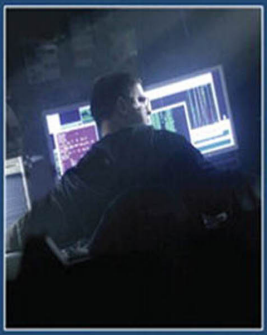
The CERT® Guide to Insider Threats



How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)

SEI SERIES • A CERT® BOOK

Dawn Cappelli

Andrew Moore

Randall Trzeciak

The CERT® Guide to Insider Threats

The SEI Series in Software Engineering

Software Engineering Institute | **Carnegie Mellon**

Addison-Wesley

Visit **informit.com/sei** for a complete list of available products.

The **SEI Series in Software Engineering** represents is a collaborative undertaking of the Carnegie Mellon Software Engineering Institute (SEI) and Addison-Wesley to develop and publish books on software engineering and related topics. The common goal of the SEI and Addison-Wesley is to provide the most current information on these topics in a form that is easily usable by practitioners and students.

Books in the series describe frameworks, tools, methods, and technologies designed to help organizations, teams, and individuals improve their technical or management capabilities. Some books describe processes and practices for developing higher-quality software, acquiring programs for complex systems, or delivering services more effectively. Other books focus on software and system architecture and product-line development. Still others, from the SEI's CERT Program, describe technologies and practices needed to manage software and network security risk. These and all books in the series address critical problems in software engineering for which practical solutions are available.

PEARSON

The CERT® Guide to Insider Threats

How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)

Dawn Cappelli
Andrew Moore
Randall Trzeciak

Addison-Wesley
Upper Saddle River, NJ • Boston • Indianapolis • San Francisco
New York • Toronto • Montreal • London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

Software Engineering Institute | **Carnegie Mellon**

The SEI Series in Software Engineering

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

Library of Congress Cataloging-in-Publication Data
Cappelli, Dawn.
The CERT guide to insider threats : how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud) / Dawn Cappelli, Andrew Moore, Randall Trzeciak.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-321-81257-5 (hbk. : alk. paper) 1. Computer crimes—Prevention. 2. Employee crimes—Prevention. 3. Information technology—Security measures. 4. Computer networks—Security measures. 5. Data protection. I. Moore, Andrew. II. Trzeciak, Randall. III. Title.
HV6773.C33 2012
658.4′78—dc23 2011047338

ISBN-13: 978-0-321-81257-5
ISBN-10: 0-321-81257-3

Text printed in the United States on recycled paper at Courier in Westford, Massachusetts.
Second printing, June 2014

For Fred, Anthony, and Alyssa. You are my life—I love you!
—Dawn

For those who make my life oh so sweet: Susan, Eric, Susan's amazing family, and my own Mom, Dad, Roger, and Lisa.
—Andy

For Marianne, Abbie, Nate, and Luke. I am the luckiest person in the world to have such a wonderful family.
—Randy

This page intentionally left blank

Contents

Preface

A night-shift security guard at a hospital plants **malware**[1] on the hospital's computers. The malware could have brought down the heating, ventilation, and cooling systems and ultimately cost lives. Fortunately, he has posted a video of his crime on YouTube and is caught before carrying out his illicit intent.

A programmer quits his job at a nuclear power plant in the United States and returns to his home country of Iran with simulation software containing schematics and other engineering information for the power plant.

A group of employees at a Department of Motor Vehicles work together to make some extra money by creating driver's licenses for undocumented immigrants and others who could not legally get a license. They are finally arrested after creating a license for an undercover agent who claimed to be on the "No Fly List."

These insider incidents are the types of crimes we will discuss in this book—crimes committed by current or former employees, contractors, or business partners of the victim organization. As you will see, consequences of malicious insider incidents can be substantial, including financial losses, operational impacts, damage to reputation, and harm to individuals. The actions of a single insider have caused damage to organizations ranging from a few lost staff hours to negative publicity and financial damage so extensive that businesses have been forced to lay off employees and even close operations. Furthermore, insider incidents can have repercussions beyond the victim organization, disrupting operations or services critical to a specific sector or creating serious risks to public safety and national security.

1. **Malware:** code intended to execute a malicious function; also commonly referred to as **malicious code.** [Note: The first time any word from the Glossary is used in the book it will be printed in boldface.]

We use many actual case examples throughout the book. It is important that you consider each case example by asking yourself the following questions: Could this happen in my organization? Could a night-shift security guard plant malicious code on our computers? Do we have employees, contractors, or business partners who might steal our sensitive information and give it to a competitor or foreign government or organization? Do we have systems that our employees could be paid by outsiders to manipulate?

For most of you, the answer to at least one of those questions will be an unequivocal *yes*! The good news is that after more than ten years of research into these types of crimes, we have developed insights and mitigation strategies that you can put in place in your organization to increase your chances of avoiding or surviving these types of situations.

Insider threats are an intriguing and complex problem. Some assert that they are the most significant threat faced by organizations today. High-profile insider threat cases, such as those conducted by people who stole and passed proprietary and classified information to WikiLeaks, certainly support that assertion, and demonstrate the danger posed by insiders in both government and private industry.[2]

Unfortunately, insider threats cannot be mitigated solely through hardware and software solutions. There is no "silver bullet" for stopping insider threats. Furthermore, malicious insiders go to work every day and bypass both physical and electronic security measures. They have legitimate, authorized access to your most confidential, valuable information and systems, and they can use that legitimate access to perform criminal activity. You have to trust them; it is not practical to watch everything each of your employees does every day. The key to successfully mitigating these threats is to turn those advantages for the malicious insiders into advantages for you. This book will help you to do just that.

In 2001, shortly before September 11, the Secret Service sponsored the Insider Threat Study, a joint project conducted by the Secret Service and the Software Engineering Institute CERT Program at Carnegie Mellon University. We never dreamed when we started that study that it would have such far-reaching impacts, and that we would become so passionate about the subject that we would end up devoting more than a decade (to date!) of our careers to the problem.

2. For information regarding the WikiLeaks insider threat cases, see http://en.wikipedia.org/wiki/Wikileaks.

When we started our work on the insider threat problem, very little was known about insider attacks: Who commits them, why do they do it, when and where do they do it, and how do they set up and carry out their crimes? After delving deep into the issue, we are happy to say that we now know the answers to those questions. In addition, we have come a long way in designing mitigation strategies for preventing, detecting, and responding to those threats.

We have the largest collection of detailed insider threat case files that we know of in the world. At the time of this publication, we had more than 700 cases, and that number grows weekly. We've had the opportunity to interview many of the victims of these crimes, giving us a unique chance to find out from supervisors and coworkers how the insider behaved at work, what precipitating events occurred, what technical controls were in place at the time, what policies and procedures were in place but not followed, and so on. We've also had the unique opportunity to actually interview convicted insiders and ask them probing questions about what made them do it, what might have made them change their mind, and what technical measures should have been in place to prevent this from happening.

We have a comprehensive database—the CERT insider threat database—where we track the technical, behavioral, and organizational details of every crime. We have combined our technical expertise in the CERT Insider Threat Center with psychological expertise from federal law enforcement, the U.S. Department of Defense (DOD), and our own independent consultants to ensure that we consider the "big picture" of the problem, not just the technical details. We have created "crime models" or "crime profiles" that describe the patterns in the crimes so that you can recognize an escalating insider threat problem in your own organization. We have created an insider threat lab where we are developing new technical solutions based on our models. We created an insider threat vulnerability assessment based on all of the cases in the CERT database so that you can learn from past mistakes and not suffer the same consequences as previous victim organizations. We publish best practices for mitigating insider threats, hold workshops, and conduct technical exercises for incident responders. Finally, we continue to collect new cases of malicious insider compromises to track the changing face of the threat.

We have been publishing our work for the past ten years; now we've decided that for the tenth anniversary of the start of our work, it is appropriate to pull all of our most current information into a book. This book provides a comprehensive reference for our entire body of knowledge on insider threats.

Scope of the Book: What Is and Is Not Included

Let's begin by defining what we mean by **malicious insider threats:**

> A malicious insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

There are a few important items to note. First of all, malicious insider threats are not only employees.[3] We chose to include contractors in our definition because contractors often are granted authorized access to their clients' information, systems, and networks, and the nontechnical controls for contractors are often much more lax than for employees. Interestingly, we did not include business partners in our original definition of insider threats in 2001. However, over time we found that more and more crimes involved not employees or contractors, but trusted business partners who had authorized access to the organization's systems, networks, or information. We encountered cases involving outsourcing, offshoring, and, more recently, cloud computing. These cases raise complex insider threat risks that should not be overlooked; therefore, we decided to add business partners to our definition.

Second, note that malicious insider attacks do not only come from current employees. In fact, one particular type of crime, insider IT sabotage, is more often committed by former employees than current employees.

Now that we have explained *whom* we will discuss in the book, let's focus on what types of crimes we will examine. Before we describe the types of crimes, it is important that you understand why we categorized them the way we have. Much of the success in our work is due to the identification of patterns found in the insider threat cases. These patterns describe the "story" behind the cases. Who commits these crimes? Why? Are there signs that they might commit a crime beforehand, so-called observable behaviors, in the workplace? When do they do it, where, and do they do it alone or with others?

