? Why can't they just cooperate in the interest of the corporation?" The answer is simple: that's life! No one said it was perfect. If you want to have a successful anti-fraud program, then you must do whatever it takes (legally of course) to accomplish that goal. Yes, it is hard work, but as a CSO and security professional, it is your responsibility to strive to create a successful anti-fraud program, and using teaming techniques helps you accomplish that goal.

TEAMING WITH YOUR SECURITY MANAGERS

As the CSO of IWC, you have other managers working for you. Your management team will be the primary vehicle for you to use to get things accomplished. Setting your expectations for them early on can help ensure good performance. Work with your management team to establish the boundaries within which you expect them to operate, vis-à-vis the anti-fraud program and other duties and responsibilities.

Consider the following:

- What do you expect from them?
- What constitutes a job well done?
- What is their level of authority?
- What are their responsibilities?
- Define the limitations of their role.
- Make sure they understand organizational goals and objectives.
- Provide them with regular performance feedback.

A common problem for new or inexperienced security managers is to rely on the skills that got them the job in the first place. In other words, they need to do the work themselves instead of managing others to get the work done. Management requires a different set of skills than those of the non-managerial security professional. Often, when faced with problems or difficult situations, new CSOs will try to do the work themselves, thus avoiding what they should be doing: managing others to get the job done.

A major role for you as the IWC CSO when working with your managers is to be their coach. Spend time with them, ensuring that they understand how to get things done through their employees and not by doing the work themselves. Your managerial approach to your managers is a key factor in how they will treat their employees. It is also a key to establishing and managing a successful anti-fraud program.

TEAMING WITH YOUR SECURITY STAFF

> The essential skill of management is the ability to develop and work with people.[1]

As the CSO for IWC, you and your security management team will depend heavily on your employees to perform their duties to the best of their abilities as professionals, thus helping to make the security functions and anti-fraud program effective and efficient. Good performance does not happen by accident. It is your responsibility as the leader and manager of the security department and anti-fraud program to create an environment in which your employees can be successful.

Without successful employees, the IWC anti-fraud program and your security services and support will fail. Creating this environment requires work. A conscious effort to get the most from employees is needed, so you must plan to develop the behavior of your security staff. When you embark on this effort, consider the following issues:

- *Collaborating:* The effectiveness of a security organization and its anti-fraud program is totally dependent on the performance of its people. For the organization to benefit the most, all employees must participate. A participatory environment is one in which all employees are part of the decision process. This environment is best accomplished when they work together cooperatively within small groups to solve problems. In this way, each member has a say in the process and a stake in the outcome. The CSO's directed initiation of an anti-fraud program project team is a good way to begin to facilitate or improve this collaboration.
- *Communicating:* Communication can be accomplished in many ways: letters, memos, e-mail, voice mail, messages, telephone calls, and face-to-face meetings. Although all these methods have value, face-to-face communication is the most effective because it allows for speaking, listening, observing, and feedback all at once. It is a very interpersonal process. When people engage in open and honest face-to-face communications, not much is hidden. Face-to-face communication allows each person to react to what is communicated at the moment it is said. Moreover, during face-to-face communications you have the advantage of reading body language, which can be very

[1] Lane, Byron, "Managing People, A Practical Guide" (Grants Pass, OR: The Oasis Press), 1990.

telling. Regular communications with your employees is a must. Communications must flow both ways — from you to them and from them to you.

Everyone in the security department must feel they are free to speak openly and honestly. Open and honest communications facilitate trust between people. Being direct and candid in all your communications will reduce the possibility of misunderstandings and also encourage people to be direct and candid. Honest communications includes being able to say, "I don't know — what do you think?" Employees hearing this said would realize you are being honest and open with them, and so you will expect them to communicate in kind. Half of the art of communicating involves listening. Being an effective listener enables you to better understand the communication, and it also demonstrates to the person speaking that you are interested in what they have to say. Listening effectively to someone will encourage him or her to be more open and candid with you. These techniques are crucial in the development of an anti-fraud program.

Some managers say they have an "open door policy," but often they don't really mean it.

- *Motivating:* Many theories have been offered on how to motivate employees. Since everyone is different, it is difficult to determine what most motivates each individual. Perhaps the best you can do as the CSO for IWC is to focus on creating an environment in which people are inspired to motivate themselves. According to Dr. Byron Lane of Pepperdine University, a critical component of motivation is giving people a stake in the organization. This will apply to the anti-fraud program development and management. When people are involved in the process of goal setting, decision making, and implementation, they will hopefully develop their own motivation. Making employees part of the process, challenging them to be involved in the organization of an anti-fraud program, and encouraging them to perform to high expectations can all generate quite a bit of positive energy and a teambuilding environment.

When you get the security staff involved, they not only feel part of the process but the message they receive from you is *they are trusted*. Participation, involvement, and trust can be a powerful means to motivate people.

- *Delegating:* The act of delegating responsibility to others can be difficult and problematic for managers. It requires giving up some control and placing your full trust in someone else. For managers who are used to getting the work done themselves, it can be difficult to rely on others. Watch for this tendency in your managers, and be careful you don't do it yourself. As the CSO for IWC, you will have many responsibilities, obligations, and, more than likely, a large workload. In effect, you cannot do it all. To be successful you must be able to delegate work effectively. This means assigning meaningful tasks and participating in the anti-fraud program, as well as giving managers and employees the authority to determine how to get the job done and the responsibility for successful completion of the effort.

Caution: Don't usurp the management authority of your security managers when dealing with their security staff.

Not everyone works the same way or has the same set of skills. Some employees to whom you delegate work require only that you clearly advise them of your expectations and then stay out of their way. Let them get the job done. They tend to be self-motivated and work well with little or no supervision. Others may require more consultations or coaching from you. They need you to be involved with them to some extent by providing guidance and support. In any case, understanding the capabilities of your employees and demonstrating your trust in them are critical components of delegating successfully. As a CSO, your delegation of authority will generally be to one or more of your managers. It is up to them to delegate to their employees.

Delegation never relieves the CSO from the ultimate responsibility of what has been delegated. If something goes wrong in the security department, it is always the CSO's responsibility. You may counsel your staff when they fail; however, to anyone outside the security department, you take full responsibility for your staff's failures, and they are given full credit and acknowledgment for their successes.

- *Goal Setting:* Establishing goals must be a process of participation. As the CSO, you will be responsible for setting department and

individual goals and for aligning these goals with company goals. Setting individual goals allows you as the CSO to define what you expect your employees to do. It also tells the employees what the company expects from them. Setting department goals helps bring the organization together working toward the same outcome. Goals should be clearly and concisely stated: they need to be specific, realistic, measurable, and mutually understood.

All involved personnel ideally should agree to the goals. Individual and department performance to goals should be monitored. If performance to the goal is not adequate, corrective action should be taken, or alternative plans should be made to get performance to goal on track. To be meaningful, goals should be valuable to the organization and the company. Goal setting is crucial to the success of the anti-fraud program project and its subsequent maintenance.

- *Evaluating:* If done properly, assessing an employee's performance does not have to be a difficult chore. Providing performance feedback to employees is essential for their development. Without honest feedback, employees don't really know how management views their performance. The performance appraisal process is best used as a development tool. It is a vehicle to facilitate open and honest discussion of issues between you and your managers or between one of your security managers and employees. Performance evaluations should not be an annual event. It should be a process that occurs all year long. This is not to say that evaluations take place every day. Periodic and timely review sessions, both formal and informal, should occur throughout the year.

Reviews can be as casual as a brief discussion of what went well and not so well with the completion of a project. Sessions might also be scheduled for specific discussion of performance issues. Most companies have a standard process requiring an annual performance assessment along with a comparison ranking system. This is not enough. Providing performance feedback (e.g., on anti-fraud program project progress and the employee's role on that project team) should not be saved up for an annual occurrence. Moreover, the documentation should not be a checklist. A narrative describing both positive and negative aspects of the employee's performance is best. This approach will lead to very specific discussions of performance issues promoting the process of communication between employees and managers. However, as much as possible, performance measurement should be as objective as possible. Giving employees measurable goals will assist in the endeavor. The employee may not like you and/or you may not like the employee; however, it is their performance to goals, and not their personalities, that should be objectively measured.

TEAMING AND DEALING WITH SATELLITE OFFICES IN IWC HEADQUARTERS IN THE UNITED STATES

As the IWC CSO, your primary focus will be on the corporate office and its main business units, not the satellite offices. It is in these main business units that most of the people, revenue, activity, and problems are found. Satellite offices, usually sales and marketing offices, generally do not require as much of your attention. They are geographically distant from the main business units and have fewer people, and thus, hopefully, fewer anti-fraud needs and problems. The IWC satellite office staffs operate independently, usually interfacing with customer representatives and other marketing and salespeople. The business environment and even the culture are different from those of the rest of IWC. You may have security managers or supervisors assigned to each satellite office to act as your representatives.

The off-site security managers' or supervisors' anti-fraud related job is to provide input to the anti-fraud program project team and especially to explain any unique differences in their working environment from that of the main office. Once the anti-fraud program is implemented, their primary relative job is to ensure compliance and offer advice to the satellite office staff as part of their overall services and support function.

TEAMING AND DEALING WITH SATELLITE OFFICES IN FOREIGN LANDS

Not surprisingly, the biggest problem with satellite offices located in foreign countries is their great geographic separation from the main business units. Other issues that impact a CSO's ability to provide overall effective and efficient anti-fraud program and CSO management oversight to those offices are that these offices:

- Have different cultures
- Speak different native languages
- Obey different government laws
- Employ mostly citizens of the foreign state, who may thus see things differently
- Use local management employing foreign methods to manage most of the functions
- Operate in different time zones

These all contribute to creating an environment that is more difficult to manage and also perhaps less safe from fraud-threat agents. As in the case of IWC, the employees in these offices operate independently with little or no supervision. Since they include sales and marketing functions, much like satellite offices in the United States, but also manufacturing facilities,

they share some of the same fraud-threat agents and vulnerability issues of those of the U.S. manufacturing plants and offices. Satellite offices must operate within the legal structure of the country they are in. This does not mean that the laws of the nation-state where the corporation is headquartered (e.g., in the United States for IWC) are not applicable to these offices; however, the laws of the country they operate within are paramount.

As the IWC CSO, you have the responsibility to work with satellite offices and the company's international lawyers to assess potential vulnerabilities and problems. As with domestic satellite offices, perhaps the best anti-fraud defense you can provide is to help them develop and incorporate an anti-fraud briefing into a security awareness program. This should increase employee consciousness of fraud in general and make them aware of potential fraud-threat attacks, vulnerabilities, and problems. However, three other functions are also very important for successfully protecting IWC assets at these foreign locations:

- Close liaison with the local law enforcement and security agencies
- Fraud-related risk assessments relative to the assets at those facilities
- An IWC anti-fraud program subset for each IWC foreign facility, which takes into consideration their unique environment. (*Note*: the basic IWC anti-fraud program should only be changed to meet the unique needs of the foreign office and should not detract from the IWC's overall anti-fraud posture.)

Based on the location of IWC's foreign offices and manufacturing plants in Asia and Europe, the CSO, with the approval of IWC executive management, has hired a U.S. citizen with security, anti-fraud, and management experience to head up each security offices abroad. Those managers were recruited away from firms already operating in those continents; therefore, travel/moving costs were minimized. In addition, they were already familiar with the local cultures.

CASE STUDY

The success of using teaming concepts will adversely be impacted by conflicts and by how you as the IWC CSO deal with the conflicts.

Assume that you as the IWC CSO have just been informed of some conflicts between members of your anti-fraud project team. How would you deal this problem?

The following information is offered as one approach to consider:

Managing conflict and dealing with difficult people is part of a CSO's job. Failure to properly deal with conflicts as they may arise on the anti-fraud program project has a direct bearing on the overall success of the

program. It is not the fun part, but it is a necessary part. Failing to deal with conflict or difficult people is a recipe for disaster.

When you do not confront conflict or difficult people, you reinforce their negative behavior. Conflict will not go away on its own. You must deal with conflict when it occurs and deal with these people early on. Before confronting those in conflict, try to determine what may be causing their improper behavior. Think about why they are acting in such a negative way:

- Is it something you or one of your managers directed the team to do that is the basis for the conflict?
- Are their differences in interpretation in management direction as to the best way to proceed?
- Have personality problems arisen on the project?
- If so, who are the ones in conflict?
- Do they have personal problems that are affecting their work?
- Are they having disagreements with other employees that continue to fester?

You and/or your security manager may need to consult with others, such as Human Relations specialists, to help you understand what is going on. Think about the consequences of conflict and what you must do to eliminate it. After you have thought through the situation, you must decide to ask the employee manager to confront the person or persons involved; you may want to sit in on the meeting; or you may want to handle it yourself — depending on the circumstances and personalities involved.

One word of caution: remember that if the employee does not work directly for you the CSO but for one of your managers, that manager is the one who must take the action with your support. Since people are not mind readers, you should discuss the matter with the manager of the employee:

- Tell the manager what you know about the conflict.
- Be brief and to the point.
- State the facts and your observations, but don't dwell on them.
- Approach the situation in a positive way but be firm.
- Do not argue if the person becomes angry.
- Try to establish a positive tone.
- Listen to what everyone has to say.
- Share your perspective and concerns without being condescending.
- Never, never embarrass or humiliate the people involved.
- Treat them with dignity and respect.
- Be firm and committed in expressing your concerns and expectations.
- Ensure that the conflict and issues are resolved and that everyone concerned agreed to the actions taken.

SUMMARY

Teaming is necessary in today's corporate environment. It has both advantages and disadvantages. It allows for the sharing of resources from other departments in order to successfully provide IWC with an anti-fraud program. It also has disadvantages, including often gaining a consensus rather than leading an aggressive effort without others trying to tell you how they think it should be done. One advantage of others' input is that they may have good ideas; a negative consequence is that they may be wrong and conflicts between team members may arise.

To be successful, the CSO must use teaming techniques to gain the support of all IWC managers and employees, including executive management, other managers, employees, associates, suppliers, and subcontractors.

12

Anti-Fraud Functions

INTRODUCTION

As part of IWC's anti-fraud program, certain anti-fraud functions must be performed. In order to get the best use of the available resources, the IWC CSO will direct that the anti-fraud program project team identify those functions that should be performed in order to establish and maintain an efficient and effective IWC anti-fraud program.

ANTI-FRAUD PROJECT TEAM FUNCTIONAL TASKS

One thing the CSO has recently learned and explained to the anti-fraud project team is that executive management has decided that no additional budget is to be allocated to the anti-fraud program. Therefore, it is incumbent upon the CSO to ensure that the project team understands that and focuses on allocation and reallocation of resources instead of proposing that more resources be added to the security department.

Since the IWC anti-fraud program will be a subset of the IWC assets protection program, some of the assets protection program functions can be expanded to incorporate the anti-fraud defensive measures.

Furthermore, the CSO directed that the anti-fraud program project team look at other departments within IWC to determine which ones (e.g., auditors, legal staff, ethics specialists) could provide additional or supplemental support to meet the objectives of the anti-fraud program.

The project team was also directed to:

- Identify all anti-fraud functions that would be unique.
- Develop a job description for each of those functions.
- Identify the reallocation of security department resources that would allow the implementation of the function, including:

- Logic for that reallocation
- The benefits of the reallocation
- The costs of the reallocation in terms of budget and adverse impacts to the security department's other duties and responsibilities
- Providing the CSO with any other information to assist the CSO in making that reallocation decision

The anti-fraud project team, through research, determined how other corporations handled their anti-fraud duties and responsibilities, including unique and general assets protection functions. They found that very few had established an anti-fraud program and those who did just expanded their assets protection functions to place greater emphasis on fraud-related matters.

The question then arose: Is a separate, albeit subset of the assets protection program actually needed at IWC? The CSO advised the project team that the idea of an anti-fraud program was based on the history of fraud-threat agent attacks against IWC and executive management's decision to place greater emphasis on anti-fraud defenses. They did not care how it was accomplished as that was the CSO's problem.

