

Contents

Introduction	xiii
Part 1 The Challenge	1
Chapter 1 The Tale of the Targeted Trojan	3
Introduction	4
The Haephrafi Case	5
The When	6
The How	6
The Hook	6
The Mechanism	6
The Who	7
The Why	7
The Cost	7
The Discovery	8
The Scope	9
Alleged Intermediary Clients	9
Alleged End-Recipients	9
Companies Identified as Victims	10
Related U.S./UK Advisories	11
UK – National Infrastructure Security Coordination Centre (NISCC)	11
U.S. – The Department of Homeland Security (DHS)	12
Chapter 2 When Insiders and/or Competitors Target a Business’s Intellectual Property	15
Introduction	16
Lightwave Microsystems	16
America Online	18
Casiano Communications	19
Corning and PicVue	20
Avery Dennison and Four Pillars	22
Lexar Media and Toshiba	24
SigmaTel and Citroen	27
3dGEO – China	29
Chapter 3 When State Entities Target a Business’s Intellectual Property	31
Introduction	32
Airbus and Saudi Arabian Airlines	33

Russian Intelligence and Japanese Trade Secrets	33
Japan and the Cleveland Clinic Foundation	36
China and Russia: TsNIIMASH-Export	38
Overt Nation State Attempts: India, Venezuela, Brazil, and Others	39
Current and Future Threats to Economic Security	41
Chapter 4 When Piracy, Counterfeiting, and Organized Crime Target a Business's Intellectual Property	45
Introduction	46
Technology Counterfeiting	50
The Apparel Industry	52
The Entertainment Industry	53
Chapter 5 Virtual Roundtable on Intellectual Property and Economic Espionage	57
Introduction	58
The Legal Perspective: Naomi Fine	60
The OpSec Perspective: Keith Rhodes	65
The Professional Investigator's Perspective: Ed Stroz	70
The DoD Cyber Sleuth's Perspective: James Christy	77
The Security and Privacy Consultant's Perspective: Rebecca Herold	81
Part 2 The Strategy	87
Chapter 6 Elements of a Holistic Program	89
Introduction	90
False Memes Lead People the Wrong Way	90
From the Industrial Age to the Information Age	91
Chapter 7 Case Study: Cisco's Award-Winning Awareness Program	97
Introduction	98
What Is This Scenario?	100
The Message Is the Medium: Be a Security Champion	102
The Message	102
When Your Message Reaches the Employees They Become Your Messengers	105
Staying on Message	106
It Takes More Than Compelling Content and Hard Work	109
Lessons Learned	110

Chapter 8 Case Study: A Bold New Approach in Awareness and Education Meets an Ignoble Fate	113
Introduction	114
The Mission, the Medium, the Message	114
Meaningful Content and Persuasive Delivery	114
Investment and Empowerment.	116
Three-Phase Approach.	116
Phase I: Engage Everyone Economically and Effectively.	117
Phase II: A Rising Tide Lifts All the Boats	119
Phase III: Deliver Vital Intelligence and Early Warning to the Executive	120
Don't Be Surprised If.	121
 Chapter 9 Case Study: The Mysterious Social Engineering Attacks on Entity Y.	 127
Introduction	128
Fundamentals of Social Engineering Attacks	129
The Mysterious Social Engineering Attacks on Entity Y	133
Guidance for the Workforce.	135
How to Recognize Elicitation	135
How to Handle the Caller	136
How to Report the Incident	136
General User-Oriented Guidance on How to Detect and Defeat Social Engineering	137
 Chapter 10 Personnel Security	 139
Introduction	140
Coming and Going: Guidelines for Background Checks and Termination Procedures	143
Two Important Caveats	154
And Everywhere in between: Guidelines for Travel Security and Executive Protection Programs.	154
 Chapter 11 Physical Security: The “Duh” Factor	 161
Introduction	162
 Chapter 12 Information Security	 187
Introduction	188

Chapter 13 The Intelligent Approach. 227

Introduction 228

The Intelligence Function As an Internal Early Warning System 230

What Happens to a Million Grains of Sand in a Perfect Storm? 232

The Partnership Issue Is a Daunting Force-Multiplier,
Double-Edged Sword. 234

**Chapter 14 Protecting Intellectual Property
in a Crisis Situation. 237**

Introduction 238

**Chapter 15 How to Sell Your Intellectual
Property Protection Program. 247**

Introduction 248

Questions to Ask and People to Approach 250

What Is Your Business Differentiation from Your Competitors? 251

 Whom Do You Have to Protect These Differentiators From? 252

 What Are the Probabilities in Terms of Likely
 Attackers, Targets, and Objectives? 254

 If the Competition Obtained or Tampered with Your
 Intellectual Property, What Harm Would Be Done? 255

 What Security Measures Would Be Cost-Effective
 and Business-Enabling? 255

Notes on Figure 15.1. 257

Notes on Figure 15.2. 257

 Executives and Board Members 257

 Research and Development 257

 Manufacturing 258

 Sales and Marketing 258

 Human Resources 258

 Operations. 259

 Risk Identification 259

Implications of IP loss 260

Notes on Figure 15.3. 261

 Implementation Plan 261

 Potential Inhibitors. 261

 Identified Milestones 261

Notes on Figure 15.4. 262

Notes on Figure 15.5. 263

 Executive Commitment 263

 Business Value Statement. 263

Notes 263

Chapter 16 Conclusion	265
Protect Your IP	266
Appendix A Baseline Controls for Information Security Mapped to ISO	267
Appendix B Leveraging Your Tax Dollar	289
Domestic	290
Department of Justice (DOJ)	290
Department of Homeland Security (DHS)	292
International	294
Department of Commerce (DOC)	294
Department of State (DOS)	294
Appendix C Notes on Cyber Forensics	297
Digital Evidence: Volume	298
Digital Evidence: Searches/Legal	299
Digital Evidence: Cell Phones	300
Digital Evidence: Accreditation	301
Definitions	302
Digital Evidence: Digital Forensics Intelligence	302
Appendix D U.S. International Trade Commission Section 337 Process	305
Appendix E U.S. Trade Representative's 2007 Special 301 Watch List	339
Appendix F U.S. Department of Justice Checklist for Reporting a Theft of Trade Secrets Offense	343
Index	349