The important thing to remember is that the patterns are different for each type of crime. There is not one single pattern for insider threats in general.

3. Henceforth, for simplicity, reference to insider threats specifically means malicious insider threats unless otherwise specified.

Instead, we have identified three models, or profiles, for insider threats. Those three types of crimes are as follows.

- **IT sabotage:** An insider's use of information technology (IT) to direct specific harm at an organization or an individual.
- **Theft of intellectual property (IP):** An insider's use of IT to steal intellectual property from the organization. This category includes industrial espionage involving insiders.
- **Fraud:** An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information that leads to an identity crime (e.g., identity theft, credit card fraud).

Note that this book does not specifically describe **national security espionage** crimes: the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation. Espionage is a violation of 18 United States Code sections 792–798 and Article 106, Uniform Code of Military Justice.[4] The CERT Insider Threat Center does work in that area, but that research is only available to a limited audience. However, there are many similarities between national security espionage and all three types of crimes: fraud, theft of intellectual property, and IT sabotage. Therefore, we believe there are many lessons to be learned from these insider incidents that can be applied to national security espionage as well.

In addition, this book deals primarily with *malicious* insider threats. We certainly recognize the importance of **unintentional insider threats**—insiders who accidentally affect the confidentiality, availability, or integrity of an organization's information or information systems, possibly by being tricked by an outsider's use of social engineering. However, we only recently began researching those types of threats; intentional attacks have kept us extremely busy for the past ten years! In addition, we believe that many of the mitigation strategies we advocate for malicious insiders could also be effective against unintentional incidents, as well as those perpetrated by outsiders. And finally, it is difficult to gather information regarding unintentional insider threats; because no crime was committed, organizations tend to handle these incidents quietly, internal to the organization, if possible.

4. Dictionary of Military and Associated Terms. U.S. Department of Defense, 2005.

Finally, we use many case examples from the CERT database throughout the book. Some of the examples go into greater detail than others; we include only the details that serve to illustrate the point we are making in that part in the book. We also have included a large collection of case examples in Chapter 8, as we believe these will be of great interest to many of you. Again, we stress that you should use that chapter to examine your organization and decide if you need to take any proactive measures to ensure that you do not fall victim to the same types of incidents.

As a matter of policy, we never identify the organizations or insiders involved in our case examples. Some, however, may be apparent to readers, inasmuch as they are drawn from public records, including court documents and newspaper accounts. For examples not in the public domain, we have further masked the targeted organizations to shield their identities.

Intended Audience

A common misconception is that insider threat risk management is the responsibility of IT and information security staff members alone. Unfortunately, that is one of the biggest reasons that insider attacks continue to occur, repeating the same patterns we have observed in cases since 1996, the earliest cases in the CERT database. IT and information security personnel will benefit from reading this book, as we will suggest new technical controls you can implement using technology you are already using in the workplace. In addition, this book can be used by technical staffs to motivate other stakeholders within their organization, since IT and information security cannot successfully implement an effective insider threat mitigation strategy on their own.

We wrote this book with a diverse audience in mind. The ideal audience includes top management, as their support will be needed to implement the organization-wide insider threat policies, procedures, and technologies we recommend. It is important that *all* managers understand the patterns they need to recognize in their employees, and to advocate up the management chain for support for an insider threat program.

For the same reasons, government leaders will benefit from this book, since they need to support the government-wide insider threat policies, procedures, and technologies we recommend.

Human resources personnel need to understand this book, as they are often the only ones who are aware of indicators of potential increased risk of insider threats in individual employees. Other staff members who should understand this information include security, software engineering, and physical security personnel, as well as data owners. It is also essential to include your general counsel in any discussions about implementing technical and nontechnical controls to combat the insider threat, to ensure compliance with federal, state, and local laws.

In summary, an effective insider threat program requires understanding, collaboration, and buy-in from across your organization.

Reader Benefits

After reading this book you will realize that the insider threat is real and the consequences of malicious insider activities can be extremely damaging. Real-life case studies will drive home the point that "this could happen to me." Many organizations focus their technical defenses against outsiders attempting to gain unauthorized access. This book emphasizes the need to balance defense against outsider threats with defense against insider threats, understanding that insider attacks can be more damaging than outsider attacks.

After reading this book you also will be able to recognize the high-level patterns in the three primary types of insider threats: IT sabotage, theft of intellectual property, and fraud. In addition, you will understand the details of how insiders commit those crimes. We present concrete defensive countermeasures that will help you to defend against insider attacks. You can compare your own defensive strategies to the controls we propose and determine whether your existing controls are sufficient to prevent, detect, and respond to insider attacks like those presented throughout the book. Once you identify gaps in your defensive posture, you can implement countermeasures we propose to fill those gaps.

Structure of the Book: Recommendations to Readers

We begin the book in Chapter 1, Overview, by describing the insider threat problem, and raise awareness to the complexity of the problem—tangential issues such as insider threats from trusted business partners, malicious

insiders with ties to the Internet underground, and programming techniques used as an insider attack tool. Next, we provide a breakdown of the crimes in the CERT database, followed by an overview of the CERT Insider Threat Center. Because our crime "profiles" or "models" have had such an impact on the understanding of insider threats, we also provide a short section describing why those models are so important. We end with a brief timeline of the evolution of our body of work in the CERT Insider Threat Center.

It is important that you read the first chapter so that you understand the concepts and terminology used throughout the remainder of the book. After that, you can use the book in various ways. If the first chapter has been an eye-opener for you and you are interested in gaining a comprehensive understanding of insider threats, continue reading the book from beginning to end. However, it is not necessary to read the book in that manner; it is designed such that Chapters 2 through 9 and the appendices can be used as stand-alone references.

Chapters 2, 3, and 4 are devoted to the three types of insider threats: insider IT sabotage, theft of intellectual property, and fraud. In each chapter we describe who commits the crime so that you know which positions within your organization pose that particular type of threat. We describe the patterns in how each type of crime evolves over time: What motivates the insider, what behavioral indicators are prevalent, how do they set up and carry out the crime, when do they do it, whether others are involved, and so on. We also suggest mitigation strategies throughout each chapter.

We recommend that everyone reads Chapter 2, Insider IT Sabotage, as that crime has occurred in organizations in every critical infrastructure sector.

Most organizations have some type of intellectual property that must be protected: strategic or business plans, engineering or scientific information, source code, and so on. Therefore, it is important that you read Chapter 3, Insider Theft of Intellectual Property, so that you fully understand who inside your organization poses a threat to that information.

Chapter 4, Insider Fraud, is applicable to you if you have information or systems that your employees could use to make extra money on the side. Credit card information and Personally Identifiable Information (PII) such as Social Security numbers are valuable for committing various types of fraud. However, it is also important that you also consider threats posed by insiders modifying information for financial gain. Do you have systems that outsiders would be willing to pay your employees to manipulate? Or

do you have systems that your employees could illicitly use for personal financial gain, perhaps by colluding with other employees? If so, Chapter 4 is applicable to you. Note that Chapter 4 also describes the insider threats in the CERT database involving organized crime, as all of those crimes were fraud.

Chapter 5, Insider Threat Issues in the Software Development Life Cycle, explores said issues. The **Software Development Life Cycle** (SDLC) is synonymous with "software process" as well as "software engineering"; it is a structured methodology used in the development of software products and packages. This methodology is used from the conception phase to the delivery and end of life of a final software product.[5] We explore each phase of the SDLC and the types of insider threats that need to be considered at each phase. In addition, we describe how oversights at various phases have resulted in system vulnerabilities that have enabled insider threats to be carried out later by others, often by end users of the system. If your organization develops software, you should carefully consider the lessons learned in this chapter. It should make you look differently at the entire SDLC: from how to consider potential insider threats in the requirements and design phases, to potential threats posed by developers in the implementation and maintenance phases.

If you are looking for information on mitigation strategies, go to Chapters 6 and 7. You can use Chapter 6, Best Practices for the Prevention and Detection of Insider Threats, to compare best practices for prevention and detection of insider threats to your organization's practices. Many of the best practices were described in previous chapters, but Chapter 6 summarizes all of the suggestions in a stand-alone reference. This chapter is based on our "Common Sense Guide to Prevention and Detection of Insider Threats," for years one of the top downloads on the entire CERT Web site.

If you are in a technical security role and would like more detailed information on new controls you can implement, you should read Chapter 7, Technical Insider Threat Controls. This chapter describes the technical solutions we have developed in the CERT insider threat lab. These technical solutions are based on technologies that you most likely are already using for technical security. We provide new signatures, rules, and configurations for using them for more effective detection of insider threats.

5. Whatis.com

Chapter 8, Case Examples, contains a collection of case examples from the CERT database. We provide a summary table at the beginning of the chapter so that you can reference specific cases by type of crime, sector of the organization, and brief summary of the crime. Many people have requested this type of information from us over the years, so we believe this will provide enormous value to many of you. We highly recommend that you review these cases and consider your vulnerability to the same type of malicious actions within your organization. Chapter 8 is also of value to researchers who might want to use case examples for their own research.