The CSO decided that the anti-fraud program as a subset but highlighted would emphasize IWC's anti-fraud philosophy and get IWC employees and others to view it as an important program for protecting IWC assets. Furthermore, after several serious past frauds against IWC, the government agencies that were concerned about IWC management protecting the stockholders' (owners') corporation would see that IWC management was placing a great deal of emphasis on fighting fraud and protecting the stockholders' value.

ANTI-FRAUD FUNCTIONS

The anti-fraud project team identified the following primary asset protection functions that were now being performed by IWC's security department:

- Administrative Security: assets protection plans, policies, processes, programs
- Physical Security: physical access control
- Personnel Security: preemployment background checks and workplace violence program
- Security Education and Awareness Training Program: assets protection briefings and related training programs
- Fire Protection: fire prevention, protection, and response
- Contingency Planning: business continuity, emergency response, crisis management, and contingency planning

- Investigations: investigations or inquiries into violations of IWC directives
- Government Security: assets protection and other support to IWC's government contracts
- Information Security: assets protection related to automated information, computer hardware, software, and related telecommunications systems
- Executive Protection: physical protection of specified members of executive management
- Event Security: assets protection projects related to IWC's sponsored events such as the annual stockholders meeting

The anti-fraud project team also found that each of these functions was authorized to conducted risk assessments and analyses related to areas under their function.

The project team found that the following security functions duties and responsibilities should be expanded to incorporate anti-fraud program functions:

- Administrative Security: Provide administrative oversight for the anti-fraud program by having the anti-fraud project team develop the program under this security organization, and once the program was implemented, to ensure it was maintained current at all times.
- Personnel Security: Ensure that all preemployment checks incorporated, in addition to normal law enforcement check inquiries, the applicant's credit, indications of bankruptcy and interviews of individuals who could vouch for the integrity and ethical conduct of the applicant.
- Security Education and Awareness Training Program (SEATP): Incorporate anti-fraud briefings, pamphlets, and training into the overall SEATP.
- Contingency Planning: Incorporate responses to fraud-threat agent attacks into the contingency planning function, including responsibilities for coordinating with the Administrative Security staff to have a fraud attack response team and processes in place to be initiated in the event of an attack.
- Investigations: Handle responsibility for conducting preliminary investigations into allegations of employee violation of government laws and regulations; inquiries to prove or disprove allegations of employee violation of anti-fraud program policy, procedures, and processes; coordination of investigations and inquiries with the IWC ethics director and IWC legal staff, and local law enforcement, when outside coordination is approved by executive management after legal staff consultations.

- Government Security: Serve as the focal point for all fraud-related matters concerning government contracts.
- Information Security: Incorporate anti-fraud defenses into the IWC computers and related networks.

The anti-fraud project team recommended that an anti-fraud specialist be assigned to provide oversight for the CSO relative to the anti-fraud program and all its aspects since so much of the anti-fraud functions were spread over almost the entire IWC security department. That person would report to the manager of the administrative security organization and be responsible for maintaining the anti-fraud program, related plans, and the like.

The CSO decided that each security manager or security organizational supervisor would be the focal point for the anti-fraud day-to-day level of efforts (LOE) within their security function. The CSO concurred with the project team recommendation and established a position within the Administrative Security organization to be the overall focal point within the IWC security department, who reported to the manager of that organization. This change was accomplished through reallocation of available resources within the security department.

ANTI-FRAUD PROGRAM'S NON-SECURITY TEAM FUNCTIONS AND MEMBERS

The anti-fraud project team identified other IWC departments that should be integral team members by function and support to the IWC anti-fraud program, as follows:

- Auditors: The CSO would coordinate the security department's anti-fraud matters with the manager of audits, who would identify the audits to be performed and incorporate anti-fraud indicators checks in all audits. The CSO and manager of audits would meet periodically to discuss anti-fraud areas of mutual concern.
- Ethics Director: The ethics directors would have the CSO as a member of the IWC Ethics Committee, and the CSO's investigations organization would conduct all fraud-related inquiries and investigations requested by the ethics director, except those minor allegations whose inquiry could easily be conducted by the applicable IWC manager.
- Legal Staff: The IWC legal staff would provide legal advice concerning fraud-related matters brought to them by the members of the investigations organization, security anti-fraud specialist, and the CSO.
- Human Relations Specialist: The Human Relations Department specialist would act as a focal point on employee matters in which some fraud-related matters were identified.

The anti-fraud program project team also recommended that the CSO head an IWC anti-fraud committee to coordinate and discuss fraud matters of mutual interest. The CSO agreed in principle to such a committee but decided against forming a separate IWC committee. Instead, in coordination and with the agreement of the ethics director, the ethics director's monthly ethics committee meeting, which includes the CSO, audit department manager, legal staff representative, and Human Resources representative, would be used as the forum for discussing fraud-related matters.

The CSO reasoned that such matters would fit well into the committee's charter of duties and responsibilities, as fraud allegations were often received via the Ethics Hotline, and all fraud-related allegations were also allegations of unethical conduct.

CASE STUDY

As the IWC CSO and member of the IWC ethics director's Ethics Committee, how would you respond to a request to conduct an inquiry into a series of anonymous Hotline calls concerning allegations of falsification of timecards by various personnel within an IWC department? These calls appeared to be coming from one person and started when that department announced a series of employee layoffs within that department.

Would you decline to conduct an inquiry or conduct an inquiry?

As the CSO, you could decline the inquiry because it seems that someone is trying to make other employees look bad and hope that such accusations would put those employees at the head of the layoff list, thus (in the eyes of the caller) protecting the job of the anonymous caller.

On the other hand, these may be valid calls and not previously reported as the person making the calls did not want to get involved — until the latest layoff announcement was given to IWC employees.

What if the ethics director did not agree and requested that the CSO's staff conduct the inquiry? If you declined, the ethics director might take the matter to your boss, or at least your relationship with the ethics director would suffer. In that event, the ethics director might decline to refer a potential fraudulent matter to you because you declined the request for inquiry in the past.

Would you recommend that the manager of the department wherein the allegations were made be told of the matter, and would you request to conduct an internal inquiry? The upside is that this matter would no longer be one for the CSO. The downside would be that such an inquiry would be conducted by inexperienced people, might cause undue animosity in that department, and might also make the Ethics Hotline process appear to be indicative of a "witch-hunt."

In this case, the IWC CSO agreed to have the security department's investigations organization to, as covertly as possible, conduct an inquiry

to prove or disprove the allegations and provide a report of findings to the ethics director and the department's manager.

SUMMARY

Anti-fraud program functions can be viewed as independent functions, or they can be integrated into the normal security department functions. The CSO's decision in that regard is often based not only on what executive management wants but also on the available budget allocated to the security department.

The most cost-effective approach, assuming limited budget — and security budgets are almost always limited — is to integrate the anti-fraud functions into the applicable security department functions and also into other IWC department functions, when logical to do so and upon agreement with the managers of the other departments.

13

Are We Winning the Battle? How Do We Know? Measure It!

INTRODUCTION[1]

Thus far we have discussed how to develop and manage an anti-fraud program. When the program is implemented and basically goes into maintenance mode, how do you know that the anti-fraud program is meeting the goals and needs of IWC? In other words, how do you know that it is successful? We touched on some ways to measure in the previous chapters. Now, we will focus on an anti-fraud metrics management system.

Another thing that the IWC and probably executive management would like to know besides whether the IWC anti-fraud program is successful is how much it is costing. Is there a cost benefit to the anti-fraud program? Is IWC getting a return on its investments?

As the CSO, are you in a position to answer such questions? If not, then you are not doing your job as a CSO and a member of the IWC management team. You may in fact be wasting resources and impeding productivity by requiring certain policies, procedures, plans, and processes be in place and followed, which in fact do not provide a cost benefit vis-à-vis protection of IWC assets from fraud attacks.

In order to not waste valuable IWC resources or abuse them, the IWC CSO must develop some measurement processes to help answer the above questions.

---

[1] Portions of the information provided in this chapter was excerpted with permissions from: *Security Metrics Management: How to Measure the Costs and Benefits of Security*: December 2005, co-authored by Dr. Gerald L. Kovacich and Edward P. Halibozek; published by Butterworth-Heinemann.

MEASURING AN ANTI-FRAUD PROGRAM'S COSTS, BENEFITS, SUCCESSES, AND FAILURES

When we talk about metrics, we are talking about a system of measuring the costs, benefits, successes, and failures of the IWC anti-fraud program.

As previously stated, there are two basic categories of anti-fraud program actions: (1) the level of effort (LOE), in other words the day-to-day operations such as conducting fraud inquiries. Although each inquiry has a beginning and an ending, the function itself is an ongoing function.

(2) There are also projects that have a stated objective with beginning and ending dates. These projects are not ongoing and are used as a formal management tool to make changes in some part of the anti-fraud program, for example, a change in a process. So, pretty much by definition, projects are measurable in that they include a list of tasks to be performed, the time it takes to perform them, and the cost of performing the tasks.

In addition, projects can be easier to measure as one can use project management software to keep track of incurred costs in materials, labor, and the like. This type of measurement is rather straightforward. Where many CSOs have difficulty is in measuring the LOE costs.

The LOE costs, benefits, successes, and failures must also be measurable. If not, then how do you know they are worth performing or whether they are working out as planned?

So, when we talk about a security and anti-fraud program's metrics management approach, we are talking about those related primarily to LOEs as projects already have built-in measurement processes. What the CSO needs is a similar built-in measurement for, as a minimum, each of the LOE anti-fraud program functions.

As you will recall, the security department's primary anti-fraud functions have been identified as:

- Administrative Security
- Personnel Security
- Security Education and Awareness Training Program (SEATP)
- Contingency Planning
- Investigations
- Government Security
- Information Security

In addition, the other IWC departments employ the following personnel to perform anti-fraud program support functions:

- Auditors
- Ethics director
- Legal staff
- Human Relations specialist

As it relates to the other IWC department's anti-fraud program support functions, the CSO does not want to impose measurement standards on these departments but can use their support to measure the LOE that flows from their support. Furthermore, other IWC departments can provide an estimate of how much time they use to support the anti-fraud program so that a total IWC cost estimate of the anti-fraud program can be made, excluding the costs by employees.

A word of caution here: be careful that the other departments don't try to charge or make a case for charging their anti-fraud tasks to your budget. Managers are always looking for ways to decrease their budget or obtain additional budget. So, don't put it past any of them to try this approach. After all, they are part of one or more aspects of the anti-fraud program processes and support the CSO in the CSO's anti-fraud program responsibilities.

COMMON LOE MEASUREMENT TECHNIQUES FOR EACH FUNCTION

Certain common measurement techniques can be used across the CSO's anti-fraud program functions. Remember that each LOE function should be measured to determine whether it is operating efficiently and effectively as determined by measuring its processing times, costs, benefits, successes, and failures.

How does the CSO establish the common measurement system for each function? The first thing the CSO should do since no measurement system is currently in place is to facilitate tracking processing time, costs, benefits, and so on, and initiate a project plan with the goal of developing a common measurement system across all anti-fraud program-related functions.

As part of that project plan, the following tasks, as a minimum, have been identified for action:

1. Determine the anti-fraud policy drivers and requirements for each function: if there is no driver or requirement for a specific anti-fraud LOE, then why do it?
2. Determine the policies that are used by the functions: policies should come from the drivers and requirements.
3. Determine the procedures that are used by the functions: they should be the most effective and efficient way to do the anti-fraud work.
4. Determine the processes that are used by the functions: processes should be continually evaluated to be sure they are as effective and efficient as possible.
5. Determine the costs to perform the functions in terms of equipment, people, and other support material using a process improvement methodology.

6. Determine the objective of each function: each objective should be linked to the drivers, requirements, and so on.
7. Determine whether each function is meeting its objective.

These tasks are then mapped using a flowchart process for each function so that the CSO can see the "big picture" for each function and also obtain the related costs and ascertain whether process improvements are required.

The IWC CSO decided to evaluate and measure the security department's anti-fraud program functions separate from the entire function (e.g., SEATP), which as you recall includes other aspects of assets protection functions. The CSO decided that the focus was on the anti-fraud program first as it is new compared to the assets protection program and provides a smaller piece of the CSO's management oversight duties and responsibilities.

The CSO will subsequently use the same approach for evaluating the entire LOE functions within the security department as a separate project. This approach will later be used in a separate project to analyze the cost benefits of the support departments to the CSO and the anti-fraud program — from the CSO viewpoint. Any changes that the CSO seeks from a support department will be requested using the results of the project plan for that support department's analyses.

EXAMPLES OF METRICS BY FUNCTION

Investigations and Noncompliance Inquiries

Anti-fraud investigations and noncompliance inquiries (NCI) are both anti-fraud program LOE functions, which, at some corporations, may be candidates for outsourcing. At this time, both are internal functions at IWC. At IWC, these two functions are very similar. However, the primary differences are scope and magnitude. That is, the term *NCI* is used to describe an investigation that is conducted due to a violation of corporate policy or procedures where a law has not been violated. At IWC an investigation is generally a much more complex process associated with a more serious situation and would involve a violation of the law or a regulation external to the corporation.

One primary reason for the differentiation is for public relations purposes. When one hears that an investigation is being conducted, it sounds more serious than if one hears a NCI is being conducted. In addition, an NCI may be used as a preliminary inquiry to assess if something is wrong and requires a full investigation. An NCI may be conducted by nearly any security professional or member of management. An investigation requires someone skilled in the techniques and processes of investigations, which

will need to have a working relationship with different governmental investigative organizations (local, state, and federal).

INVESTIGATIONS AND NCIS METRIC CHARTS

The Investigations and NCI function's primary drivers are identified and graphically depicted. In this case, the complaints and allegations from various sources are considered the security drivers. (See Figures 13-1 and 13-2.)

Beginning with this overview diagram, the CSO's security manager and staff can begin to analyze the function in more detail, identify each step in the process, and determine:

- The time it takes to do each step in the process
- The number of people involved in each step
- The number of times one LOE is performed each month (e.g., one NCI)
- The pay of each person involved in each step broken down into an hourly wage
- The cost of the equipment and supplies that support the function

Using this information for each fraud investigation and fraud NCI, one can begin to determine the costs of this function in total and also broken down by labor, equipment, supplies, and such.

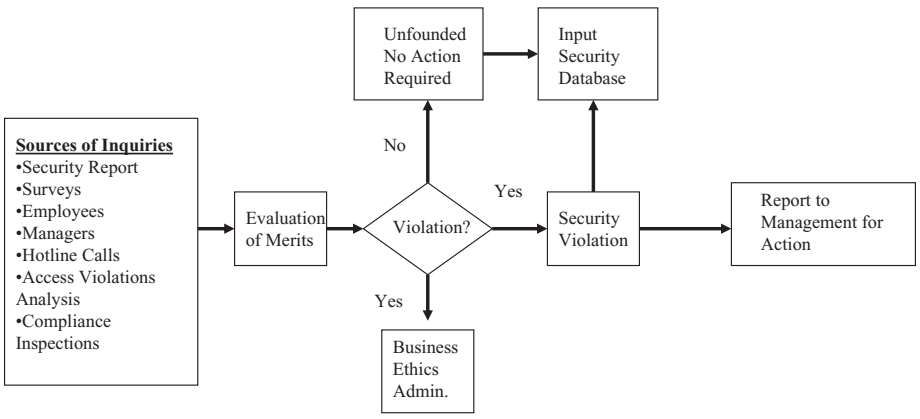


Figure 13-1. Overall flowchart of the drivers of investigations and noncompliance inquiries (NCI).

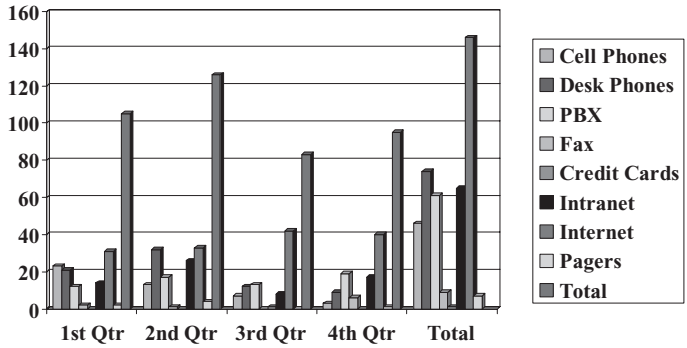


Figure 13-2. Number of technology fraud-related NCIs by calendar quarters and by type.

One can also add the square feet of office space, use of utilities, and the like if micro-detail is needed. In doing so, however, one must look at such costs across all investigations and inquiries and then take the total number that makes up the fraud investigations and NCIs and prorate the costs accordingly for fraud investigations and NCIs.

This approach can be used for all anti-fraud functions.

Remember: one important driver for the Investigations and NCI process is the total number of IWC employees: The more employees, statistically the larger number of employees who will violate IWC's anti-fraud program policy, procedures, or government laws.

Another driver is the number of fraud-related requests for support from other organizations (such as the legal and ethics staffs and their need to have investigators support their processes). Remember that the Investigations and NCI organization is also a service and support organization and as such must provide professional support to other IWC organizations when that service and support is requested and determined to be warranted.

EXAMPLES OF ANTI-FRAUD INVESTIGATIONS METRICS

A CSO can use many different anti-fraud metrics to help understand, assess, and manage the fraud investigations and fraud NCI processes. A problem that may face the CSO, as with all other security metrics, is determining the most useful metrics. When in doubt as to the most valuable metrics, the CSO can start by identifying as many as possible and then sort through them to determine which offer the most utility.

Don't forget that once the CSO or project team appointed by the CSO develops a process flow diagram depicting the macro process and then develops flow diagrams for the investigative subprocesses or micro processes, the CSO can begin to develop points for different processes measurements.

An example of such a data collection list for fraud investigations may look like the following (a list for the NCI function would be almost identical):

- Number of investigations opened per month
- Number of investigations closed per month
- Number of investigations pending per month
- Average time used to conduct an investigation
- Average cost in terms of investigator's time, IWC employees' time, administrative time, and cost of resources used
- Same information as above broken down by type of fraud investigation
- Same information as above broken down by quarters, year, and multiple years
- Identification of the IWC departments where the incident took place
- Identification of the IWC departments where the subject (employee) of the investigation was assigned
- Number of allegations proven correct
- Number of allegations proven wrong
- Subject of investigations employees' position and job code
- Type of investigations broken down by departments
- Department information broken down monthly, quarterly, annually, and multiple years
- Association of a cost chart with each of the above charts, where applicable

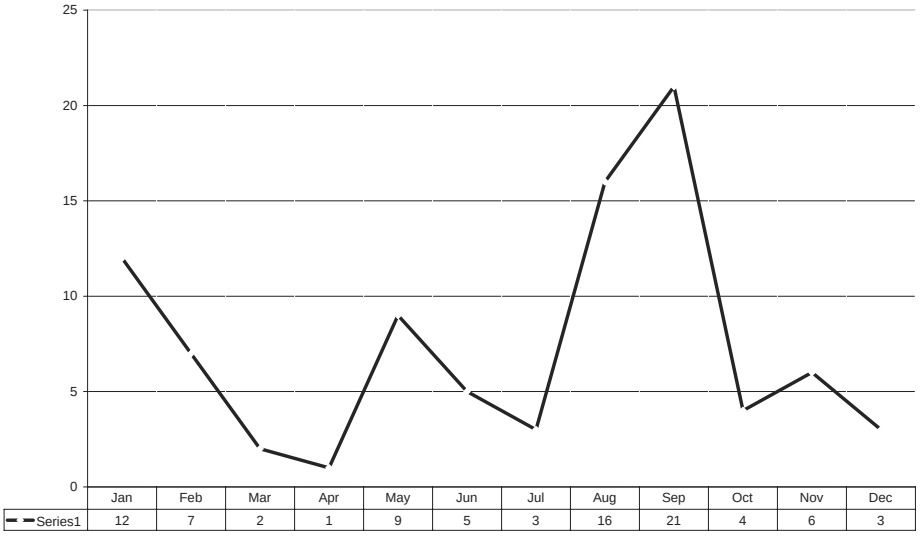
By using this approach, one can begin to get a sense of the type of information that offers potential for developing useful metrics. Furthermore, the CSO can relate the potential data points to what he or she needs to know. For example, if the CSO is attempting to determine the average time to conduct a fraud investigation, tracking the time taken to complete all steps from the opening of an investigation to the closing of an investigation will provide that data. The CSO can further analyze that information by sorting investigations by type. An investigation into the fraudulent timecards, on average, may require less time than an investigation into fraudulent use of information systems.

Remember also that once the time elements are known they can be costed-out by using the salary rate on an hourly basis for the investigator, those interviewed, time conducting records' checks, surveillance, report writing, and the like.

Metrics developed and used in the fraud investigations and fraud NCI processes may provide value beyond the investigative processes itself. Trend data may be developed and used to drive changes in other routine anti-fraud policies, procedures, and processes. For example, if investigative trend data or fraud survey results reveal the potential for travel voucher fraud by a group within one department, additional controls may be implemented for that department or throughout IWC to deter the submission of fraudulent expense claims; for example, a travel briefing can be given to the employees before they go on a business trip and in that briefing (preferably provided online for convenience and to save money) it can be explained that controls are in place to identify fraudulent travel claims and that such claims once submitted by the employee and proven false would be grounds for employment termination.

The information gathered may be used proactively to reduce the number of incidents requiring fraud investigations, thus reducing the overall workload for security investigators. Learning from security incidents helps prevent their occurrence in the future.

The following figures (13-3 through 13-9) are just a few examples of graphically depicted security metrics charts that a CSO may find useful in the effort to assess the effectiveness of the Investigations and NCI process and better manage the organization.



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Series1	12	7	2	1	9	5	3	16	21	4	6	3

Figure 13-3. Number of fraud-related NCIs conducted in 2006 by month as a line chart.

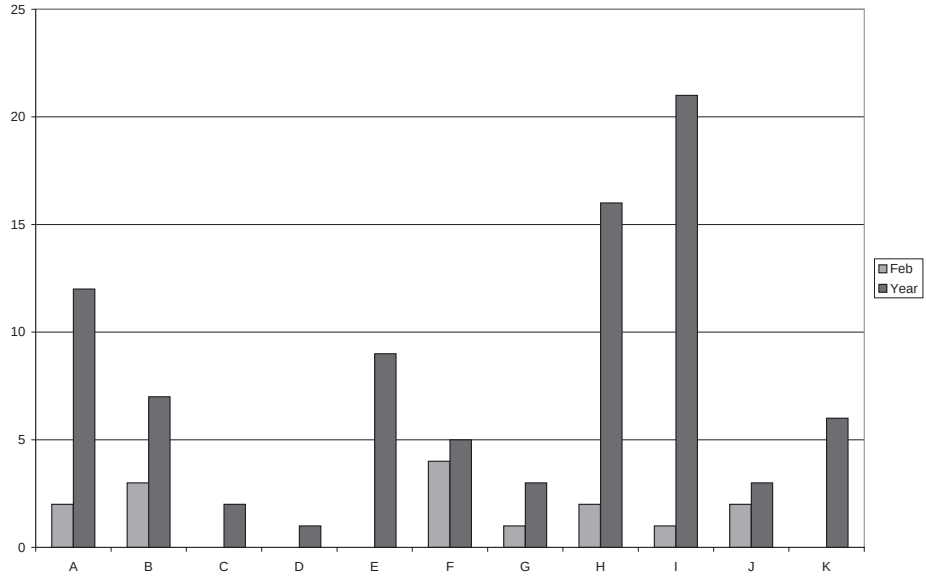


Figure 13-4. Number of fraud-related NCIs conducted in 2006, by department.

- The number of IWC employees has increased based on IWC's need to rapidly build up the workforce to handle the new contract work.
- The number of fraud-related noncompliance inquiries has increased during that same time period.
- The number of fraud-related investigations has increased during that same period of time.
- This increased workload has caused some delays in completing the inquiries and investigations in the 30-day period that was set as the goal.
- The ratio of incidents compared to the total number of employees indicates:
  - Personnel may not be getting sufficient information during their new-hire briefings.
  - Personnel being hired may not be thoroughly screened prior to hiring.

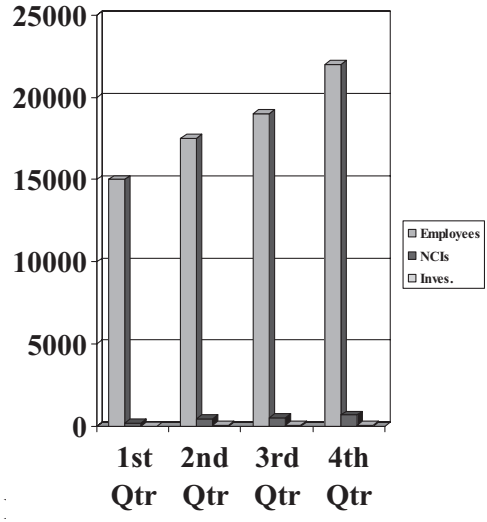


Figure 13-5. Number of fraud-related investigations and NCIs in 2006 based on IWC population.

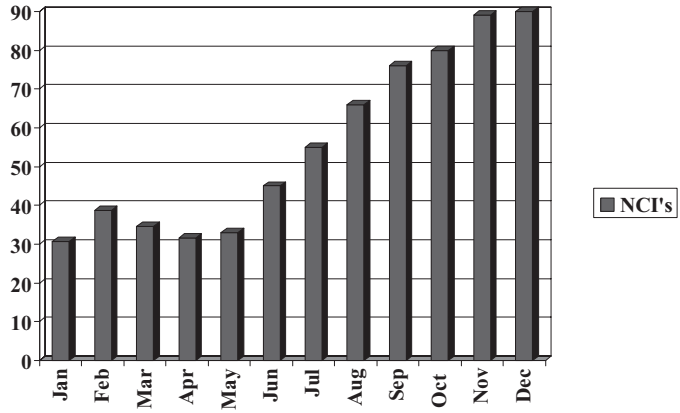


Figure 13-6. Number of new fraud-related NCIs per month — all locations — 2006.

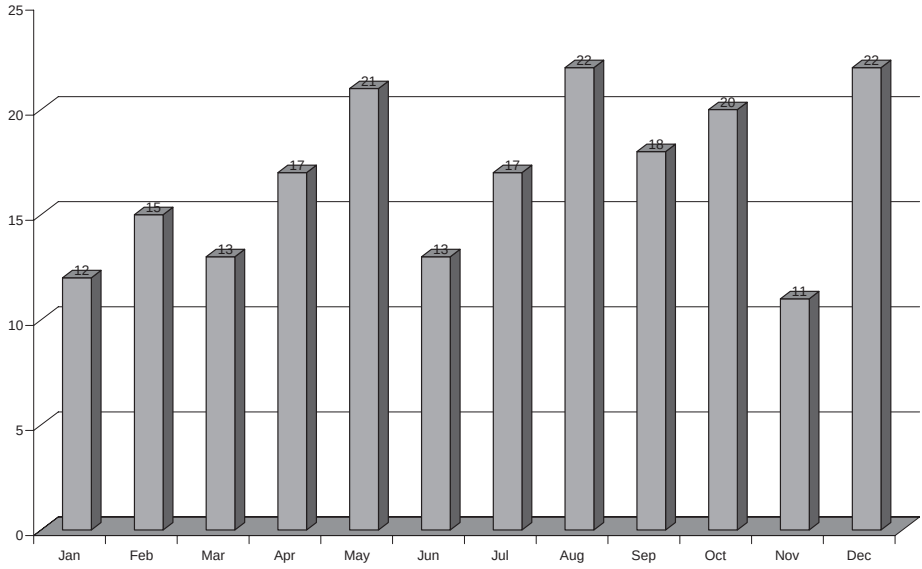


Figure 13-7. Number of NCIs conducted per month by average time per NCI.

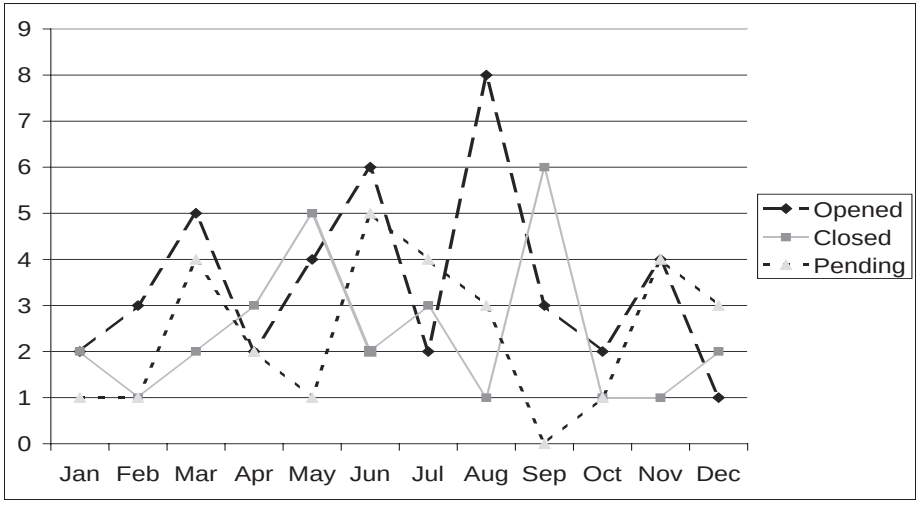


Figure 13-8. NCIs opened, pending, and closed per month.

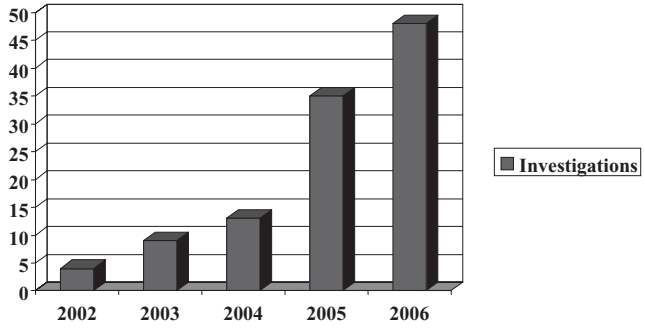


Figure 13-9. Total number of fraud-related investigations over a five-year period.

PROCESS MEASUREMENTS

Process measurements can tell you a lot about a process. The type of measures used should correlate to what the CSO wants or needs to track and understand. For example, if it is important to the CSO to know what percentage of cases are closed each month, then that information should be tracked, quantified, and a cost associated with each, total and average.

The ultimate goal for the CSO should be to understand what it is that drives the need for fraud-related NCIs and investigations. Can those drivers be changed to such a degree as to eliminate or reduce the need for fraud-related NCIs or investigations? Maybe employees are not aware of some anti-fraud controls in place and thus violated them out of a lack of knowl-

edge. Or perhaps more emphasis in the anti-fraud portions of the SEATP and a special online bulletin to each employee would make them all aware of the controls and how to follow the proper procedures. Measuring will also tell the CSO if the changes made had any effect on the process. Of course, cost issues must always be considered

> Quality in a product or service is not what the supplier puts in. It is what the customer gets out and is willing to pay for. A product is not quality because it is hard to make and costs a lot of money, as manufacturers typically believe. — *Peter Drucker*[2]

So, by linking drivers and requirements to policies to procedures to processes and so on, one can begin the analyses of each fraud-related function to determine their costs, whether or not such function should be performed in the manner prescribed — in other words, determine the most cost-effective approach to complying with the anti-fraud program, making changes to the anti-fraud program and minimizing violations of the anti-fraud program defensive measures (e.g., controls).