Chapter 9, Conclusion and Miscellaneous Issues, contains a final collection of miscellaneous information that didn't fit anywhere else in the book. For example, we provide an analysis of insiders with connections to the Internet underground. We also provide details on insiders who attacked not their own organization, but trusted business partners that had a formal relationship with their employer.

After the chapters, we provide a series of appendices.

Appendix A, Insider Threat Center Products and Services, contains information on products and services provided by the CERT Insider Threat Center, including insider threat assessments, workshops, online exercises, and technical controls. We also discuss sponsored research opportunities for the Insider Threat Center. If you are extremely concerned about insider threats and want immediate assistance from the CERT Program, be sure to read this appendix.

Appendix B, Deeper Dive into the Data, contains interesting data mined from the CERT database.

Appendix C, CyberSecurity Watch Survey, contains data collected from the CyberSecurity Watch Survey, an annual survey we conduct in conjunction with *CSO* Magazine and the Secret Service.[6]

Appendix D, Insider Threat Database Structure, contains the database structure for the CERT database. If you are interested in exactly what kind of data we track for each case, you should read this appendix. Also, we frequently respond to queries to mine the CERT database for interesting data—if you see a field or fields you would like us to explore with you, please contact us. We can be reached via email at insider-threat-feedback@cert.org.

Appendix E, Insider Threat Training Simulation: MERIT *InterActive*, contains detailed information about an interactive virtual simulation we

6. Note that in some years Deloitte and Microsoft also participated in the survey.

developed for insider threat training. It is basically a prototype of a video game for insider threat training. What do you need for a successful video game? Good guys playing against the bad guys, complex plots, interesting characters—that's insider threat! We didn't want to distract you with that information in the body of the book, but some of you might find it interesting, so we included it in this appendix. In addition, if you are interested in new and innovative training methods, this appendix should be of interest.

Appendix F, System Dynamics Background, provides background information on **system dynamics**.[7] We provide brief references to system dynamics throughout the book, but it is not necessary that you understand system dynamics when you read the book. Nonetheless, we wanted to provide more in-depth information for those of you who wish to learn more.

Finally, the book concludes with references, a glossary, and a complete index.

Note that the accompanying Web site, www.cert.org/insider_threat, contains our system dynamics models for use by other researchers. It is also updated regularly with new insider threat controls, best practices, and case examples.

In summary, the book is intended to be a reference for many different types of readers. It contains the entire CERT Insider Threat Center body of knowledge on insider threats, and therefore can be used as a reference for raising awareness, informing your risk management processes, designing and implementing new technical and nontechnical controls, and much more.

About the CERT Program

The CERT Program is part of the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh. Following the Morris worm incident, which brought 10% of Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. This center was named the CERT Coordination Center (CERT/CC).

7. "System dynamics is a computer-aided approach to policy analysis and design. It applies to dynamic problems arising in complex social, managerial, economic, or ecological systems—literally any dynamic systems characterized by interdependence, mutual interaction, information feedback, and circular causality" (www.systemdynamics.org/what_is_system_dynamics.html).

While we continue to respond to major security incidents and analyze product vulnerabilities, our role has expanded over the years. Along with the rapid increase in the size of the Internet and its use for critical functions, there have been progressive changes in intrusion techniques, increased amounts of damage, increased difficulty of detecting an attack, and increased difficulty of catching the attackers. To better manage these changes, the CERT/CC is now part of the larger CERT Program, which develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of critical services.

When created, the CERT acronym stood for Computer Emergency Response Team, originally focused on incident response. In the years since, the CERT acronym continues to be used but it no longer represents the single focus as we have expanded beyond incident response into areas such as network situational awareness, malicious code analysis, secure coding, resilience management, insider threat, digital investigations and intelligence, and workforce development.

The CERT Insider Threat Center

The objective of the CERT Insider Threat Center is to assist organizations in preventing, detecting, and responding to insider compromises. We have been researching this problem since 2001 in partnership with the DOD, the U.S. Department of Homeland Security (DHS), other federal agencies, federal law enforcement, the intelligence community, private industry, academia, and the vendor community. The foundation of our work is the CERT database of more than 700 insider threat cases. We use system dynamics modeling to characterize the nature of the insider threat problem, explore dynamic indicators of insider threat risk, and identify and experiment with administrative and technical controls for insider threat mitigation. The CERT insider threat lab provides a foundation to identify, tune, and package technical controls as an extension of our modeling efforts. We have developed an assessment framework based on the fraud, theft of intellectual property, and IT sabotage case data that we have used to assist organizations in identifying their technical and nontechnical vulnerabilities to insider threats, as well as executable countermeasures. The CERT Insider Threat Center is uniquely positioned as a trusted broker to assist the community in the short term, and through our ongoing research.

Dawn Cappelli and Andy Moore have been working on CERT insider threat research since 2001, and Randy Trzeciak joined the team in 2006. Dawn is the technical manager of the CERT Insider Threat Center, Andy is the lead researcher, and Randy is the technical lead for insider threat research. Although our insider threat team has now grown into an official Insider Threat Center, for many years the CERT Program's insider threat team consisted of Andy, Randy, and Dawn, which is why we decided to team up and capture our history in this book.

Summary

The purpose of this book is to raise awareness of the insider threat issue from the ground up: staff members in IT, information security, and human resources; data owners; and physical security, software engineering, legal, and other security personnel. We strongly believe after studying this problem for more than a decade that in order to effectively mitigate insider threats it takes common understanding, support, and communication from all of those people across the organization. In addition, buy-in is needed from upper management, as they will need to support the cross-organizational communication required to formulate an effective mitigation strategy. And finally, it requires awareness and consideration by government leaders, as some of the issues are even larger than individual organizations. Employee privacy issues and mergers and acquisitions with organizations outside the United States are two such examples.

This book covers our extensive work in studying insider IT sabotage, theft of intellectual property, and fraud. Although it does not deal explicitly with insiders who committed national security espionage, many of the lessons in this book are directly applicable to that domain as well.

Most of the book can be read and easily understood by technical and nontechnical readers alike. The only exception is Chapter 7. If you are not a "technical" person you are best off skipping this chapter. However, we strongly suggest you lend the book to your technical security staff so that they can consider implementing these controls.

Now that you understand the purpose of the book and its contents, we will begin to dig a little deeper into each type of insider crime, our modeling of insider threats, and the CERT Insider Threat Center in Chapter 1. We recommend that you read that chapter next so that you understand the basic concepts. After completing Chapter 1 you will have the foundation you need so that you can explore the rest of the book in any order you wish!

This page intentionally left blank

Acknowledgments

We would like to start by thanking our amazing team at the CERT Insider Threat Center. This book represents the hard work of many brilliant people. First, thank you to our current team in the Insider Threat Center, listed here in the order in which they joined the team: Adam Cummings, Mike Hanley, Derrick Spooner, Chris King, Joji Montelibano, Cindy Nesta, Josh Burns, George Silowash, and Dr. Bill Claycomb. And a special thank you to Tara Sparacino and Cindy Walpole, who helped us to keep our heads above water at work while we wrote this book in our "spare time." The CERT Insider Threat Center is part of the Enterprise Threat and Vulnerability Management (ETVM) team in the CERT Program. The ETVM team is a very tight-knit group, and we would be remiss if we did not acknowledge these awesome, dedicated technical security experts, again listed in the order in which they started on the team: Georgia Killcrece (retired, but sorely missed!), Robin Ruefle, Mark Zajicek, David Mundie, Becky Cooper, Charlie Ryan, Russ Griffin, Sandi Behrens, Alex Nicoll, Sam Perl, and Kristi Keeler.

Thank you to the current and former CMU/SEI/CERT staff members who have participated in our insider threat work over the years: Chris Bateman, Sally Cunningham, Casey Dunlevy, Rob Floodeen, Carly Huth, Dr. Joseph ("Jay") Kadane, Greg Longo, David McIntire, David Mundie, Dr. Dan Phelps, Stephanie Rogers, Dr. Greg Shannon, Dr. Tim Shimeall, Rhiannon Weaver, Pam Williams, Bradford Willke, and Mark Zajicek. And a special thank you to Dr. Tom Longstaff, who was the CERT technical manager for the original Insider Threat Study, and worked on the CERT Program's original insider threat collaboration with the U.S. Department of Defense (DOD) Personnel Security Research Center.

Thank you to the many fabulous graduate students who have worked on our insider threat projects throughout the years, starting with our two current students: Todd Lewellen, Lynda Pillage, Jen Stanley, Chase Midler, Andrew Santell, Luke Hogan, Jaime Tupino, Tyler Dean, Will Schroeder,

Matt Houy, Bob Weiland, Devon Rollins, Tom Caron, John Wyrick, Christopher Nguyen, Hannah Joseph, and Akash Desai. Many of those students were from the Scholarship for Service Program—we commend the U.S. federal government for this program, which produces the most outstanding talent in the cybersecurity field.