CASE STUDY

As a CSO, you decided that it would be a good idea to use the anti-fraud program driver's metrics, which tracks the number of employees, the number of anti-fraud inquiries, and investigations conducted over time. You have gone through the analytical process to make that decision based on answering the following how, what, why, when, who, and where questions:

- *Why* should this data be collected? To determine the ratio of employees to the workload, manpower requirements could therefore be forecasted over time.
- *What* specific data will be collected?
  - Total number of IWC employees
  - Total number of anti-fraud noncompliance inquiries
  - Total number of anti-fraud investigations
- *How* will these data be collected?
  - Total Employees: The collection will be accomplished by taking the total number of paid employees from the Human Resources Department's master personnel database file.

[2] http://www.quoteland.com/search.asp.

  - Total Number of Fraud-Related NCIs: This information will be gathered by the unit coordinator from the unit's NCI database file.
  - Total Number of Fraud-Related Investigations: The unit coordinator will also gather this information from the unit's investigations database file.
- *When* will these data be collected? The data from each of the previous months will be compiled on the first business day of each of the following months and incorporated into the crime investigations drivers' graph, maintained on the Investigations and NCI's administrative information system.
- *Who* will collect these data? The data will be collected, input, and maintained by the unit's coordinator.
- *Where* (at what point in the function's process) will these data be collected? The collection of data will be based on the information available and on file in the Investigations and NCI's database at close of business on the last business day of the month.

The CSO organizational manager and security staff can analyze the NCI data, for example, to determine:

- The reason for each employee's noncompliance
- The position and organization of the employee
- The employees' seniority dates
- Identification of the patterns
- Main offenses

That information would then be provided to the project team assigned to the goal of decreasing the need for fraud-related NCIs and Investigations. Based on that information, the briefings would be updated and more emphasis placed on those areas causing the majority of problems. In addition, the departments with the highest number of fraud-related NCIs and investigations may be targeted for special briefings and meetings with the department managers to discuss ways of improving their anti-fraud program support.

Remember that numerous types of graphic depictions of data can be a great tool for management. They include bar charts, pie charts, and line charts and can be monthly, quarterly, weekly, or annually. The timeliness of the charts should be dependent on the manager's need for the information.

The key to the data collection and their related graphic depictions is to give more attention to trends than to monthly numbers. The goal is to continue to maintain and improve on positive trends. Negative trends should be analyzed for systemic causes, and project plans should be implemented to reverse the negative trends. The metrics could then be used to monitor the process and to determine whether process changes actually

cause the reversal of the negative trends. If not, then new analyses and a rethinking of the problem are needed.

The organizational manager in coordination with the CSO began this process by, of course, identifying the drivers requiring the functions to be performed. Subsequently, the processes were flowcharted, and a process analysis summary was developed to help provide a high-level view of the process. That process summary included the following information:

- Security Department: Investigations and NCIs
- Process Definition: Professional fraud-related investigative services in support of IWC and its customers
- Subprocesses
  - Conduct fraud-related investigations
  - Conduct fraud-related NCIs
  - Conduct fraud prevention surveys
  - Conduct fraud prevention special briefings
- Requirements and Directives that Govern the Process
  - IWC's Assets Protection Program (IWC APP)
  - Contractual security requirements
  - Position descriptions
  - Corporate policies
- Suppliers
  - IWC employees
  - Customers
    - IWC management
    - IWC customers
- Input
  - Complaints
  - Allegations
  - Requests for assistance
  - Security requirements
- Output
  - Investigative reports
  - NCI reports
  - Inspection reports
  - Fraud risk assessment reports
  - Fraud survey reports
  - Briefings
  - Testimony
- Key Metrics
  - Subprocess 1: Case totals year-to-date and five-year trends, case aging charts
  - Subprocess 2: Fraud Prevention Surveys completed; Results; and Cost-Benefits charts

    - Subprocess 3: Number of fraud-related NCIs completed each year; costs; and IWC departments where conducted
    - Subprocess 4: Number of fraud-related investigations completed each year; costs; and IWC departments where conducted
- Customers and Expectations
    - IWC management (Internal customers): Timely and complete investigative and NCI reports
    - IWC customers: Timely and complete investigative and NCI reports as applicable to external customers
    - All: Most effective and efficient anti-fraud program possible.

Using the preceding identification process, the IWC CSO can not only view a summary of investigative and NCI organizational fraud-related metrics and processes but establish a form or format for such summaries and require their use throughout the security department.

SUMMARY

Metrics is an excellent managerial tool that can be used to determine the costs, benefits, successes, and failures of the IWC anti-fraud program. Project plans are a formal management tool used to establish measurement projects and subsequent processes. The LOEs are the anti-fraud program functions that can also be measured and subsequently analyzed to ensure the most cost-effective and efficient anti-fraud program possible.

This page intentionally left blank

III

THE FRAUDULENT FUTURE

Section III, the final section of this book, summarizes the author's views on future corporations and frauds, on where high technology is headed, and on what that means to you and fraud-threat agents.

The final chapter provides a summary of the main points of this book, as well as some final thoughts about fraud. The four chapters of Section III are:

Chapter 14 What Will the Fraudulent Future Hold for Corporations?
Chapter 15 The Impact of High Technology on Fraud
Chapter 16 What the Security and Other Anti-Fraud Professionals Must Do Now to Personally Prepare to Combat Tomorrow's Frauds
Chapter 17 Summary and Final Thoughts

Upon completion of this last section of the book, you should:

- Have a basic understanding of the twenty-first-century corporate environment, fraud-threat agents, and their modus operandi.
- Know how to establish and manage a basic anti-fraud program for a corporation or other business entity.
- Be able to begin to defend corporate assets against defrauders and potential defrauders.
- Gain some insights into who should lead an anti-fraud program so that you can decide for yourself where such a position should be located within the bureaucracy of a corporation.

This page intentionally left blank

14

What Will the Fraudulent Future Hold for Corporations?

INTRODUCTION

Two of today's best interpreters of trends and projecting them into the future are Alvin and Heidi Toffler. Over the years they have talked about viewing our history and the future in terms of "Three Waves." Use of the Tofflers' model of evolution provides a useful framework for discussing the future of corporations and fraud.

The *First Wave* is the agricultural revolution, which took thousands of years to develop, mature, and in some countries, has begun to fade. According to the Tofflers, this period — at least in the United States — started with the beginning of the human race and ended in about 1745. Obviously, agriculture is necessary for us humans to survive, but in modern societies, it does not have the force it once had. During this period, people lived in small and sometimes migratory groups, feeding themselves through fishing, foraging, hunting, and herding.

During this First Wave, information was passed by word of mouth or in written correspondence, usually sent by a courier. People were dispersed, and transportation was primitive. This meant that there was less contact among people. During this period, relatively few people could read or write.

Today very few nation-states remain in this First Wave of existence as technology has allowed the once less-advanced nation-states to begin to catch up to the rest of the world. For example, the use of cell phones has permitted developing nation-states to minimize their land lines for telecommunications and for the most part to go directly to wireless, which is a tremendous cost savings and permits faster communications development. They have also been able to take advantage of satellites provided by more modern nation-states.

The problem of fraud in the First Wave societies is as one would expect: it is mostly a one-on-one, person-to-person type of fraud. After all, defrauders take advantage of what they can, and defrauding a poor farmer offers little opportunities to be successful or profitable.

Although there were always defrauders around in the First Wave period, their schemes were generally not very sophisticated compared to today's fraud schemes because they lacked sophisticated technology to support their schemes. Furthermore, they were more localized owing to the lack of modern transportation systems.

The Second Wave, or what the Tofflers call the "rise of industrialized civilization", took less than three hundred years to develop and mature, at least in the United States. This was the age of steel mills, oil refineries, textile plants, mass assembly lines, and the like. People migrated to centralized locations to work in these industries. This period lasted until just a few years after World War II. In the United States, its decline, according to the Tofflers, is believed to have started about 1956, when for the first time, white-collar workers outnumbered blue-collar workers.

The Second Wave period saw the building of great cities and the era of great inventions like the telegraph, telephone, air transportation, automobiles, and computers. This period also witnessed expansions in education, mass transportation, and exponential growth in communications — the sharing of information.

The sharing of information became easier following the development of communications systems and the increased consolidation of people into large cities. This change also made it easier to educate the people, giving them the skills needed to work in the more modern factories and offices of the period.

The sharing of information through various communication channels brought new challenges. For communication protection, cryptography came into its own during this period. Cryptography was used primarily by the government as a high-technology anti-espionage tool. During the post–World War II years, the U.S. federal government owned most of the computers. Although businesses were beginning to look at the use of computers, most were cost-prohibitive; these systems were primarily operated in standalone mode. In other words, the computers did not talk to other computers.

As societies and corporations began massing into cities and using some of the advanced technologies that were coming into their own, the defrauders also migrated to the cities. However, since technology was limited, so was the defrauders' use of it. It is believed that they were able to take advantage of "modern" transportation systems to ply their fraud schemes throughout larger regions than in the past.

The *Third Wave*, the age of technology and information, is sweeping across the globe and will have done so in decades, not centuries.

> Mass production, the defining characteristics of the Second Wave economy, becomes increasingly obsolete as firms install information-intensive, often robotized manufacturing systems capable of endless cheap variation, even customization. The revolutionary result is, in effect, the demassification of mass production.[1]

We are now in the Third Wave, with some saying we are moving into the Knowledge Age; during this period, we have witnessed more advances than during the First and Second Wave periods combined. We have experienced the rapid growth of high technology, which is playing a major role in our rapidly changing world.

Remember the old business saying, "Time is money"? Well, in our world of international, global competition, that saying is truer now than ever before. Managers and security professionals must also understand this better than ever before. Fraud concerns cannot be a roadblock to business; however, the issue must be addressed.

Since this is "our age," it is easier to see the development of fraud in this period. Through today's technology and the advantage of technologies' vulnerabilities criminals have had more opportunities to successfully perpetrate frauds.

As suggested earlier, today's frauds are more sophisticated and more global, and their numbers have grown. It is expected that unless corporations take some significant actions, notably implementing aggressive antifraud programs supported by government agencies and a realignment of criminal justice priorities, the current trend of increasing frauds is expected to continue.

> Globalization is the term used to describe the changes in societies and the world economy that result from dramatically increased international trade and cultural exchange. It describes the increase of trade and investing due to the falling of barriers and the interdependence of countries. In specifically economic contexts, the term refers almost exclusively to the effects of trade, particularly trade liberalization or "free trade. . . . More broadly, the term refers to the overall integration, and resulting increase in interdependence, among global actors (be they political, economic, or otherwise).[2]

---

[1] Quoted from *Creating a New Civilization* by Alvin and Heidi Toffler, and published by Turner Publishing Inc., Atlanta 1995.

[2] http://en.wikipedia.org/wiki/Globalization

As the war on terrorism and violent crimes continue, it is expected that fraud will be given low priority by all concerned. However, even terrorists are using fraud schemes to gain access to funds for their attacks as governments continue to try to stop all illegal financial funding of terrorism around the world.

GLOBALIZATION OF BUSINESS TO CONTINUE

Corporations will continue to expand their markets, facilities, and areas of operation around the world, many of which are supported by the host nation-states that also benefit from such trades from:

- Increased employment of its citizens
- A rise in the nation-states' standard of living
- More tax revenue to the nation-states
- The ability of citizens to purchase cheaper goods

Many oppose globalization, believing that it contributes to the exploitation of the poor. Arguments can be made on both sides of this issue, but suffice it to say that globalization will not stop. Along with that expansion, increased risks due to today's and tomorrow's defrauders and their attack methodologies may be encountered for the foreseeable future.

All businesses evolve over time and take advantage of new markets, new technologies, and new processes as they become available. Today's business environment has become increasingly more global and more competitive with more corporations, foreign and domestic, competing with like products for the same customers.

Corporations have always sought ways to cut costs and increase profits. However, in view of today's rapidly changing business environment with increased competition from all over the world, this is no longer something to consider but something that must be immediately implemented as new ways are discovered to replace employees with robotics, streamline processes such as inventory, and the like.

For example, one day we may see robots reporting the news as news anchors. After all, those reporting the news from the newsroom desks basically just read the teleprompter. Since they are computerized, they can also provide updated news broadcasting through news media feeds from around the world.

EMPLOYEES OF THE FUTURE

Employees will continue to be the first to go in the effort to become more competitive. With modern corporations not only paying wages but also

providing very expensive benefits such as medical costs for employees, when employees are laid off, more than an employee's salary is being saved. Also being saved are the once paid-out benefits and even office space and office supplies. Although the saving of office space and supplies may seem trivial, just think about the cost of maintaining and leasing office space, and if a corporation were to reduce its employee base by say 1,000, an immense savings would be accomplished.

Corporations' executive management also consider the benefits of encouraging employees to leave after some period of time so that they can also save money in the following areas:

- Higher wages paid long-term employees
- Medical costs associated with employees; as employees stay on and get older, they are more susceptible to medical problems, which may increase over time and thus cost the corporations more money
- Retirement pay
- Corporations' agreement to match or provide some funds for an employee's long-term savings accounts

Corporations are for the most part no longer interested in employees who are loyal to the corporation over their working lifetime until retirement. They only want employees to be loyal to the corporation for the short period of time they will be employed and then move on.

In tomorrow's corporations, it will be very unusual for someone to work for the same corporation for 40 or so years, until they are ready to retire. It is also unlikely that these corporations will also hire their sons or daughters, who during the Second Wave would also work there until retirement.

Employees of the future will be of two basic types: generalists and specialists. Both will be needed, and each will be their own "company" and be hired for specific jobs for a specific period of time. Corporations will pay them a fee with no additional benefits.

There will be a demand (it is already starting in the United States) that these contracted employees have a "mobile" benefits plan for such benefits as medical and dental insurance. When not on contract, they will draw unemployment as they do today. They will also be able to build up retirement funds as they do today with some government support.

THE FUTURE GLOBAL CORPORATION

What will the future global corporation look like? It will continue to be dependent on and be process-driven by high technology. This situation will increase their process efficiencies and allow them to expand into new markets and in fact create markets where none exist today. This

dependency on high technology coupled with the products and locations will also make them more and more vulnerable to fraud-threat agents.

> The ability to learn faster than your competition may be the only sustainable competitive advantage — *Arie de Geus*[3]

Future global corporations will be more automated and take greater advantage of high technology, using robotics and employing fewer people all over the world but working together electronically. So, employees, as is the case for some today, will be working out of the local kiosks or their homes. Having such globally dispersed environments may make it more difficult for defrauders to do serious harm to globally operating corporations except through computer networks.

It would not be surprising that the competition increases to such an extent that competitors may under the guise of a fraud-threat agent attack its competitors. In the past, criminal tactics have been used to steal information and proprietary processes and devices from their competitors, so why not use fraud tactics to delay and stop their competitors' progress in gaining a competitive edge; for example, use a front corporation to supply them with counterfeit products such as drugs and aircraft parts (as is already occurring)? How would one know the difference? That of course would be another challenge to add to the assets protection and anti-fraud burden of the security professional, corporate procurement, and supply managers.

> An analysis of the history of technology shows that technological change is exponential, contrary to the common-sense "intuitive linear" view. So we won't experience 100 years of progress in the 21st century — it will be more like 20,000 years of progress (at today's rate). The "returns," such as chip speed and cost-effectiveness, also increase exponentially. There's even exponential growth in the rate of exponential growth. Within a few decades, machine intelligence will surpass human intelligence, leading to The Singularity — technological change so rapid and profound it represents a rupture in the fabric of human history. The implications include the merger of biological and nonbiological intelligence, immortal software-based humans, and ultra-high levels of intelligence that expand outward in the universe at the speed of light."[4]

---

[3] Toffler, *Creating a New Civilization*, page 257.

[4] http://en.wikipedia.org/wiki/Law_of_Accelerating_Returns

FUTURE OF FRAUD ATTACKS ON CORPORATIONS

It is expected that the current trends of global fraud attacks, whereby advantage is taken of technology and technology vulnerabilities, will continue. Gradually, some nation-states will see the negative aspects of these fraud attacks on their economies and will pressure corporations in their nation-states to stop using fraudulent tactics when doing business and also increase their anti-fraud defenses because it hurts both the nation-state's economy and the world-view of that nation-state.

As pressure is brought to bear on these businesses from competing nation-states and their corporations through such global organizations as the World Trade Organization (WTO), fraud will be fought more aggressively in some nation-states than in others. Nonetheless, other developing nation-states and their corporations will seek to use fraud to their advantage to help their economy.

Based on the current management philosophy of corporate management as noted earlier, there is less and less chance of employees being loyal to the corporation. Therefore, there are fewer employee concerns about protecting corporate assets from any types of attacks, including fraud attacks.

> America is where the future usually happens first. If we are suffering from the crash of our old institutions, we are also pioneering a new civilization. That means living with high uncertainty. It means expecting disequilibria and upset. And it means no one has the full and final truth about where we are going — or even where we should go.[5]

With less concern for the protection of corporate assets, it then follows that the corporate employee are more likely to take advantage of assets protection vulnerabilities and perpetrate a fraud or other types of crimes that will be to their advantage and easily justified. For example, employees may get a layoff notice at the same time that the corporation announces record profits and the issuance of large bonuses to management. The employees may resent the corporation to such an extent that they will perpetrate a fraud to get their share of the profits. After all, one must take care of oneself and family first.

Other potential defrauders would be those employees contracted for a specific period of time. They may have access to corporate assets to complete their contracts. In the event of a contract dispute, the contracted employee may very well rationalize that fraud against the company.

---

[5] Ibid.

FUTURE ANTI-FRAUD PROTECTION NEEDS OF CORPORATIONS

Today's security professionals have been rather complacent as to their responsibilities vis-à-vis anti-fraud programs. To date, they have more often than not opted to let auditors and others take the lead in this endeavor, to include conducting initial inquiries to prove or disprove allegations of fraud. In the future, this trend is expected to continue unless assets protection security professionals take on this aspect of their assets protection duties.

> [I]nformation is now the same thing as a physical object. If you view an organism as so dangerous as to require P4 containment — the highest level complete with airlocks, moon suits, double door autoclaves and liquid waste sterilizers — then keep information about that organism under the same kinds of wraps.[6]

How will financial customers feel when they can no longer trust the financial institutions' calculations or ATMs due to attacks from fraud-threat agents?

Corporations responsible for these and other infrastructures have a serious duty to make them impervious to attacks from fraudsters. All corporations have the responsibility to protect their employees and to safeguard the corporate assets of their owners from such attacks:

- As a security professional, do you think this safeguarding is adequately being accomplished today?
- If not, why not?
- What responsibilities do you have to ensure that your corporation's assets are protected from fraud attacks?
- If you are not leading this defensive effort, as a security professional responsible for assets protection, don't you think you should?
- If so, what are you doing about it?

All corporations should have sound plans to defend their assets against all types of attacks from threat agents — and fraud-threat agents' attacks are no exception. Security professionals should incorporate those anti-fraud plans into their assets protection and business plans, maintain those plans, and periodically test the anti-fraud defenses.

---

[6] See *Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies- and What it Means to be Human*, by Joel Garreau, page 165. Doubleday and Company, NY. 2005.

A combination of proactive offensive and defensive methodologies should be used, and high-technology and sophisticated processes should be integrated into your anti-fraud plans, policies, procedures, processes, and projects. You must also help to ensure that such philosophies are integrated into all aspects of your corporation's business.

CASE STUDY

As the CSO for an international corporation, you are asked to provide a briefing to executive management on the global state of fraud and its potential impact on corporate facilities worldwide.

How would you go about gathering information and presenting that information?

One approach would be to:

- Identify the information you will need to provide in that briefing and meet the expectations of the executive management.
- Use an Internet search engine to search for that information.
- Collect the information.
- Analyze the information.
- Determine the location of all corporate facilities.
- Determine the threats, vulnerabilities, and risks to the corporation associated with the fraud-threat agents.
- Determine the location, number, type of fraud-threat agent attacks against the corporation over the last five years, and produce trend-line charts for each location and a summary chart.
- Develop not more than ten briefing charts:
  - Number of charts depending on the time allotted for the briefing
  - Half the allotted time left for discussion and questions
  - One chart to be a list of recommendations with backup charts of justification and cost benefits that can be used to support the recommendations
  - One chart for each facility location showing the results of your previously conducting fraud risk assessment and a summary chart

Remember that executive management does not have time for lengthy and complicated briefings.

SUMMARY

Corporate globalization will continue into the foreseeable future. Defrauders will also continue to go global and reach into corporations from around

the world. Defrauders will continue to take advantage of technology vulnerabilities and the lack of aggressive anti-fraud defenses to stop them.

As nation-states mature and become a part of the global economy, some will continue to look the other way while defrauders ply their skills, which by side-benefit help the nation-state become more economically competitive through attacks by fraud-threat agents on foreign corporations, providing fraudulent products and services.

15

The Impact of High Technology on Fraud

INTRODUCTION

Since today's and tomorrow's fraud schemes so often use high technology (technology based on the microprocessor), it is important to discuss its use to perpetrate frauds and to defend against frauds.

HIGH-TECHNOLOGY FRAUDS

The number of frauds related to high technology has increased as the number of individuals, networks, corporate intranets, the Internet, National Information Infrastructures (NIIs), and Global Information Infrastructure (GII) accesses have grown. More networks therefore means that more people have access to more information. Some of those who have this access, both legal and illegal, will be defrauders.

The price and power of cellular phones, computers, and many other high-technology devices have made them more accessible to an increasing number of people on a global basis. This has occurred as the communications infrastructure has expanded and as nations have entered the Information Age, to the point where the technologies in many regions are now almost ubiquitous, with children as young as six having cellular phones and computers.

Some of these "children" are computer hackers because the protection of these valuable assets is often not what it should be and the vulnerabilities of the high-technology devices and equipment make it rather easy to break into the computers.

As with any industry, technology, or other assets that have a real or perceived value, there are those who want to take what others have; however, they neither want to pay for them nor work for them. This has been the case since the beginning of the human race with no end in sight.

High-technology frauds are therefore expected to continue to increase in terms of both number and impact. The level of sophistication is also expected to increase, as the high-technology itself becomes more sophisticated. Because the global accessibility of networks, computers, and information provides mass communications, those fraud miscreants and juvenile delinquents who use these devices for illegal acts also share their techniques with others around the world. This gives those "hacker wannabes" and others the ability to download attack tools and execute them with little knowledge of how they operate and what systems they are attacking.

Current communications and computers are such that these miscreants no longer have to physically meet to exchange knowledge and tools. In the past, they would only pass their knowledge on to people they knew and trusted. Now, with the need to meet removed, the information spreads much more rapidly. These types of attackers have and will continue to increase in the foreseeable future because very little technical knowledge is required.

The more sophisticated attackers will also continue to grow in number.

Although the Internet originated in the West, the countries that are now joining the Internet are some of the most densely populated regions of the world. As the people in countries such as China, India, and Pakistan gain access to the Internet, the result will inevitably be a huge cultural shift.

According to an online source, Global Reach,[1] the online users' language by population had reached over 801.4 million as of September 2004. The languages involved were as follows:

- Dutch 1.7%
- Portuguese 3.1%
- Italian 3.8%
- Korean 3.9%

[1] See http://globalreach.biz/globstats/index.php3 — last revised March 2004.

- French 4.2%
- German 6.9%
- Japanese 8.4%
- Spanish 9%
- Chinese 13.7%
- English 35.2%

The West will suddenly find itself in the minority, and the values it subscribes to will not necessarily be those understood by most users of the Internet. Furthermore, the fraud miscreants in these countries may use sophisticated fraud attack programs that have been developed in their regions and that have not been found on the Internet before. These and others will continue to find an increasingly more profitable job market. They will be the new "hired defrauders" of the global organized crime rings, drug cartels, terrorists, and governments. They will be hired to infiltrate systems and to perpetrate frauds.

With the increased dependencies of businesses and government agencies on the Internet, NII, and GII, these miscreants will select more and more lucrative targets. This high-technology global increase in crime will be fueled by the exponentially increasing electronic commerce and electronic, online banking. Crime always follows the money, and the penalties for online crimes are much lower than those for the equivalent physical crime.

Justifiable concerns have long been raised regarding the possibility that the highly skilled workforce of the former USSR, encountering difficulties finding work, might be recruited to work for other nations and organized crime. The next area of concern must be countries such as China and India, both of which have large numbers of highly skilled but very poorly paid workers.

Do you recall the discussion earlier in the book about motive, opportunity, and rationalization? When you are out of work, have a family, and are hungry, it may not take much convincing for you to turn to crime. The rationale is that after all, you're going after foreign corporations and governments, which during your whole life have constantly been labeled the "evil enemy." With such a backdrop, it is easy to convince yourself (rationalize) that attacking and defrauding them are of little consequence.

The future will continue to see major increases in fraud-threat agent attacks related to high technology as more and more global businesses and government agencies become more reliant on the Internet.

As noted in earlier chapters, many cases have been documented showing the use of networks to defraud corporations and perpetrate other criminal acts.

HIGH-TECHNOLOGY ANTI-FRAUD DEFENSES

Information systems security (InfoSec) is the main tool for preventing high-technology frauds through the Internet, GII, NII, and corporate networks. In the future, the gap between the sophisticated attacks on systems, PBXs, cellular phones, and other devices, and defenses will close, but the reality is that improvements in security will never catch up.

Although new fraud-threat agent attacks will still hold the edge, the future will find quicker recoveries, countermeasures, counterattacks, and new defenses all working together to provide an anti-fraud "layered defense" approach.

The increase in InfoSec will occur because corporations and nation-states, which are already almost totally dependent on access to the GII, Internet, and NII, will start to understand the importance of this resource to their effective functioning and anti-fraud defenses. As greater dependence on the networks is acknowledged, fraud-threat agent attacks will be detected, but it will be absolutely crucial to immediately address any attacks and to learn and share lessons with others in the profession.

The information systems security profession will become one of the most important and dominant professions in the twenty-first century, gaining executive management recognition, support, and authority. This will be coupled with more aggressive defense and high-technology fraud prevention programs that will include tracing the sources of the attacks and possibly even counterattacking. This aggressive approach by businesses and government agencies will be due to the continuing inability of law enforcement agencies to identify, apprehend, and prosecute these miscreants.

> As microprocessors and new uses for them in support of anti-fraud defenses begin to emerge, hopefully corporations will begin to make more concerted efforts to integrate them into their anti-fraud processes.

Effective and efficient use of high technology will result in the delivery of more timely anti-fraud defenses and, in so doing, may even drive down the amount of fraud. This is because some frauds are thought to be committed out of the defrauder's belief that the corporation's defenses are vulnerable to attack.

In the future, secure local, national, and global links will be established to track convicted fraud miscreants regardless of their location. High technology will also assist in the investigation of frauds related to high technology, but once the defrauder is apprehended, anywhere in the world, the production and delivery of evidence and the prosecution and incarceration will be done on a global scale using means such as teleconferencing as the medium.

Therefore, because of the global dependence on the Internet, NII, and the GII, the United Nations and organizations such as the European Union will support international global high-technology anti-fraud laws that will lead to the investigation, apprehension, and prosecution of these offenders. All or most of the information-dependent nations will support such processes because they will all be the main victims of these global attackers.

The fraud investigator should look at both current and future high technologies and study ways that they could be put to good use in supporting the corporation's anti-fraud defensive processes and investigations.

The CSO responsible for the corporate anti-fraud program must be computer literate and work closely with the information technology (IT) department to ensure that the security is in place and will also support the anti-fraud defensive efforts. More often than not, the InfoSec specialist or manager will report to the corporation's chief information officer (CIO) or IT manager, and not to the CSO as should be the case. However, that is another matter and beyond the scope of this book. Nevertheless, since many of today's fraud trends indicate that the GII, Internet, and corporate networks are used as the vehicles to perpetrate fraud attacks, a successful corporate anti-fraud program must take into account the vulnerabilities of these high-technology networks, equipment, and devices to successful fraud-threat agent attacks and coordinate the needed anti-fraud defenses with the InfoSec specialists.

CASE STUDY

As a CSO concerned with the vulnerability of the corporation's networks to successful fraud-threat agent attacks, what would you do to ensure that adequate anti-fraud measures were in place and current?

One approach would be to meet with those responsible for the networks' protection, determine what protective measures are in place; and then match those to the fraud schemes associated with high technology and related cases to determine the extent of vulnerabilities to fraud-threat agents.

One could coordinate with the InfoSec specialist and management and jointly conduct as risk assessment of the networks specific to the fraud threat indicators. Defensive measures would be increased if the identified risks were unacceptable.

SUMMARY

The future, based on today's trends, continues to indicate that we will be getting more of the same — more frauds, security lagging behind the fraud miscreants, and their techniques used to successfully attack computer networks around the globe.

High technology will be used as part of the corporation's anti-fraud defenses or to support the anti-fraud defenses. The criminal justice systems of nation-states will continue to be slow but will adopt and adapt high technology to provide for more effective and efficient investigations of frauds and better prosecution of the defrauders.

16

What the Security and Other Anti-Fraud Professionals Must Do Now to Personally Prepare to Combat Tomorrow's Frauds

INTRODUCTION

Whatever aspects of security — assets protection — one talks about, there are insufficient defenses in place to protect the corporate assets. This insufficiency is caused in part by:

- Security professionals not establishing a proactive, or an aggressive, anti-fraud program.
- Defensive policies, procedures, processes, plans, and programs not keeping pace with the fraud threats.
- Supporting devices or equipment (e.g, high-technology devices) not available or not installed to meet the new fraud threats.
- Lack of sufficient budget to install proper anti-fraud defensive measures (but this is also used as an excuse as security professionals and others do not properly allocate resources based on the associated risk to the assets as the primary priority).
- Failure of security professionals and others responsible for some aspect of the assets protection and anti-fraud programs to meet the challenges.

In this book we have focused on those aspects of the assets protection efforts and a program as they relate to defending corporate assets against fraud-threat agents through policies, procedures, processes, plans, and programs.

It is now time to discuss what the security (assets protection and anti-fraud) professionals must do so that they will be at least as knowledgeable of fraud schemes, techniques, and related attack methodologies as the defrauders who attack the corporate assets.

BECOMING AND STAYING PROACTIVE AND AGGRESSIVE IN FIGHTING FRAUD

In order to be successful in protecting corporate assets from attacks by fraud-threat agents, one must know at least as much as the attackers. Sadly, this does not seem to be the case inasmuch as fraud after fraud is being committed against corporations while the corporation's chief security officer (CSO) may often be surprised; as are the others on the fraud fighting team responsible for protecting corporate assets.

The response of most, if not all, CSOs is that they are very busy, doing the best they can, and as the old song goes, "and the beat goes on." Such comments may have some truth, but that does not help protect these assets from successful fraud attacks. The CSO and the others responsible for protecting corporate assets from successful fraud attacks must do better.

> For these fraud fighters to consider themselves professionals, they absolutely must do better or not call themselves professionals.

It is a sad commentary on the state of anti-fraud efforts throughout corporations that the defrauders and associated other miscreants continue to outsmart the assets' defenders. Often these defrauders do so with very little challenge from the assets' defenders. What is more, these defrauders often operate with very little education or even business experience.

GETTING A FRAUD EDUCATION

So, what can an anti-fraud program leader, for example, the CSO, do personally to help gain the edge on these defrauders?