A special thank you to Dr. Eric Shaw, who has been a Visiting Scientist in the CERT Program and a clinical psychologist at Consulting & Clinical Psychology, Ltd. Eric has been the guiding force in the psychological aspects of our research since the conclusion of our first Insider Threat Study with the Secret Service National Threat Assessment Center.

Thank you to Noopur Davis, Claude Williams, and Dr. Marvine Hamner, who worked for us as visiting scientists.

Thank you to the CERT Program's director, Rich Pethia, and deputy director, Bill Wilson, who have given us the autonomy and authority over the past decade to take our research in so many exciting directions. Thank you to our retired boss, Dr. Barbara Laswell, who helped us evolve from the Insider Threat Team of three people into the CERT Insider Threat Center. Thank you to SEI Director Dr. Paul Neilson and Deputy Director Clyde Chittister, for their support and recognition. We're extremely grateful to Terry Roberts for the visibility she has brought to our work. And thank you to Dr. Angel Jordan, former provost of Carnegie Mellon University, who has been an advocate for our work over the years.

We would like to thank the Secret Service, our original partner in this quest to understand and help organizations protect themselves from malicious insider attacks. Thank you to National Threat Assessment Center (NTAC) staff members who participated on the project, especially research coordinator Dr. Marisa Reddy Randazzo, who founded and directed the Insider Threat Study within NTAC; Dr. Michelle Keeney, who took over when Marisa left; Eileen Kowalski, who was the lynchpin throughout the project; and Matt Doherty, the Special Agent in Charge of NTAC. Also, thank you to Jim Savage, the sponsor of our original work with the Secret Service. Finally, a big thank you to our Secret Service liaisons for the Insider Threat Study, who moved to Pittsburgh and joined the CERT Program for a few years: Cornelius Tate, Dave Iacovetti, and Wayne Peterson. What great times we had in those good old days! And thank you to our current Secret Service liaisons, Tom Dover and Ryan Moore.

A special thank you to Dr. Douglas Maughan and the DHS Science and Technology (S&T) Directorate, who took over funding of the original CERT/Secret Service Insider Threat Study shortly after DHS was formed.

We're especially excited that Doug came back to us last year and told us he wanted to get the old team back together—and funded our current study of insider threats in the financial sector. In addition, we're receiving assistance on that project from the Secret Service, U.S. Department of the Treasury, and the financial sector. Thank you to Brian Peretti, who was in the very first financial sector review of our work for the original study, and is now back on the team in our current fraud project. And thank you to Ed Cabrera and Trae McAbee from the Secret Service—we could not possibly succeed in the current study without all of your hard work in gathering all of the case files and scheduling the interviews. Thank you to Pablo Martinez for being a strong supporter of our work, starting back in the original study, and continuing today.

Thank you to the Army Research Office and Carnegie Mellon CyLab, especially Dr. Pradeep Khosla, Dr. Virgil Gligor, Dr. Adrian Perrig, Richard Power, Gene Hambrick, and Dr. Don McGillen, who provided seed funding for many of our insider threat projects that have grown into full bodies of work. Your support sustained the insider threat database for years, enabled us to experiment with our modeling work, provided the infrastructure for the insider threat lab, and funded one of our most "fun" projects: our insider threat "video game."

We are especially grateful to our current sponsors at the U.S. DHS Federal Network Security (FNS) branch, Matt Coos and Don Benack, as well as the project leads, Rob Karas, Sean McAfee, and Will Harmon. Don and Matt had the vision to step up to the plate three years ago and fund our work "for the good of all." They realized the importance of our work and were willing to fund it before insider threats became a top-priority issue in the current cybersecurity environment. Thanks to their foresight, we can offer technical controls, assessments, and training to the community. We're excited about the opportunity to continue to make an impact together!

We are also thankful to our sponsors and collaborators in the DOD and intelligence community: Dr. Deborah Loftis, Laura Sellers, Dr. Stephen R. Band, Dr. Aaron J. Ferguson, Dr. Lynn Fischer, Dr. Howard Timm, Dr. Katherine Herbig, Dr. Ron Dodge, and Dr. Kirk Kennedy. Their expertise and experience have enabled a much richer treatment of the insider threat problem than would have otherwise been possible.

Our work in the system dynamics modeling of insider threats began and continues to be influenced by the Security Dynamics Network (SDN), a largely unfunded and loosely coordinated group of national laboratories and universities applying system dynamics to explore issues

of cybersecurity. In the past, the group has focused on malicious insider threats and has been a source of expertise, information, and inspiration for the insider threat models developed in this book. We are very thankful to the members of the SDN, especially its founder, Dr. Jose Gonzalez of Agder University College; Dr. David Andersen and Dr. Eliot Rich of the University at Albany; Dr. Ignacio Martinez-Moyano of Argonne National Laboratory; Dr. Stephen Conrad of Sandia National Laboratories; and Dr. Jose Maria Sarriegui of the University of Navarra. A special thank you goes to Dr. Elise Weaver of the Human Resources Research Organization, who worked with us as a Visiting Scientist at the CERT Program and assisted us in our very first system dynamics modeling efforts.

We would also like to thank all of the SEI business development staff members who have helped us with our insider threat work over the years: Jan Philpot, Mike Greenwood, Joe McLeod, Frank Redner, David Ulicne, Bob Rosenstein, Greg Such, Dave Scherb, and Angela Llamas-Butler. Thank you to Summer Fowler and Lisa Marino, who have helped us with project management activities that have become increasingly complex over the years, and Michele Tomasic, who has helped us with so many things over the years. Thank you to Bill Shore and everyone in the SEI Security Office, and Dave Thompson and everyone in SEI IT, especially Jerry Czerwinski and Craig Lewis; and thank you to Linda Pesante and her staff, especially Ed Desautels and Paul Ruggerio, who have helped us with editing and technical writing over the years. Also, thank you to David Biber for the wonderful graphics he has created for us over the years, including nice crisp images for this book!

Finally, we would like to thank Dr. Don Marinelli, cofounder of Carnegie Mellon's Entertainment Technology Center (ETC), and the ETC faculty and students who worked with us to create the first video game for insider threat training. Semester 1: faculty advisors Dr. Scott Stevens and Jessica Trybus; student team Ankur Ahlawat, Chris Daniel, Aditya Dave, and Todd Waits; and visiting scholars Soo Jeoung Kim and Michelle Macau. Semester 2: faculty advisors Dr. Scott Stevens and Dr. Ralph Vituccio; and student team Stephen Calender, Julie Charles, Evan Miller, and Todd Waits. We still hope to interest a sponsor in turning that prototype into an operational system someday!

If we forgot someone who has helped us throughout the years, we apologize profusely! We tried hard to include everyone, but if we overlooked you, please let us know.

From Dawn: Thank you to my wonderful husband and soul mate, Fred—you've been inspiring me for 35 years and without you I can't imagine where I would be! To my daughter and best girlfriend, Alyssa—I treasure all of our fun times together. To my son, Anthony—you are truly the happiest person I know! Thanks to my sister, Cindy, who has always been there for me. And finally, thank you to the greatest parents in the world—whom I miss terribly. Your faith and encouragement made me what I am today.

Thank you to Andy and Randy—how exciting to accomplish this together after all of those years as team "Andy, Randy, and Dawn!"

From Andy: My heartfelt thanks go, most of all, to my beautiful wife, Susan, for sharing our life adventure. Coming home to you each day is the best thing in my life! And thanks to my incredible son, Eric, who put up with my having my nose in a laptop during many early morning hours. Your achievements continue to amaze me and your love and friendship enrich our lives immeasurably. Finally, thanks to Dawn and Randy's steadfast dedication and friendship. It is hard to believe how far we've come in the ten years since it all started.

From Randy: Thank you, Marianne, for being my wife and best friend! You are truly a blessing to me, to our family, and to all the other lives you touch. To my daughter, Abbie, you are an amazing, intelligent, and strong young lady. To Nate the Great, always keep those around you laughing. To Luke, thank you for making every day fun. Thank you to my parents for all of the hard work and sacrifices you made over the years!

Finally, thank you to Dawn and Andy for bringing me into the circle of trust. It is truly a pleasure working with both of you!

This page intentionally left blank

Chapter 3

Insider Theft of Intellectual Property

Insider theft of intellectual property (IP): *an insider's use of IT to steal proprietary information from the organization. This category includes industrial espionage involving insiders.*

Intellectual property: intangible assets created and owned by an organization that are critical to achieving its mission.[1]

Types of IP Stolen

The types of IP stolen in the cases in our database include the following:

- Proprietary software/source code
- Business plans, proposals, and strategic plans
- Customer information
- Product information (designs, formulas, schematics)

1. While IP does not generally include individuals' Personally Identifiable Information (PII), which an organization does not own, it could include a database that the organization developed that contains PII.

What if one of your scientists or engineers walked away with your most valuable trade secrets? Or a contract programmer whose contract ended took your source code with him—source code for your premier product line? What if one of your business people or salespeople took your strategic plans with him to start his own competing business? And possibly worst of all, what if one of them gave your intellectual property to a foreign government or organization? Once your IP leaves the United States it's extremely difficult, often impossible, to get it back.

Those are the types of crimes we will examine in this chapter. Organizations in almost every critical infrastructure sector have been victims of insider theft of IP.

In one case of insider theft of IP, an engineer and an accomplice stole trade secrets from four different high-tech companies they worked for, with the intention of using them in a new company they had created with funding from a foreign country. In another, a company discovered that an employee had copied trade secrets worth $40 million to **removable media,**[2] and was using the information in a side business she had started with her husband. In yet another, a large IT organization didn't realize that it had been victimized until it happened to see a former employee at a trade show selling a product that was remarkably similar to the organization's!

When we began examining the theft of IP cases in our database we surmised that insiders probably stole IP for financial reasons. We were very wrong about that! We found that quite the opposite is true: Very few insiders steal intellectual property in order to sell it. Instead, they steal it for a business advantage: either to take with them to a new job, to start their own competing business, or to take to a foreign government or organization.

Very few insiders steal intellectual property in order to sell it. Instead, they steal it for a business advantage: either to take with them to a new job, to start their own competing business, or to take to a foreign government or organization.

Another misconception about theft of IP is that system administrators are the biggest threat, since they hold "the keys to the kingdom." Not according

2. **Removable media:** computer storage media that is designed to be removed from the computer without powering the computer off. Examples include CDs, USB flash drives, and external hard disk drives.

to our data! We don't have a single case in our database in which a system administrator stole intellectual property, although we do have a few cases involving other IT staff members. However, keep in mind that we only have cases in which the perpetrator was discovered and caught; it is possible that system administrators *are* stealing IP and are simply getting away with it.

In fact, the insiders who steal IP are usually current employees who are scientists, engineers, programmers, or salespeople. Most of them are male. We checked the U.S. Bureau of Labor Statistics to determine if most of those types of positions are held by men, but the results, listed here for 2010, were inconsistent.

- 12.9% of all architectural and engineering positions were held by women.
- 45.8% of all biological scientists were women.
- 33.5% of all chemists and materials scientists were women.
- 26.2% of all environmental scientists and geoscientists were women.
- 39.5% of all other physical scientists were women.
- 49.9% of all sales and related occupations were held by women.[3]

Insiders who steal IP are usually current employees who are scientists, engineers, programmers, or salespeople.

We are not suggesting that you assume men are more likely than women to commit these types of crimes. On the contrary, we suggest that rather than focusing on demographic characteristics, you should focus on the following:

- Understanding the positions at risk for these crimes
- Recognizing the patterns and organizational factors that typically surround insider theft of IP incidents
- Implementing mitigation strategies based on those patterns

These types of crimes are very difficult to detect because we found that these insiders steal information for which they already have authorized

3. ftp://ftp.bls.gov/pub/special.requests/lf/aat11.txt

Insiders steal information for which they already have authorized access, and usually steal it at work during normal business hours. In fact, they steal the same information that they access in the course of their normal job. Therefore, it can be very difficult to distinguish illicit access from legitimate access.

access, and usually steal it at work during normal business hours. In fact, they steal the same information that they access in the course of their normal job. Therefore, it can be very difficult to distinguish illicit access from legitimate access.

Fortunately, we have come up with some good strategies based on our MERIT model of insider theft of intellectual property that we will detail in this chapter. The first half of this chapter describes the model at a high level. In the second half of the chapter we will dig deeper into the technical methods used in committing these crimes and mitigation strategies that you should consider based on all of this information.

The MERIT model describes the profile of insider theft of IP by identifying common patterns in the evolution of the incidents over time. These patterns are strikingly similar across the cases in our database. Unfortunately, we were not quite as lucky in creating our theft of IP model as we were in creating our insider IT sabotage model. While we found one very distinct pattern that was exhibited in almost every IT sabotage case, we could not identify a single pattern for theft of IP. Instead, we ended up identifying two overlapping models.

- **Entitled Independent:** an insider acting primarily alone to steal information to take to a new job or to his[4] own side business
- **Ambitious Leader:** a leader of an insider crime who recruits insiders to steal information for some larger purpose

The cases in our database break up just about 50/50 between the two models. In addition, the models have different but overlapping patterns; the Ambitious Leader model builds from the Entitled Independent model. This is good news, as our suggested mitigation strategies apply to both models.

4. Most of the insiders who stole IT property were male. Therefore, male gender is used to describe the generic insider in this chapter.

In this chapter we will describe the patterns identified in both models, and will present mitigation strategies that use those patterns to your advantage.[5] These techniques include a combination of automated and manual countermeasures. In addition, some are focused on protection of your most valuable information assets, while others are targeted at specific employees triggered by indicators that could suggest an increased risk of attack.

For example, if you can identify your most critical assets, technical solutions such as **digital watermarking,**[6] **digital rights management,**[7] and **data loss prevention systems**[8] can be implemented to prevent those assets from leaving your network. There are several drawbacks to these technical solutions, however. First of all, most organizations can't or haven't identified and located all of their most critical computer files. This can be an overwhelming task, particularly in a large organization. In addition, many of you have trusted business partners that legitimately move your critical files back and forth from their own networks to yours. Those types of environments can complicate use of those types of technologies.

Because of the complexity of implementing a purely technical solution focused on critical assets, we also suggest targeted monitoring of employees or contractors who are leaving your organization. We found that most insiders steal intellectual property as they are leaving the organization, suggesting that it could be beneficial to watch their actions more closely, specifically those involving removable media, email, and other methods used in exfiltrating information.

We will provide suggested countermeasures throughout this chapter, and detailed technical information for the theft of IP cases in the section Mitigation Strategies for All Theft of Intellectual Property Cases at the end of the chapter. The bottom line is that unlike IT sabotage, where the goal is to catch the

5. Material in this chapter includes portions of previously published works. Specifically, the insider theft of intellectual property modeling work was published by Andrew Moore, Dawn Cappelli, Dr. Eric Shaw, Thomas Caron, Derrick Spooner, and Randy Trzeciak in the *Journal of Wireless Mobile Networks, Ubiquitous Computing,* and *Dependable Applications* [Moore 2011a]. An earlier version of the model was published by the same authors in [Moore 2009].

6. **Digital watermarking:** the process of embedding information into a digital signal that may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification (Wikipedia).

7. **Digital rights management (DRM):** a term for access control technologies that are used by hardware manufacturers, publishers, copyright holders, and individuals to limit the use of digital content and devices.

8. **Data loss prevention (DLP) systems:** refers to systems designed to detect and prevent unauthorized use and transmission of confidential information (Wikipedia). Also commonly called **data leakage tools.**

insider as he is setting up his attack—planting malicious code or creating a backdoor account—you cannot really detect theft of IP until the information is actually in the process of being stolen—as it is being copied to removable media or emailed off of the network. In other words, your window of opportunity can be quite small, and therefore you need to pay close attention when you see potential indicators of heightened risk of insider theft of IP.

We have some "good-news" cases that indicate that it is possible to detect theft of IP using technical measures in time to prevent disastrous consequences.

- An organization detected IP emailed from a contractor's email account at work to a personal email account, investigated, and discovered significant data exfiltration by the contractor. The organization found the contractor was working with a former employee to steal information to start a competing business. Obviously, the stolen IP was extremely valuable, as the contractor was arrested, convicted, ordered to pay a fine of $850,000, and sentenced to 26 years in prison!
- After a researcher resigned and started a new job, his former employer noticed that he had downloaded a significant number of proprietary documents prior to his departure. This led to his arrest before he could transfer the information to his new employer's network. The information was valued at $400 million.
- During an organization's routine auditing of **HTTPS traffic**[9] it discovered that an employee who had turned in his resignation had exfiltrated proprietary source code on four separate occasions to a server located outside the United States. Although the employee claimed the transfer was accidental, and that he had only uploaded open source information, he was arrested.

Impacts

The impacts of insider theft of IP can be devastating: Trade secrets worth hundreds of millions of dollars have been lost to foreign countries, competing products have been brought to market by former employees and contractors, and invaluable proprietary and confidential information

9. **HTTPS traffic:** network traffic that is encrypted via the Secure Sockets Layer protocol.

has been given to competitors. More than half of our theft of IP cases involved trade secrets.

More than half of our theft of IP cases involved trade secrets.

In addition, impacts in these cases can reach beyond the victim organization. Here are some examples.

- Source code for products on the U.S. Munitions List was shared with foreign military organizations.[10]
- A government contractor stole passwords that provided unauthorized access to sensitive, potentially classified information.
- Source code was added to software in a telecommunications company that enabled the perpetrators to listen in on phone calls made by 103 high-ranking government and nongovernment officials.

Estimated financial impacts in the theft of IP cases in the CERT database averaged around $13.5 million (actual) and $109 million (potential).[11] The median estimated financial impact was $337,000 (actual) and $950,000 (potential). This means that a few extremely high-impact cases skew the average significantly. The highest estimated potential financial losses were

- $1 billion in a high-tech case in the IT sector
- $600 million in a telecommunications company
- $500 million in a pharmaceutical company
- $400 million in a chemical company
- $100 million in a biotech company

The highest estimated actual financial losses were

- $100 million in a manufacturing business
- $40 million in a manufacturing business
- $6 million in the financial services sector
- $1.5 million in a high-tech software development organization

10. In U.S. law, the U.S. Munitions List is the list of weapons and similar items that are subject to licensing because of the danger they pose. The U.S. Munitions List is related to the International Traffic in Arms Regulations. Farlex Financial Dictionary. Copyright © 2009 Farlex, Inc.