The CSO, security staff, and others on the anti-fraud team must begin by educating themselves on the:

- Profiles of fraud-threat agents
- Specific motivations of fraud-threat agents
- Fraud schemes

- Fraud cases
- Anti-fraud defenses that have worked
- Anti-fraud defenses that have not worked

This education can be done formally through fraud-related courses at universities, technical institutes, and colleges. This "education" can also be gained by attending conferences that offer fraud-related topics as part of their lecture series. You may even be able to find online anti-fraud-related courses that will make it more convenient to gain this knowledge.

The informal education process must also include the CSO and others who set up communication channels with government agency representatives, peers, consultants, and others who can share fraud and anti-fraud related information with you.

In addition, you should identify a set of Web sites that you should check anywhere from daily to weekly in order to stay up to date on fraud-related matters. Some websites may even offer notification of fraud-related updates and e-mail services, sending you the latest information on fraud-related matters.

Yes, it takes time and you have other things to do. I guess my response to any complaints would be "Too bad!" It is part of your assets professional job. Take a time management course and move on!

GAINING FRAUD-RELATED CERTIFICATIONS

As an assets protection and/or fraud fighter, related certification programs are available that would be to your advantage to obtain. You will not only learn more about fraud-related matters but also obtain certification, which may help you get that next job.

What is meant by certification? For our purposes, certification means that, based on your experience, education, and successful passing of a test, generally given by a related association, you are certified as having the basic knowledge and ability certifying you as a professional or an expert in a particular field.

Using the word "expert" may not be the right thing to do because in the security and anti-fraud business, everything seems to be changing so rapidly that it is impossible for anyone to be an expert. Let's then say that by being certified, you are considered to have the *expertise* in the particular field.

Several certifications are directly or indirectly related to the position of a CSO and fraud fighters. A professional CSO should have the basic knowledge in some, if not all, of these anti-fraud and CSO-related certifications' areas of study.

Several associations certify professionals in various security-related professions. Some certifications are widely acknowledged throughout industry whereas others are not. Its sponsor may have developed some as part of a "get-rich" scheme. These certifications may look good on paper but are meaningless in the field.

No certification is worth anything without being accepted by the professionals responsible for assets protection and anti-fraud defenses, by related professions, and, most importantly, by executive management. The Certified Public Accountant (CPA), for example, is widely recognized throughout industry.

ASSOCIATIONS

As a security professional, it is more than likely that you will be involved with professional security associations. These associations differ in specific focus, but all have one common purpose: to enhance and improve the profession of security. Be they private, corporate, institutional, commercial, industrial, governmental, or any other type of security organization, these associations seek to advance the cause of the profession.

Members are asked to support the associations' efforts to seek a higher degree of professionalism and recognition of the security discipline. Some of these associations will work with local colleges and universities in an effort to build curricula consistent with contemporary issues in security. Together, they assist in the preparation and development of future security professionals, experts who are capable of dealing with new and more complicated security issues.

Association membership may be a general membership, as is the case with the American Society for Industrial Security (ASIS), the largest professional security association in the world. Membership may also be very specific to a type of industry such as the security committee within the Aerospace Industries Association (AIA). Within AIA, security professionals from aerospace companies work together for the benefit of the entire industry. Common challenges, issues, practices, and objectives are addressed by the memberships, who are usually senior security managers of member companies.

At least six security and anti-fraud-related associations have been around for many years and are also considered to be very professional organizations:

- American Society for Industrial Security (ASIS), which offers a Certified Protection Professional (CPP)
- Association of Certified Fraud Examiners (ACFE), which offers a Certified Fraud Examiner (CFE)

- Information Systems Security Association (ISSA), in association with another organization, which sponsors a certification as a Certified Information Systems Security Professional (CISSP)
- High Technology Crime Investigation Association (HTCIA)
- Information Systems Audit & Control Association (ISACA), which offers certifications as Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM).
- Communications Fraud Control Association (CFCA), members of whom consider themselves "the Premier International Association for revenue assurance, loss prevention and fraud control through education and information."

These associations sponsor conferences and lectures through which you can gain additional knowledge on matters related to fighting fraud.

Although not an association, the MIS Training Institute (MISTI) offers excellent fraud-related courses. They consider themselves the "International Leader in Audit and Information Security Training." Whether or not you agree with that statement, you will find that overall their conferences and courses are very informative.

GAINING ANTI-FRAUD EXPERIENCE

Let's assume you agree and establish a personal fraud awareness program for yourself as part of your own career development program and maybe those of your security staff, assuming you are the CSO or one of the security managers for a corporation. How will you gain the experience to help you establish, maintain, and manage a corporate anti-fraud program?

The best experiences may be unwanted and come from being involved in attempted or successful fraud attacks against your corporation's assets. Yes, this is good experience but surely an unwanted one.

Another way to gain experience is through fraud survey or risk assessment processes. As you gain new information about defrauder profiles, schemes, and actual fraud cases, you can attempt — under controlled conditions — to determine whether such attacks would be successful against one or more of your corporation's assets.

Such tests can often be conducted in a teaming effort with members of the audit staff and based on the corporate cultures, coordinating the matter with the legal staff and ethics director.

For example, you may know of cases where defrauders successfully set up bogus employees and had the corporation issue them weekly paychecks, paid them an excessive amount of money, and/or paid them for overtime that was never worked. You would be checking for anti-fraud defenses (controls) in place so that would not happen. This can be checked

by getting on a computer used by one of the payroll employees and establishing a bogus employee and see what happens.

If the defenses prevent an employee from adding a "ghost" employee, such as maintaining adequate separation of functions so that a bogus employee cannot be inputted, then controls may be adequate. But further testing may be needed to be sure. Be certain to operate under adequate safeguards.

As a test, you may want to establish a bogus employee with a certain profile for overtime, pay, and such. Once that ghost employee is in the database, an attempt should be made to provide that employee with more pay than is authorized based on the employee's profile.

Another test would be to compare the payroll of checks issued against the employees in the corporation and determine whether checks are issued to employees not in the employee database. Also test to see whether more than one check was issued to an employee, contractor, supplier, and so on.

These are just some simple examples of what can be done to gain experience as you take on the role of the defrauders and use the schemes you have learned through your education process; as well as learn about the actual cases of frauds that are being perpetrated on a regular basis.

The examples cited are based on actual fraud investigations of schemes that have been used much too often against both government agencies and corporations. Controls should be in place to prevent these very basic frauds; however, you may be surprised to learn how often they are successful even today.

This controlled test method allows you to gain a type of "real-world" experience while at the same time determining whether your corporation has adequate anti-fraud defenses.

Many of these types of tests in some corporations are continually being conducted by auditors who are aggressive and get into a more proactive anti-fraud mode. If you determine that your corporation's audit department has such a test program, you should discuss the program with the audit manager and establish a process for conducting these with the assistance of the security department's fraud specialist.

Beware of office politics: the auditors may believe you are trying to take over what they consider one of their primary functions. Building up rapport with the audit manager over time may help you in mitigating that potential problem.

In addition, as the CSO, you may be able to get into the anti-fraud communications loop that the auditor has access to, or you may at least be in a position to receive the latest information about fraud from the audit manager's point of view.

Once your relationship as the CSO is established with the corporate audit manager, you can also provide that manager with the information you received about fraud-related matters. You can also share information

about fraud inquiries, risk assessments, and fraud surveys that your staff have conducted or are scheduled to conduct as the audit manager shares the audit schedule with you. So, it is a win-win situation.

> If the audit department has an aggressive anti-fraud audit process in place, be careful and remember teaming methods as well as office politics issues. You don't want to alienate your best anti-fraud friend, the audit manager.

TO CONDUCT OR NOT TO CONDUCT FRAUD LECTURES AND WRITE FRAUD ARTICLES

Once you become a "fraud expert," you may want to share your information with your peers and others. You can do so by volunteering to teach a course on fraud at the local college or university or at a conference. You may also consider writing some fraud-related articles for a newspapers or magazine.

This is an admirable goal that you should strive for if you want to consider yourself a true security or anti-fraud professional, giving something back to the profession. However, a word of caution is needed here. By placing yourself, and thus your corporation, in the public spotlight, you may also be spotlighted by the defrauders of the world. So caution is needed, and one should discuss the matter with the ethics director and legal representative, and of course your boss.

Such a spotlight may make the corporation appear to be doing a great job in protecting the assets of the corporate owners, or stockholders. However, some may take it as a negative by implying that the corporation is so rife with fraud that it needs a special program in order to defend itself against frauds. The corporation's public relations manager should also be contacted and discuss the pros and cons of such public visibility.

In addition, global defrauders, having heard about your lectures, witnessed them, or read your articles, may consider it a challenge and attack your corporation in order to successfully perpetrate a fraud and also make a point as they think of you as throwing down the gauntlet to challenge them.

CASE STUDY

A CSO decided to get "up to speed" on fraud-related matters. If you were that CSO, how would you begin?

If you say you would take the approach cited above, well, yes, eventually that would work. However, first you may want to consider the following steps:

- Identify your current and specific fraud-related education.
- Identify your current and specific fraud-related experiences.
- Identify what you would consider the perfect, more knowledgeable fraud-related expert's profile.
- Using a matrix approach, identify the areas where you are lacking in your fraud education and experiences.
- Set up a project plan to obtain the necessary education and gain the necessary experiences.
- Once completed, establish a maintenance process to keep current.
- Consider obtaining various fraud-related certifications. (These may also help when seeking that next career development position.)

SUMMARY

In order to call oneself a true security or assets protection professional, one must maintain currency in fraud-related matters. As a professional, you should bring yourself up to date by obtaining continued education and experiences in fraud-related matters.

Establishing a formal career development program related to anti-fraud matters will provide a focused approach to gaining the required fraud-related knowledge.

17

Summary and Final Thoughts

INTRODUCTION

This final chapter, as the title implies, summarizes some main points scattered throughout this book and provides some concluding thoughts on fraud and on who should lead an anti-fraud program.

This book was written with the objective of trying to convince the security "professionals" that today's current approach to fighting fraud does not seem to be working inasmuch as frauds continue to increase and therefore, some professional should take the leadership role and devise a formal program to fight fraud. That role should be assumed by the corporate CSO, the assets protection and security professional, who is already responsible for the overall protection of corporate assets.

Fraud is a multibillon dollar industry and is growing. This situation must be stopped, for all frauds hurt not only the corporations and employees who are the victims of frauds but also the nation-states where the corporations do business. It is a drain on the economy and on the nation-state's income from tax revenues; it also adversely affects the global economy.

> Modern nation-states are battling for economic power, and fraud attacks against nation-states and their corporations that adversely impact their ability to successfully compete in the global marketplace.

Methods tried in the past have not worked as well as they should. A new, aggressive, and formal approach must be taken, led by the security professional such as the CSO. At the same time, this approach must be

cost-effective, for, as with all overhead functions (and this is considered an overhead function), it is a "parasite" on the profits of a corporation.[1]

SUMMARY

We live, work and play in a fast-paced, global environment where, thanks to technology, we can communicate and do business around the world in nanoseconds. Technology has changed not only the way we communicate but also the way corporations operate.

Today technology is driving the world where the only constant seems to be change itself. These changes seem to be occurring faster and faster. No position, no job, no process, no corporation, no product, no way of doing business is safe from change. Some welcome it, others hate it, while still others take advantage of it for their own selfish reasons. These include the global miscreants perpetrating frauds from within and outside corporations.

Fraud victims are ordinary people, stockholders and any other being or entity that will provide the greedy miscreants their rewards without having to legally earn them. In this book, the focus was on establishing and managing an anti-fraud program for a corporation with the premise that the corporate CSO must lead that effort.

As part of that effort, a formal corporate anti-fraud program must be established and managed as a standalone program or as a subset of the corporation's assets protection program. This includes identifying the assets protection and anti-fraud drivers and requirements and subsequently establishing anti-fraud policies, procedures, processes, plans, projects, and related operations.

> [P]ractitioners aren't saints, they're human beings, and they do what human beings do — lie, cheat, steal from one another, sue, hide data, fake data, overstate their own importance, and denigrate opposing views unfairly. That's human nature. It isn't going to change.[2]

---

[1] Remember that the term "corporation" is being used as a "catch-all" term for corporations, charities, government agencies, and any other entity that can be considered a fraud target.

[2] Quoted from Michael Crichton's book *NEXT*, published by Harper Collins Publishers, New York, 2006.

FINAL THOUGHTS

The premise put forth in this book is:

> *A chief security officer (CSO), having the overall leadership responsibility for protecting the business's or government agencies' assets from threat agents, should therefore lead the anti-fraud program to protect those assets from fraud threat agents.*

As discussed, that is a team effort, but there must be a leader for that program, and that leader is the one responsible for the overall protection of assets. If the person responsible for leading the protection of assets for the corporation is a person other than a CSO, then whoever that person is should lead the anti-fraud program efforts.

An anti-fraud program is more necessary than ever today when increasing amounts of frauds are being perpetrated throughout corporations. Depending on the corporate culture and assuming that the anti-fraud program is necessary, should it be a standalone program or a subset of the corporation's overall assets protection program?

I believe it should be a subset of the overall corporate assets protection program. Why? Because there would be many resource allocation issues and potential for redundancies if it were not. Redundancies are not an affordable option in today's tight budget environments, especially in the budget of the security department, which never seems to be large enough.

Now that you have completed all but this final chapter of *Fighting Fraud*, you should have some opinions on how you would proceed to establish and manage an anti-fraud program for a business or government agency, whether it be for a corporation, charity, government agency, or any other entity.

Your experience, coupled with your formal education and training, may tend to favor one profession or another in leading an anti-fraud program.

WHAT OTHERS THINK ABOUT THE ANTI-FRAUD LEADERSHIP POSITION IN A CORPORATION

- **Roscoe Hinton, special agent (Retired), U.S. Air Force Office of Special Investigations and former fraud investigative specialist and supervisory agent, who has conducted and overseen many investigations into corporate fraud and government-related frauds,** says: *It should be someone who had authority to change procedures,*

correct systemic weaknesses and dole out punishment as deemed fit.

That's why central system fraud dropped off the map. No one could ever prosecute the person(s) at the top so settlements became the norm. Pretty soon AUSA (Assistant U.S. Attorney)'s saw no benefit in prosecuting the lowly employee who was simply following procedures without being able to hold the "procedure" person liable. . . . this was given in testimony.

Corporations, top audit firms and even small businesses adopted the stance "I will get as much as I can from the government and if he is not smart enough to catch me then what's the harm since the government is omnipotent." That mentality was and still is pervasive, look at the Gulf contractors, the contractor hiring practices in D.C. to include involvement from high ranking government officials.

WE HAVE REVERTED BACK TO THE POLICY OF "NO HARM NO FOUL.". I am speaking for US government contract fraud. . . . Until the government prosecutors take fraud seriously, the criminal punishment will be light, therefore not a deterrent.

- **Joseph T. Wells, CFE, CPA, chairman of the Board of Directors, Association of Certified Fraud Examiners**, says: *Frankly, I think that your . . . premises are totally off the mark.*
- **Motomu Akashi, former security manager for an international corporation**, says: *Fraud examiners and investigators could be included in the security organization, but, on the other hand, it could be part of an audit organization or finance office or any other organization depending upon the desire of the CEO. Many times, specialized examiners and investigators are placed outside of the main organization structure to allow them independence and free, unobstructed access to all organization within the corporation.*

  The CSO, in many cases, is not positioned high enough in the corp. ladder to effectively conduct independent fraud examinations over the entire corporate structure without interference of other senior executives.

  So, I feel that you could make your premises, but I wonder if it will hold water in all cases.
- **Ed Halibozek, Vice President of Security, Northrop Grumman Corporation,** says: *How we do it is really a joint effort with Corporate audit (lead), security and legal.*
- **Charles A. "Chuck" Sennewald, CPP, CSC, CPO, security management consultant and author, says:** *Of course the premise is valid! In my view to have no program and/or no fixed responsibility for such a protective strategy would be a form of corporate negligence.*
- **Andy Jones, head of Security Technology Research at the Security Research Centre for British Telecom, United Kingdom**, says: *I believe that the leadership for a corporation's anti-fraud program should be*

with the Chief Security Officer (CSO) as this is the rational place for it to sit. The CSO is responsible for the security of all of the company assets, whether they are physical, electronic or personnel and they must be able to address fraud as he/she would address any other threat to the organization.