11. Twenty-five of the 85 cases of theft of IP had known estimates on actual or potential financial impact.

These are only some of the cases with the highest financial consequences. We provided this list for several reasons. First, we are frequently asked how to calculate return on investment (ROI) for insider threat mitigation. That is a very difficult question, and one that has not yet been answered adequately for cybersecurity in general. To start, you should identify what your critical assets are, and estimate the potential loss if those assets were to leave your organization. The losses we listed from actual cases should help you to convince your management that insider threat is not to be taken lightly!

Second, although almost half of the insider theft of IP cases occurred in the IT sector, we want to emphasize that these types of crimes have resulted in significant losses in other sectors as well.

We strongly suggest that you pay close attention to this chapter if you are concerned about the security of your proprietary and confidential information. Now that we have caught your attention, let's look at the characteristics and "big picture" of insider theft of intellectual property.

General Patterns in Insider Theft of Intellectual Property Crimes

The intent of our MERIT model of insider theft of intellectual property is to describe the general profile of insider theft of IP crimes. The MERIT models describe the patterns in the crimes as they evolve over time—profiling the life cycle of the crime, rather than profiling only the perpetrator.

The MERIT model of insider theft of IP was first published in 2009. The model was created using system dynamics modeling, which is described in the original report and in Appendix F, System Dynamics Background. Over the years, however, we have found that a higher-level view of that model is more useful in describing the patterns to practitioners so that clear, actionable guidance can be provided for mitigating these incidents. That higher-level form of the model and accompanying countermeasure guidance is presented in the remainder of this chapter.

As mentioned earlier, our overall model for theft of IP actually consists of two models: the Entitled Independent and the Ambitious Leader; we will present those one at a time. We have broken each model down into small pieces in this chapter in order to make it more understandable. The full model of the Entitled Independent is shown in Figure 3-1. Figure 3-2 shows the full model of the Ambitious Leader.

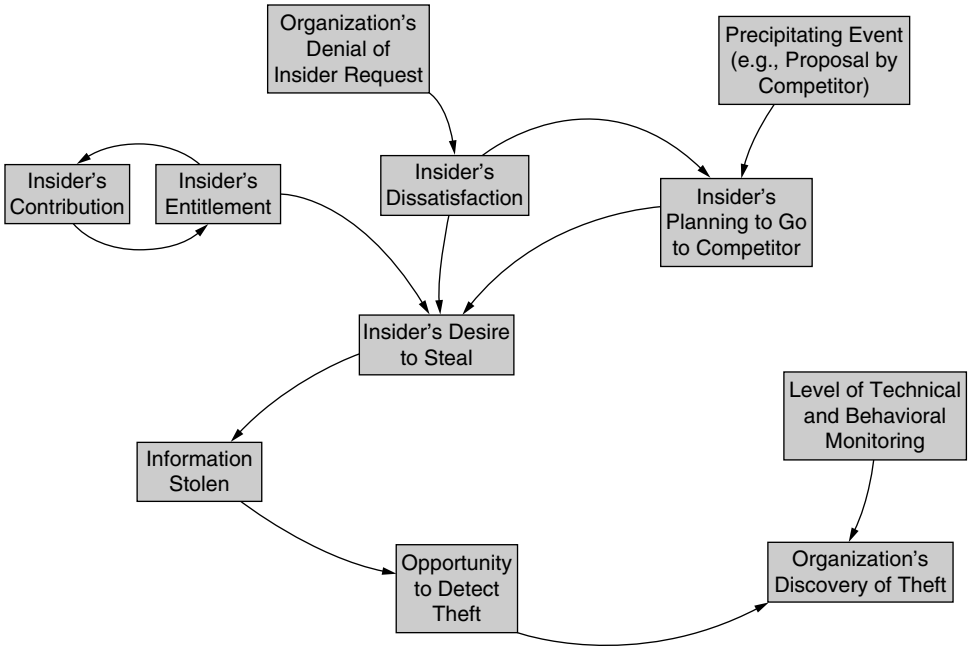


Figure 3-1 *MERIT model of insider theft of IP: Entitled Independent*

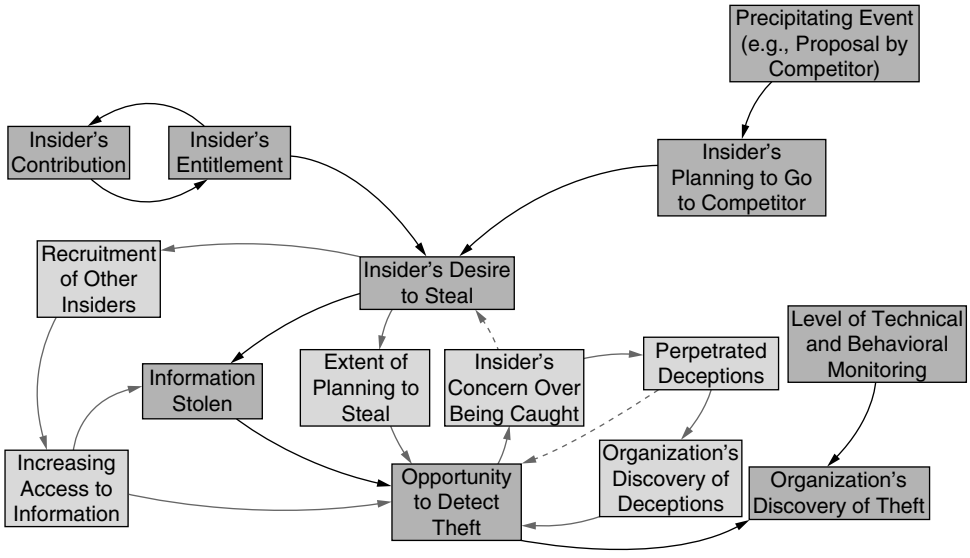


Figure 3-2 *MERIT model of insider theft of IP: Ambitious Leader*

The Entitled Independent

This section describes the model of the Entitled Independent, an insider acting primarily alone to steal information to take to a new job or to his own side business.

NOTE

Most insiders felt entitled to take the information they were accused of stealing.

Based on our review of incident descriptions and interviews with victim organizations, investigators, and prosecutors of insider cases, we determined that most insiders felt entitled to take the information they were accused of stealing. The majority of the insiders stole information that they had worked on while employed by the organization.

Insider Contribution and Entitlement

Figure 3-3 shows how the insider's feeling of entitlement toward the information he develops escalates over time. The employee comes into your organization with a desire to contribute to its efforts. As time goes on and he develops information, writes source code, or creates products, his contribution becomes more tangible. These insiders, unlike most employees and contractors, have personal predispositions that result in a perceived sense of ownership and entitlement to the information created by the entire group. The longer he works on the product, the more his sense of entitlement grows.

This sense of entitlement can be particularly strong if the insider perceives his role in the development of products as especially important. If his work is dedicated to a particular product—for example, development of a software system, or the building of customer contact lists—he may have a great sense of ownership of that product or information. This leads to an even greater sense of entitlement. In addition, consistent with good management practice, individuals may receive positive feedback for their efforts,

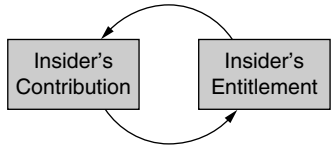


Figure 3-3 *Insider entitlement*

which may further reinforce their sense of ownership, because of their predispositions.

Evidence of entitlement was extreme in a few cases. One Entitled Independent, who had stolen and marketed a copy of his employer's critical software, created a lengthy manuscript detailing his innocence and declaring that everyone at the trial had lied. After being denied a raise, another insider stole the company's client database and threatened to put them out of business on his way out the door.

What Can You Do?

Knowing that insiders who steal IP tend to steal the assets they helped to develop is a key factor in designing a mitigation strategy. If you can identify your critical intellectual property, you can narrow down the list of employees and contractors who are at highest risk of stealing it to those who are working on it now or have worked on it in the past.

In addition, keep in mind that people move around within your organization. How good are you at adjusting access controls as those moves happen? Just because someone has moved to another project or area of the organization doesn't mean he doesn't still feel a sense of entitlement to his past work. Erosion of access controls is a problem that needs to be solved in order to reduce risk of insider theft of intellectual property. Almost three-quarters of the insiders in our theft of IP cases had authorized access to the information stolen at the time of the theft, but that doesn't mean that all of them *should* have had access. In many organizations, employees tend to transfer over time to different parts of the organization. They often accumulate privileges needed to perform new tasks as they move, without losing access they no longer need. Unfortunately, many insiders, at the time when they stole information, had accesses above and beyond what their job descriptions required.

We suggest that you periodically review and adjust your access controls for critical assets. We helped one organization set up an effective mechanism for controlling access once an employee transfers to another group. The organization realized that it couldn't disable the employee's access immediately upon transfer since there is typically a transition period in which the employee still needs access to his old team's information. So the organization set up an automated email to be sent from its HR system to the employee's previous supervisor three months after the date of transfer. This email lists all of the email aliases the employee is on, shared folders and collaboration sites to which the employee has access, and so on, and suggests that the supervisor contact IT to disable any access that is no

longer necessary. This mechanism has been very successful in controlling the erosion of access controls in the organization.

Some insiders exhibited an unusual degree of possessiveness toward their work before stealing it. For instance, a few insiders kept all source code on their own laptops and refused to store it on the file servers, so they would have full control over it. This type of behavior should be recognized and remediated as early as possible.

Insider Dissatisfaction

Dissatisfaction played a role in many of the Entitled Independent cases. Dissatisfaction typically resulted from the denial of an insider's request, as shown in Figure 3-4. Denial of an employee or contractor request can lead to dissatisfaction, which in turn decreases the person's desire to contribute. This also affects the person's sense of loyalty to you. Dissatisfaction often spurred the insider in our cases to look for another job; the majority had already accepted positions with another company or had started a competing company at the time of their theft. Once the insider receives a job offer and begins planning to go to a competing organization, his desire to steal information increases. This desire is amplified by his dissatisfaction with his current employer and his sense of entitlement to the products developed by his group.

> Dissatisfaction often spurred the insider in our cases to look for another job.

In one-third of the cases, the insider actually used the proprietary information to get a new job or to benefit his new employer in some way.

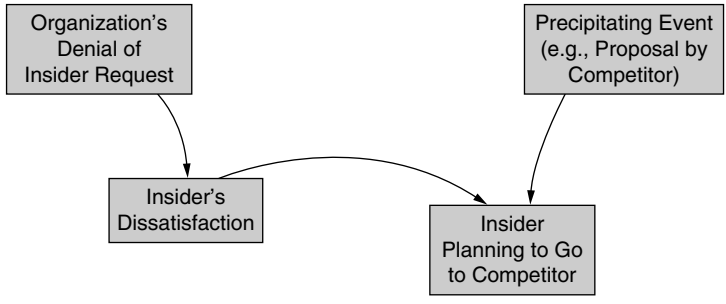


Figure 3-4 *Insider dissatisfaction leading to compromise*

Issues Leading to Dissatisfaction

Issues leading to dissatisfaction in the CERT database include the following:

- Disagreement over ownership of intellectual property
- Financial compensation issues
- Disagreement over benefits
- Relocation issues
- Hostile work environment
- Mergers and acquisitions
- Company attempting to obtain venture capital
- Problems with supervisor
- Passed over for promotion
- Layoffs

In more than one-third of the cases, the insider took the information just in case he ever needed it, with no specific plans in mind. One insider actually broke into his organization's systems after he was terminated to find out whether the organization had made any further progress on the product he had helped develop while he worked there.

What Can You Do?

It is inevitable that many of your employees will find new jobs at some point in time. Now that you understand that these departing employees could pose increased risk of insider theft of intellectual property, you should consider a review of your termination policies and processes. As soon as an employee turns in his resignation, you need to be prepared to act, as you will see in the next section. If you can quickly and easily identify the critical information that employee has access to, you can kick into prevention and detection mode.

Also, food for thought: Some of the insiders who stole IP were contractors. How do you handle contractors when they leave your organization? In our insider threat assessments we have discovered a disturbing trend in ill-defined or loosely enforced procedures for contractor terminations. Although contractors only account for 12% of our insider theft of IP crimes, the risk they pose should not be disregarded. Contract award cycles can range from five years, to three, to even one year. Are you able to track access granted to contractors and ensure appropriate

access even when contractors and contracting organizations change on a frequent basis?

Insider Theft and Deception

NOTE

The insider's plan to leave the organization, dissatisfaction, and his sense of entitlement all contribute to the decision to steal the information.

As shown in Figure 3-5, eventually the desire to steal information becomes strong enough, leading to the theft and finally the opportunity for you to detect the theft. Perhaps someone observes an employee's actions, or consequences of those actions, that seem suspicious in some way. The most likely person to discover an insider theft according to our data is a nontechnical employee; in cases where we were able to isolate the person who discovered the incident, 72% were detected by nontechnical employees. Therefore, you should have processes in place for employees to report suspicious behavior, employees should be aware of those processes, and you should follow up on reports quickly, particularly if they concern an employee who fits the profile described in our models.

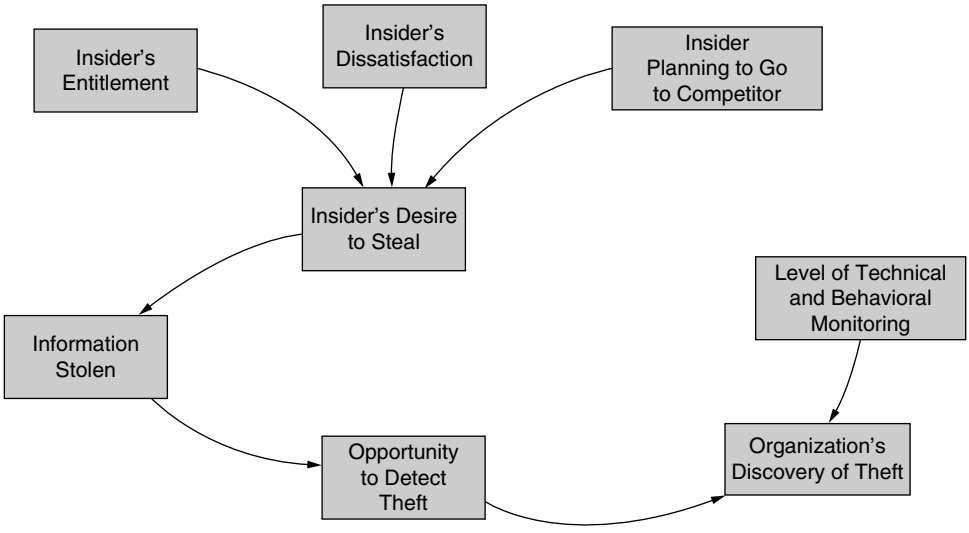


Figure 3-5 *Insider theft and deception*

Our Entitled Independents did not exhibit great concern with being caught. Even though signed IP agreements were in place in around 40% of the cases, fewer than one-quarter of the Entitled Independents tried to deceive the organization while taking their information. While explicit deception is not a major factor in most of these crimes, the fact that it did occur in one-fourth of them suggests that you need to anticipate it when designing your countermeasures.

For example, upon announcing his resignation, one insider lied to his manager and said he had no follow-on employment, even though he had told a coworker about his new job at a competitor. If you become aware of deliberate deception like this, it may be an indicator of problems to come. Deceptions generally make it harder for you to sense the risk of theft, and that is why the insider does it. But if you are vigilant, deceptions may be discovered, alerting you to increased risk of insider threat. If the organization in this example had known that the insider had given contradictory information to his manager and coworker, it may have been forewarned of the heightened risk.

In general, your accurate understanding of your risk is directly related to your ability to detect the insider's illicit actions. With sufficient levels of technical and behavioral monitoring, these actions may be discoverable.

NOTE

Most information was stolen within one month of resignation using a variety of methods.

Most of these crimes tend to be quick thefts around resignation. More than one-half of the Entitled Independents stole information within one month of resignation, which gives you a well-defined window of opportunity for discovering the theft prior to employee termination. It is important that you fully understand the one-month window, however, as it is a bit more complex than it first appears. First, the one-month window includes the month *before* the insider turns in his resignation and the month *after* he resigns; actually two months total. This means that you need to have technical measures in place at all times so that you can go back in time and review past online activity. Second, some of these insiders stole IP long before resignation; just because they stole it within one month of resignation doesn't mean that is when they first started stealing it. Some of them stole slowly over time,

committing their final theft right before resignation. However, fewer than one-third of the insiders continued their theft for more than one month.

One insider planned with a competing organization abroad and transferred documents to the company for almost two years prior to her resignation. However, for the most part, the insiders did steal the information quickly upon resignation.

NOTE

The one-month window includes the month before the insider resigns and the month after he resigns—actually two months in total.

In one case the insider accepted a position with a competing organization, resigned his position, and proceeded to download proprietary information to take with him to the new company before his last day of work. He stole the information despite warnings by his new employer not to bring any proprietary information with him to his new position. When questioned about the theft, the insider admitted to downloading the information, saying that he hoped to use it if he ever started his own business.

In a similar case, the insider accepted a position with a competitor and started downloading documents containing trade secrets the very next day. A few weeks later, after several sessions of high-volume downloading, the insider left the organization and started working for the competitor. Just two days after starting his new job, the insider loaded the stolen files onto his newly assigned laptop, and within a month had emailed the trade secrets to his new coworkers. This exemplifies the lack of any effort to conceal the theft.

A wide variety of technical means were used in the theft cases to transfer information, including email, phone, fax, downloading to or from home over the Internet, malicious code collection and transmission, and printing out material on the organizations' printers. One particularly vengeful insider acted in anger when his employer rewarded executives with exorbitant bonuses while lower-level employees were receiving meager raises or being laid off. He began downloading confidential corporate documents to his home computer, carrying physical copies out of the offices, and emailing them to two competitors. Neither of the two competitors wanted the confidential information and both sent the information they

received back to the victim organization. This insider also made no attempt to conceal or deny his illicit activity.