- **Bill Boni, Corporate Vice President (of a security sector for an international corporation)** says: *In my opinion the emerging role of CSO's at major organizations is to manage holistically all operational risk management processes to keep impacts within acceptable range. Since every company has fraud and since the volume of losses can be significant, perhaps even rise to level of material losses the overall fraud prevention and response program role should be under direction of the CSO.*

  This allows the CSO to make decisions with full appreciation as to the extent of resource/effort required in each operational risk area; to manage operational risks as a "portfolio," not as an independent silo of controls!

  Thus the CSO's role and principal value to the organization is to balance off investments and results in fraud prevention controls against other areas such as info security controls, disaster and business continuity control, etc. — to reach the overall lowest level of adverse/acceptable losses.

  The CSO should be focused on optimizing controls across the risk portfolio so as to leverage investments in policy, process, technical and other operational controls with expected impact of reducing fraud through innovative application of prevention, detection and response mechanisms.

  Some examples probably include the investigative processes, digital forensic tools which are commonly used for a variety of activities not strictly limited to fraud. In our age of blended threats involving cyber, human, and financial dimensions the prevention, detection and response mechanisms all bring greater value to the organization if they are operated with understanding of the value they bring to cover multiple threats.

  A CFE should help ensure the CSO's overall program is managed with the best practices experience offered by this certification and associated references/research/resources;

  The CSO may be the CFE or if they are not, a CSO would probably be very well served by having on staff or on retainer senior and skilled personnel possessing the CFE capabilities, just as the CSO may well need a CISM/CISSP, certified info security officer (CISO); a CPP certified expert in physical/corporate security or other credential and experienced "experts" for those elements of the operational risk mgt framework of greatest significance to the specific organization's mission.

Saying "only" a CFE can lead fraud prevention programs is self evidently not true, absent a governmentally mandated regulatory licensing scheme (like CPA's), which I believe is very unlikely to happen.

Saying the expertise such as a practitioner will obtain via CFE certification and programs of study/training will significantly enhance the effectiveness and impact of a fraud prevention program, especially if operating synergistically across the portfolio of risks, makes a lot of sense to me.

The above is my opinion and does not represent the official position of the management or shareholders of my employer, nor of any professional organization in which I am member or on the Board of Directors.

TOBY J. F. BISHOP, CFE, CPA, FCA, PRESIDENT AND CHIEF EXECUTIVE OFFICER, ASSOCIATION OF CERTIFIED FRAUD EXAMINERS WORLD HEADQUARTERS

The following are some of Bishop's comments taken from e-mail discussions with the author:

There are a few points. . . . The rationale section states (That of the author's book prospectus)*: "Fraud examiners specialize in fraud-related matters; however, few come from outside the audit or investigative profession. Furthermore, within a corporation they are usually investigators (react to fraud allegations) or auditors (look for compliance). They are all in a reactive role. They are not in a leadership position responsible for the protection of corporate assets — defending the assets against frauds — a proactive but defensive posture is needed."*

The ACFE's membership statistics do not match up with the statement that few fraud examiners come from outside the audit or investigative profession. It is also not accurate to state that all fraud examiners are in a reactive role and that they are not in a leadership position responsible for the protection of corporate assets.

That might perhaps have been true fifteen years ago but certainly not in recent years or today, as I know from my own experience in practice over the past twenty years. I meet an increasing number of fraud examiners in major corporations who are senior members of management with proactive anti-fraud responsibilities. Also, there is a massive shift in emphasis taking place right now that is shifting corporate resources from mainly a reactive role to mainly a proactive role, as many fraud examiners (including me) have been recommending for over a decade.

. . . It would definitely be a good thing to have corporate security professionals who are trained in fraud prevention, deterrence, detection and investigation participating at all levels in the anti-fraud efforts for companies. I share your enthusiasm for having trained and experienced anti-fraud professionals involved. I have a somewhat different perspective of the outlook if security professionals choose not to participate in this activity. If they don't others will fill that role. Either way, the job will get done.

We should strongly encourage fraud examiners, auditors, investigators and corporate security professionals to share a common body of anti-fraud knowledge and work together to fight fraud effectively.

Having rival factions would not only be counter to the ACFE's philosophy of spanning all professions and industries but it would also likely impair outcomes. . . .

. . . I'm happy to agree to disagree on some points. The world would be a dull place if we all agreed on everything. I am very sensitive to the points about the role of CFEs, since that is what the ACFE is all about and it's my duty to act in the best interests of our members.

IN CONCLUSION — MY THOUGHTS

In the past, security professionals have been very lax in meeting their responsibilities in protecting corporate assets. Many are retired government law enforcement officers hired by executive management based on their past titles because corporate management seldom thinks of security as anything other than a guard and the group that controls security alarms and badge systems.

Many of these retired law enforcement persons (local, state, and national) are more than happy to sit around and be "retired in place" because they do not want to take on more than they have to. After all, they will get good pay and good benefits, so why work harder than management demands? Not all think that way of course, but one may be surprised as to how many do.

Such thinking still permeates many of the corporate security offices and staff. That may be at least one reason why stockholders/owners continue to be victims of crime.

If we look back, we see that with the advent of the computer and automated information systems and networks, the task of protecting the systems and the information that they stored, processed, transmitted, and displayed fell to the information technology department within a corporation. This occurred because, as with fighting fraud, the security specialists failed to provide the leadership needed to protect valuable corporate

assets — information systems and the information that they processed, stored, transmitted, and displayed.

History has shown the results: information stolen, fraudulently manipulated, and destroyed, and systems compromised, even by children! Even to this day, it seems that most security professionals are very happy to leave the protection of these very vital corporate assets to the "computer folks."

One wonders what would have happened if at the very beginning of this age of information and computers, the security professionals had led the protection efforts of these vital assets. Would we still have the same assets protection issues that continue to plague us? I guess we will never know.

One would think that when it came to fighting fraud that the security professionals would have stood up and led the anti-fraud program efforts, but for the most part they have not. They have left it to the accountants and auditors with obvious results — fraud continues to increase on a global scale.

> Today's frauds are becoming more technology driven, more sophisticated, more numerous, and more global.

What has been the response of some corporations in fighting fraud? They appear to:

- Do only the minimum necessary to stay out of trouble with government agencies.
- Want to "hide" frauds when they can so that stockholders don't find out how corporate managers are failing to properly safeguard the corporate assets.
- Try to hide them so that they don't have "public relations problems."

What has been the response of criminal justice agencies regarding fighting fraud?

- Legislators pass new and more complicated laws.
- Regulators pass new and more complicated rules and regulations.
- Law enforcement at all levels tends to give secondary importance to frauds with priorities and budgets going to fight pornography, drugs, and violent crimes.[3]

[3] This is not to say that these are the correct priorities and the priorities voiced by the public, but rather to point out some possible reasons that fraud matters are given a lower priority.

- Courts in general give only "slap-on-the-wrist" punishments, often with immediate probation and community service in lieu of incarceration.
- The judges, when they do give the fraud miscreants "jail time,"send them to a confinement facility which some do not consider to be much of a prison at all since they offer tennis courts and allow the inmate to do pretty much whatever he or she wants except leave the facility — sort of a little home away from home.

Does crime pay — often yes! Does fraud pay? More often than not these days it appears so!

The problem is compounded by those miscreants who operate in a global environment and are out of reach of their victims' legal retaliations and the law enforcement agencies where the victims are located.

Sometimes the major fraud miscreants are the "neighbor next door," the little ole granny, or CEOs and CFOs who are respectable members of the community, give to charities, help the community, and are church-goers.

The juries are made up of like people who may find that the defrauders' rationale has some validity, and they feel sorry for them as these poor defrauders cry:

- "I didn't know it was wrong!"
- "I am sorry and have prayed every night for God's forgiveness."
- "No one really got hurt."
- The big corporation, government agency, or insurance company was the only one affected, and we all know how they operate!"

So, in the absence of some drastic changes, which are doubtful, frauds will continue to pay.

SOME REFERENCES

In writing this book, some thought was given to supplying the reader with an attachment full of Web sites, books, and other references relating to fraud as discussed here. That approach was abandoned because one should be in a position to keep current with fraud-related matters. In order to do so, when it comes to obtaining more information and the most current information on any and all aspects of frauds, what better place to look these days than the Internet?

Therefore, it did not seem logical to provide information that in many cases would be outdated before this book was published — another example of the fast pace of things driven by or supported by technology.

Another reason we decided to forego references was that you the reader may have unique needs and require more specific and more narrowly focused information on fraud matters. So, what may seem to be a good list of references may in fact not meet your needs at all.

Using one of the more popular search engines, by typing in the word:

- *Fraud*, the systems found 138,000,000 hits
- *Fraud Prevention*, 8,800,000 hits
- *Fraud Defenses*, 6,000,000 hits
- *Fraud Crimes*, 2,150,000 hits
- *Fraud Laws*, 8,860,000 hits
- *Fraud Regulations*, 5,870,000 hits
- *Fraud Rules*, 17,500,000 hits

Keep in mind that the "hits" probably include some sites that are not relative to our discussion or your needs. So the problem also revolved around which ones to list.

With that observation, I close and hope that neither you and yours nor your employer or the corporation in which you hold your savings in the form of stock ever fall victims to fraud. However, the chances these days that you will go unscathed are not very good, nor are the chances good that you will recover your losses or that the defrauders will be identified and incarcerated for as long as you think they should be. Such is life in the fraud-ridden twenty-first century.

For those in the security profession who are responsible for assets protection but who do not consider fighting fraud to be part of the duties and responsibilities, I say, "Shame on you! You cannot consider yourselves security professionals!"

For those those who are the professional fraud fighters of the twenty-first century — Good Luck and Good Hunting!

END OF LINE[4]

[4] Phrase borrowed from that classic Sci-Fi movie, *Tron*.

About the Author

Dr. Gerald Kovacich has over 40 years of anti-fraud, security, information warfare, counterintelligence/counterespionage, criminal and civil investigations, and information systems security experience in the US government as a special agent, as a manager for global corporations, and as an international consultant.

He has worked for numerous technology-based, international corporations as an information systems security manager, corporate information warfare technologist, investigations manager, security audit manager, and anti-fraud program manager, as well as an international lecturer and consultant on these topics.

More specifically as it relates to anti-fraud matters, Dr. Kovacich specialized in anti-fraud programs in the public and private sector. As a special agent with the U.S. Air Force Office of Special Investigations (AFOSI), he conducted numerous operations to include numerous fraud surveys, overt and covert fraud operations, and fraud investigations and provided consultation on how to mitigate frauds for U.S. Government agencies as well as international corporations.

Prior to retirement, Dr. Kovacich was the Deputy Fraud Chief of a major regional AFOSI office that had responsibility for U.S. Air Force and related U.S. government fraud investigations, surveys and risk assessments. In that position, he also provided management oversight to approximately 25 special agents conducting fraud inquires, risk assessments, surveys, operations, and investigations.

During the period 1980–1982, Dr. Kovacich developed and was supervisory agent for the first five U.S. Air Force computer fraud surveys and risk assessment operations. This included handpicking the team members, writing the operational plans, leading the team's operations, and writing the final reports based on a unique format that he developed.

Dr. Kovacich was formally trained in combating fraud at the U.S. Air Force Office of Special Investigations Academy; on computer fraud

investigations by the FBI; and as a contracting officer, logistics officer and supply officer by the U.S. Air Force. This has given him unique insight on how such processes worked and their vulnerabilities to frauds.

As a consultant, Dr. Kovacich worked to establish proactive anti-fraud programs for international corporations as a consultant to their management teams. He has also conducted numerous international and national lectures on the topic of fighting fraud.

Prior to his retirement, as a security professional he was certified as a Certified Fraud Examiner by the Association of Certified Fraud Examiners (ACFE). He was also the ACFE project lead for ACFE's chapters' development in Southeast Asia and was the project lead for developing ACFE's computer fraud manual. He has also presented numerous lectures for ACFE.

He was also a Certified Protection Professional (CPP) and also a Certified Information Systems Security Professional (CISSP).

Dr. Kovacich is currently living on an island in Washington State where he continues to write and conduct research relative to these topics and other security-related topics.

Index

Access
  fraud importance, 68
  fraud-threat agent amplification, 72–73
Accident, irrelevance to fraud commission, 56–57
Accounting fraud
  accounting firm case study, 158–159
  accounts receivable
    borrowing against accounts receivable, 116
    fictitious accounts, 115
    lapping, 114–115
    payment diversion on old written-off accounts, 115
  cash schemes
    check swapping, 113
    fictitious refunds and discounts, 113
    journal entries, 113–114
    kiting, 114
    receipt alteration, 113
    skimming, 112
    voids/under-rings, 112–113
  Enron, 140–141
  off-book, 111–112
  on-book, 111
ACFE, *see* Association of Certified Fraud Examiners
Actual fraud, definition, 29
Adelphia, fraud case, 129–131
Administrative security, functions, 262–263
Advance fee, fraud schemes, 121
Affordability-based budget, 229
Africa, global marketplace expansion and fraud, 6–7
Agricultural Age, crime features, 17, 285–286
AIB, *see* Allied Irish Bank
Akashi, Motomu, 312
Allfirst, fraud case, 131–132
Allied Irish Bank (AIB), fraud case, 131–132
Amazon, Internet fraud prevention, 93
American Society for Industrial Security (ASIS), certification, 304
Annual business plan, evaluation for anti-fraud program establishment, 172, 176
Anti-fraud program
  company evaluation for establishment, *see* Company evaluation, anti-fraud program establishment
  drivers, 183–184, 195–196
  evaluation, *see* Evaluation
  functions, 261–266
  importance, 311
  integration in development, 185–186
  management, *see* Management, anti-fraud program
  planning, *see* Planning, anti-fraud program

Anti-fraud program (continued)
policy document, 184–185, 206–210
prospects for corporation needs, 292–293
team building, *see* Teaming
Asbestos, mass torts and fraud, 160
ASEAN, *see* Association of Southeast Asian Nations
ASIS, *see* American Society for Industrial Security
Assets
definition, 32, 198
information, 227
people, 227
physical assets, 227
types, 33
Assets protection program
document evaluation for anti-fraud program initiation, 186–188
updating, 190–192
Association
Association of Certified Fraud Examiners (ACFE), certification, 304
Association of Southeast Asian Nations (ASEAN), anti-fraud initiatives, 47–48
ATM, *see* Automatic teller machine
Auditor
chief security office relations, 307
fraud protection responsibility, 84–85
functions, 264
Automatic teller machine (ATM)
bank-initiated complaints, 102
card loss and theft, 103
case study of fraud, 156
customer claim resolution, 103–104
customer-initiated complaints, 102
deposit-related incidents, 102–103
growth of networks, 101
susceptibility to fraud, 104
withdrawal-related incidents, 102

Bank fraud, United States federal statutes, 43
Bank of the West, Internet fraud prevention, 92
Bishop, Toby J. F., 314–315
Boeing, government contractor fraud case, 143–144
Boni, Bill, 313–314
Bribery
international database, 148–149
overview, 116
Budgeting, anti-fraud program
affordability-based budget, 229
definition, 228
development questions, 230
resource categories, 229–230
zero-based budget, 228–229
Business plans, evaluation for anti-fraud program establishment
annual business plan, 172, 176
strategic business plan, 170–171
tactical business plan, 171–173

Capital asset, definition, 33
Capitalism, global trends, 5
Capture, fear in fraud-threat agent inhibition, 69
Cell phone
Internet access, 10
prepaid cell phone fraud case, 147–148
Certification, anti-fraud professionals, 303–305
CFCA, *see* Communications Fraud Control Association
Check kiting, 114
Chief executives, *see* Executive management
Chief security office (CSO)
anti-fraud program
establishment, *see* Company evaluation, anti-fraud program establishment
management, *see* Management, anti-fraud program
planning, *see* Planning, anti-fraud program
assets protection program document evaluation for anti-fraud program initiation, 186–188

executive management expectations, 220–222
leadership, 216
perceptions of others, 311–315
responsibilities, 86–88
Churchill, Winston, 200
Citigroup, customer data loss, 95
Civil fraud, definition, 31
Click fraud
case studies, 142, 146
definition, 104–105
signs, 105
Clip-on fraud
detection, 107
overview, 106–107
Collaborating, security staff, 253
Commercial asset, definition, 33
Commercial group, malicious fraud-threat agent, 60–61
CommonWealth Central Credit Union, Internet fraud prevention, 93–94
Communicating, security staff, 253–254
Communications Fraud Control Association (CFCA), 305
Company evaluation, anti-fraud program establishment
business plans
annual business plan, 172, 176
strategic business plan, 170–171
tactical business plan, 171–173
chief security officer history, 173–176
competition, 166, 168
departmental interactions, 178–180
manufacturing
locations, 167–169
process, 169
mission statement, 179–180
networking, 167–168
organizational structure, 166, 176–178
proprietary process, 167–168
quality statement, 180
strategic plans, 180–181
vision statement, 179
Computer fraud
hard drives, 133–134
historical perspective, 98
overview, 97–98
perpetrators, 98
types, 99–101
Conflicts of interest
fraud schemes, 116
purchasing fraud, 117
Contingency planning, functions, 262–263
Corporate managers, fraud protection responsibility, 82–83
Corporate policy, violation versus fraud, 37–38
Corporation location, fraud frequency effects, 7–8
Corporation type, fraud frequency effects, 7
Cost of participation, fraud-threat agent inhibition, 70
Credit card
information theft and fraud, 149–151
skimming, 95–96
Criminal, malicious fraud-threat agent, 61–62
Criminal fraud, definition, 31
Criminology, theories of fraud, 53–56
CSO, *see* Chief security office
Curiosity, fraud-threat agent motivation, 67
Cybercrime, *see* Internet

Data diddling, computer fraud, 99
Data leakage, computer fraud, 99
Debt collecting fraud, case study, 134–135
Delegating, security staff, 255
Deming, W. Edwards, 79
Disaffected staff, malicious fraud-threat agent, 63
Durkheim, Emile, 55–56

Earned interest, borrowing on, 119
e-bay, Internet fraud prevention, 91–92

Education, fraud-threat agent amplification, 73
e-mail
  address disguise, 101
  case study of fraud, 124
  dead soldier scam, 139
  Internet fraud prevention, 91–95
  Nigerian scam, 111–112
  phishing case study, 128–129
Employees
  fraud protection responsibility, 82–83
  future trends, 288–289
Employment application fraud, overview, 108
Emulex, fraud case study, 139–140
Enron, fraud case study, 140–141
Ethics director
  fraud protection responsibility, 83–84
  functions, 264
EU, *see* European Union
European Union (EU), anti-fraud initiatives, 45–47
Evaluation
  anti-fraud program
    case study, 278–281
    investigations, 270–274
    level of effort, 268–270
    noncompliance inquiries, 270–274
    objective goals, 268
    process measurements, 277–278
    process summary, 280–281
  assets protection program document, 186–188
  business plans, 170–173
  company, *see* Company evaluation, anti-fraud program establishment
  security staff, 256
Event security, functions, 263
Executive management
  anti-fraud program attitudes, 80–81
  chief security officer expectations, 220–222
  fraud perpetuation, 80, 129–131
  fraud protection responsibility, 81–82
  security team members, 246–248
Executive protection, functions, 263
Experience, gaining, 205–307

Failure, fear in fraud-threat agent inhibition, 69–70
Fame, fraud-threat agent amplification, 72
FCPA, *see* Foreign Corrupt Practices Act
Fire protection, functions, 262
Foreign Corrupt Practices Act (FCPA), 148
Formal project plan, definition, 34
Fraud
  criminology theory of motivation, 53–56
  definition, 28–31
  elements, 29
  prospects, 291
  responses to fighting
    corporations, 316
    government, 316–317
  schemes, *see specific schemes*
  types, 31
Fraud examiner
  certification, 85
  responsibilities, 85–86
Fraud feasor, definition, 31–32
Fraud-threat agent
  access, 67–68
  amplifiers, 71–73
  capabilities, 64
  case study, 74–78
  catalysts, 68–69
  definition, 4
  inhibitors, 69–71
  malicious agents
    commercial group, 60–61
    criminals, 61–62
    disaffected staff, 63
    hackers, 62–63
    overview, 57
    pressure group, 59–60
    state sponsored fraud threat, 58
    subversive organizations, 63–64

terrorists, 58–59
motivators, 65–67
system-related factors, 74
threat components and relationship, 74–75
Fraudulent act, definition, 31

Galbraith, John, 53
Ghost employees, 119
Globalization
anti-fraud corporation needs prospects, 292–293
aspects in fraud, 9, 287
benefits to nation-states, 5–6
definition, 3
global corporation features, 289–290
progression, 4–5, 26, 288
Goal setting, security staff, 255–256
Google
click fraud case, 146
privacy concerns, 145
Government contractor, fraud case studies, 135–136, 143–144
Government security, functions, 263–264

Hacker
case study, 161
malicious fraud-threat agent, 62–63
Halizobek, Ed, 312
Hard drive, disposal, 133–134
Health insurance fraud
case study, 154–155
medical equipment fraud, 121
Medicare fraud, 122
rolling lab schemes, 121
services not performed, 122
Hesburgh, Theodore, 217
High Technology Crime Investigation Association (HTCIA), 305
High-technology fraud, *see also* Internet
anti-fraud defenses
corporation needs prospects, 292–293
education, 302–303
information systems security, 298–299
insufficiencies, 301
proactive measures, 302
trends, 295–297
Hinton, Roscoe, 311–312
HTCIA, *see* High Technology Crime Investigation Association
Human error, irrelevance to fraud commission, 56–57
Human relations specialist, functions, 264
Hurricane Katrina, fraud, 132

Identity theft
approaches, 108–109, 137
banker case study, 158
dish washer case study, 136–137
prevention, 153
Industrial Age, crime features, 17, 286
Informal project plan, definition, 34
Information security, functions, 263–264
Information superhighway, *see* Internet
Information Systems Audit and Control Association (ISACA), certification, 305
Information Systems Security Association (ISSA), certification, 305
Intangible asset, definition, 33
Intent, proof of, 28
Internet, *see also* Click fraud; e-mail; High-technology fraud
cell phone access, 10
crime
case studies, 24–25
challenges, 23–24
history, 18–19, 286–287
prospects, 21, 295–297
global connectivity and fraud dangers, 21–22
highway metaphor, 14–15
international cybercrime
case study, 154
collaborations, 19–20

Internet (continued)
law enforcement capabilities and limitations, 22–23
New Jersey fraud sweep, 155
organized crime and cybercrime, 132–133
prevalence of I-Way robbery, 20–21
Inventory fraud
embezzlement charging to inventory, 118
personal use of goods, 118
theft, 117–118
Investigations
evaluation, 270–274
functions, 263
obligations, 37
Investment fraud schemes
avoidance of other losses or expenses, 119
borrowing on earned interest, 119
use as collateral, 118
Invoice, falsification, 117
Iraq war, corruption cases, 152–153
ISACA, *see* Information Systems Audit and Control Association
ISSA, *see* Information Systems Security Association

Jones, Andy, 312–313
JPMorgan Chase & Co, Internet fraud prevention, 91

Katrina, *see* Hurricane Katrina
Kickbacks, 116
Kiting, checks, 114

Lapping, accounts receivable, 114–115
Law
Asia, 47–48
case study, 48–50
corporate policy violation versus fraud, 37–38
enforcement activity and fraud-threat agent effects, 71, 73
Europe, 45–47
United States
bank fraud, 43
civil litigation, 43–44
consumer protection laws, 40
enforcement, 41
federal anti-fraud laws, 38–40
mail fraud statutes, 41–43
money laundering, 43
phone company compliance, 44
securities violations, 44
Treasury collection, 44
Leadership
chief security officer , 216
qualities, 217
versus management, 217–218
Lecturing, caveats, 307
Legal staff, functions, 264
Letter of credit fraud, 122
Level of effort (LOE), evaluation, 268–270
Lobbyist, corruption case study, 153–154
LOE, *see* Level of effort
Logic bomb, computer fraud, 99

Mail fraud, United States federal statutes, 41–43
Management, anti-fraud program
budgeting, 227–230
case study, 242–244
chief security officer leadership, 216
consultants, 226
controlling, 230–232
customer expectations
executive management expectations of chief security officer, 220–222
external customers, 219–220
internal customers, 219
fraud threat management, 241–242
incorporation aspects, 225–227
leadership versus management, 217–218
oversight management, 235
overview, 215
performance assessment, 232
performance management, 233–234
planning, 223–225
process management, 232–233

project team functional tasks, 261–262
protected asset types, 227
quality management, 235
response to fraud incidents, 240–241
risk management, 222–223, 235–239
security department vision, mission, and quality statements, 223
technology to deliver support and services, 234–235
Manufacturing, evaluation for anti-fraud program establishment
locations, 167–169
process, 169
MasterCard, fraud risk, 149–150
Medical equipment fraud, 121
Medical research fraud, case study, 151–152
Medicare fraud, 122
Merchandise receipt, fraud case study, 141
Microprocessor, size trends, 11
Microsoft, digital signature fraud, 144
Million-dollar dump, mortgage fraud, 97
Mission statement
evaluation for anti-fraud program establishment, 179–180
security department, 223
Money laundering, United States federal statutes, 43
Mortgage fraud
case study, 142–143
economic impact, 96
million-dollar dump, 97
rent-to-steal, 96
straw-man swindle, 97
Motivating, security staff, 254
Motive
anti-fraud program planning, 206
criminology theory, 53–56
fraud attack, 76

Nanotechnology
applications, 11–13
definition, 11
fraud utilization prospects, 13–14
NCI, *see* Noncompliance inquiries
Nigerian scam
principles, 109–110
variations, 111–112, 160
Noncompliance inquiries (NCI), evaluation, 270–274

Office Européen de Lutte Anti-Fraude (OLAF)
objectives, 45–47
organization, 46
Office politics, 250–252
OLAF, *see* Office Européen de Lutte Anti-Fraude
Opportunity
anti-fraud program planning, 206
fraud attack, 77
Overbilling, 117
Overtime abuses, 119

PayPal, Internet fraud prevention, 92
Payroll and personal expenses fraud
ghost employees, 119
overtime abuses, 119
withholding tax schemes, 119
Peer perception, fraud-threat agent inhibition, 71
Peer pressure, fraud-threat agent amplification, 72
Performance management, 233–234
Personal gain, fraud-threat agent motivation, 66–67
Personnel security, functions, 262–263
Phishing, *see* e-mail
Phreaker, overview, 100
Physical security, functions, 262
Piggybacking, computer fraud, 99
Planning, anti-fraud program
accountability, 212
assets protection risk analysis, 204
assets protection risk assessment, 202–203
case study, 213–214
company evaluation, *see* Company evaluation, anti-fraud program establishment

Planning, anti-fraud program (continued)
defense-in-depth approach, 204
drivers of anti-fraud program, 183–184, 195–196
flow of tasks, 204–205
off-site facilities, 212
policy document, 184–185, 206–210
procedures, 210–211
project management chart and components, 192–195
recruiting security professionals, 212–213
risk assessment, 196–199
team, 189–190, 195
threat assessment
man-made threats, 200–201
natural threats, 200
updating with assets protection program, 190–192
Plans, definition, 34
Policy, definition, 34
Political cause, fraud-threat agent motivation, 66
Ponzi scheme, 123
Power, fraud-threat agent motivation, 67
Pressure group, malicious fraud-threat agent, 59–60
Prime bank note fraud, 122–123
Procedures, definition, 34
Process management, 232–233
Processes, definition, 34
Procurement/contract, fraud schemes, 120
Product type, fraud frequency effects, 8–9
Project, definition, 34
Project management, chart and components for anti-fraud program planning, 192–195
Public perception, fraud-threat agent effects, 70, 73
Publishing, caveats, 307
Purchasing fraud schemes
checks payable to employees, 117
conflicts of interest, 117
fictitious invoices, 117
overbilling, 117
overview, 116
Pyramid scheme
Internet case study, 146–147
overview, 123–124

Quality statement
evaluation for anti-fraud program establishment, 180
security department, 223

Rationalization
anti-fraud program planning, 206
fraud attack, 76
Real asset, definition, 33
Religion, fraud-threat agent motivation, 67
Rent-to-steal, mortgage fraud, 96
Resumé
employment application fraud, 108
truthfulness and employee trustworthiness, 90
Risk assessment, anti-fraud program planning, 196–199, 202–203
Risk management, anti-fraud program, 235–236
Risk, definition, 203
Rolling lab schemes, 121

Salami technique, computer fraud, 99
Scavenging, computer fraud, 99
School system, fraud case study, 138–139
Scripting, fraud-threat agent amplification, 73
SEATP, *see* Security Education and awareness training program
Secular beliefs, fraud-threat agent motivation, 66
Securities fraud
case study of cybercrime, 133
Emulex case study, 139–140
overview, 107–108
Securities and Exchange Commission enforcement, 137–138

Security Education and awareness training program (SEATP), functions, 262–263
Sennewald, Charles A., 312
Skimming
  cash, 112
  credit cards, 95–96
Social Security, e-mail scam, 156–157
SOW, *see* Statement of work
Stamp fraud, case study, 157–158
State sponsored fraud threat, overview, 58
Statement of work (SOW), anti-fraud program, 225, 229
Stock fraud, *see* Securities fraud
Strategic business plan, evaluation for anti-fraud program establishment, 170–171
Straw-man swindle, mortgage fraud, 97
Subversive organization, malicious fraud-threat agent, 63–64
Superhighway
  advent, 14–15
  crime impact and history, 15–18
  information superhighway, *see* Internet

Tactical business plan, evaluation for anti-fraud program establishment, 171–173
Tangible asset, definition, 33
Teaming
  advantages, 245–246
  anti-fraud program planning, 189–190, 195
  case study, 258–259
  corporate peers, 248–250
  executive management as team members, 246–248
  office politics, 250–252
  satellite offices
    domestic, 257
    foreign, 257–258
  security managers, 252
  security staff, 253–256
Technical difficulty, fraud-threat agent inhibition, 70
Telecommunications fraud
  cell phones, 101
  clip-on fraud, 106–107
  hack-attacks, 100
  phreakers, 100
  prepaid cell phone fraud case, 147–148
Telemarketing, fraud, 120, 121
Terrorism
  fraud inflation of costs of attacks, 38
  funding, 4
  malicious fraud-threat agent, 58–59
  motivation, 67
Threat
  assessment for anti-fraud program planning
    man-made threats, 200–201
    natural threats, 200
  definition, 201
  vulnerabilities, 201–202
Trap door, computer fraud, 99
Trojan horse, computer fraud, 99

Urban legends, harm to corporations, 151

Virus, computer fraud, 99
Vision statement
  evaluation for anti-fraud program establishment, 179
  security department, 223
Vulnerable, definition, 202

Watkins, Sherron, 140–141
Wells Fargo, Internet fraud prevention, 91
Wells, Joseph T., 312
Whistleblowing
  Enron, 140–141
  importance, 49–50
  risks, 49–50
Wire tapping, computer fraud, 100
Withholding tax, fraud schemes, 119
Worm, computer fraud, 99

Y2K, fraud case study, 144–145

Zero-based budget, 228–229