We will explore the technical details of the theft of IP cases later in this chapter, following the Ambitious Leader model.

What Can You Do?

Our case data suggests that monitoring of online actions, particularly downloads within one month before and after resignation, could be particularly beneficial for preventing or detecting the theft of proprietary information. You need to consider the wide variety of ways that information is stolen and design your detection strategy accordingly. **Data leakage tools**[12] may help with this task. Many tools are available that enable you to perform functions such as the following:

- Alerting administrators to emails with unusually large attachments
- Tagging documents that should not be permitted to leave the network
- Tracking or preventing printing, copying, or downloading of certain information, such as PII or documents containing certain words such as new-product codenames
- Tracking of all documents copied to removable media
- Preventing or detecting emails to competitors, to governments and organizations outside the United States, to Gmail or Hotmail accounts, and so on

You might also consider a simple mechanism to protect yourself from being the unknowing recipient of stolen IP from another organization. As part of your IP agreement that you make new employees sign, you might want to include a statement attesting to the fact that they have not brought any IP from any previous employer with them to your organization. We are heartened by the fact that many of the theft of IP cases in our database were detected by the new employer, and reported to the victim organization and/or law enforcement. You should be sure that you have a process defined for how you would respond to that twist of insider threat. In addition, you may consider asking departing employees to sign a new

12. **Data leakage tools:** systems designed to detect and prevent unauthorized use and transmission of confidential information (Wikipedia). Also commonly called **data loss prevention (DLP) systems.**

IP agreement, reminding them of the contents of the IP agreement while they are walking out the door.

The Ambitious Leader

This section describes the Ambitious Leader model. These cases involve a leader who recruits insiders to steal information with him—essentially a "spy ring." Unlike the Entitled Independent, these insiders don't only want the assets they created or have access to, they want more: an entire product line or an entire software system. They don't have the access to steal all that they want themselves, so they recruit others into their scheme to help.

We omitted the What Can You Do? section from most of the Ambitious Leader scenarios because it is so similar to the Entitled Independent model. But we provide extensive advice at the end of the chapter when we explore the technical details in all of the cases.

More than half of the Ambitious Leaders planned to develop a competing product or use the information to attract clients away from the victim organization. Others (38%) worked with a new employer that was a competitor. Only 10% actually sold the information to a competing organization.

About one-third of our theft of IP cases were for the benefit of a foreign government or organization. The average financial impact for these cases was more than four times that of domestic IP theft. In these cases, loyalty to the insider's native country trumped loyalty to the employer. Insiders with an affinity toward a foreign country were motivated by the goal of bringing value to, and sometimes eventually relocating in, that country.

In general, the cases involving a foreign government or organization fit the Ambitious Leader model. However, because the consequences of these crimes are much more severe, and both government and private organizations are so concerned about this threat, we have included a separate section at the end of the Ambitious Leader model that analyzes those crimes in a bit more depth.

About one-third of our theft of IP cases were for the benefit of a foreign government or organization. The average financial impact for these cases was more than four times that of domestic IP theft.

The rest of this section describes additional aspects of the Ambitious Leader model not exhibited by Entitled Independents. These cases are more complex than the Entitled Independent cases, involving more intricate planning, deceptive attempts to gain increased access, and recruitment of other employees into the leader's scheme.

The motivation for the Ambitious Leader is slightly different from that of the Entitled Independent. There was little evidence of employee dissatisfaction in the Ambitious Leaders. Insiders in this scenario were motivated not by dissatisfaction, but rather by an Ambitious Leader promising them greater rewards.

In one case, the head of the public finance department of a securities firm organized his employees to collect documents to take to a competitor. Over one weekend he then sent a resignation letter for himself and each recruit to the head of the sales department. The entire group of employees started work with the competitor the following week.

In another case, an outsider who was operating a fictitious company recruited an employee looking for a new job to send him reams of his current employer's proprietary information by email, postal service, and a commercial carrier.

Except for the dissatisfaction of the Entitled Independent, the initial patterns for Ambitious Leaders are very similar. In fact, the beginning of the Ambitious Leader model is merely the Entitled Independent model without the "organization denial of insider request" and "insider dissatisfaction." Most Ambitious Leaders stole the information that they worked on, just like the Entitled Independents. The difference is that they were not content only to steal the information they had access to; they wanted the entire system, program, or product line, and needed a more complex scheme to get it.

Theft took place even though IP agreements were in place for almost half (48%) of the Ambitious Leader cases. In at least one case, the insider lied when specifically asked if he had returned all proprietary information and software to the company as stipulated in the IP agreement he had signed. He later used the stolen software to develop and market a competing product in a foreign country.

Insider Planning of Theft

The Ambitious Leader cases involved a significantly greater amount of planning than the Entitled Independent cases, particularly the recruitment

of other insiders. Other forms of planning involved creating a new business in almost half of the cases, coordinating with a competing organization in almost half of the cases, and collecting information in advance of the theft.

This aspect of the insider behavior is reflected in Figure 3-6, which describes the Ambitious Leader formulating plans to steal the information prior to the actual theft. This extensive planning is an additional potential point of exposure of the impending theft, and therefore results in measures by the insider to hide his actions. In most of the Ambitious Leader cases, the insider was planning the theft a month or more before his departure from the organization.

The one-month window surrounding resignation holds for most Ambitious Leaders just as it does for Entitled Independents.

Increasing Access

In more than half of the Ambitious Leader cases, the lead insider had authorization for only part of the information targeted and had to take steps to gain additional access. In one case involving the transfer of proprietary documents to a foreign company, the lead insider asked her supervisor to assign her to a special project that would increase her access to highly sensitive information. She did this just weeks prior to leaving the country with a company laptop and numerous company documents, both physical and electronic.

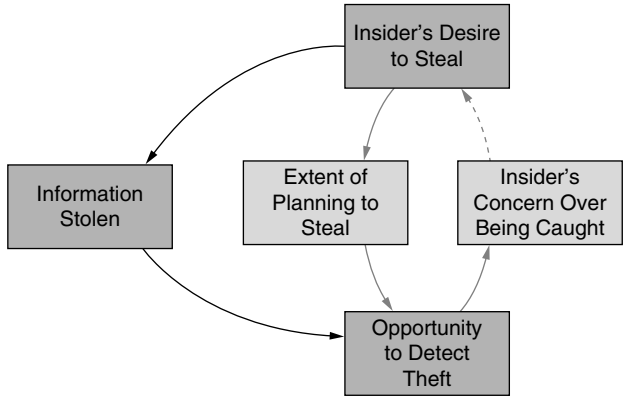


Figure 3-6 *Theft planning by Ambitious Leader*

As shown in Figure 3-7, the recruitment of additional insiders is the primary means Ambitious Leaders use to gain access to more information. The need for recruitment increases the amount of planning activity necessary to coordinate insider activities.

Organization's Discovery of Theft

There are many more avenues for you to detect heightened risk of insider theft of IP in Ambitious Leader cases than in Entitled Independent cases. Entitled Independents are often fully authorized to access the information they steal, and do so very close to resignation with very little planning. In addition, Entitled Independents rarely act as if what they are doing is wrong, probably because they feel a proprietary attachment to the information or product. Ambitious Leaders, on the other hand, often have to gain access to information for which they are not authorized. This involves, in part, coordinating the activities of other insiders and committing deception to cover up the extensive planning required.

What Can You Do?

Figure 3-8 illustrates the avenues available for you to continually assess the risk you face regarding theft of IP. Because deception is such a prominent factor in Ambitious Leader cases, its discovery may be a better means to detect heightened insider risk here than in Entitled Independent cases.

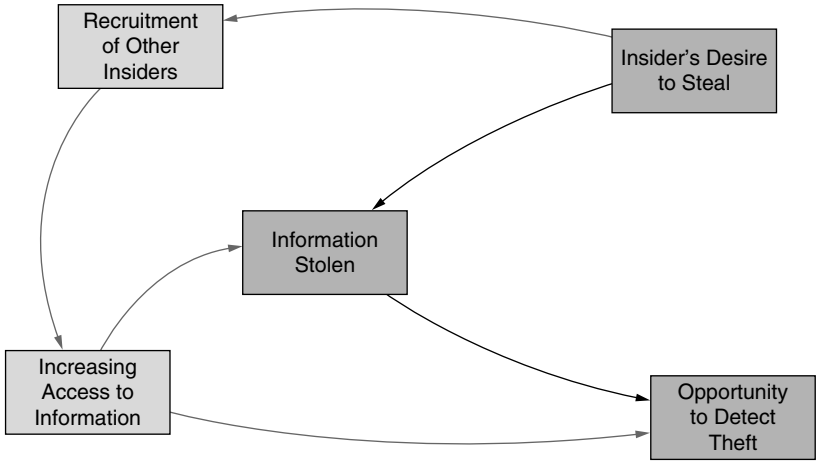


Figure 3-7 *Increasing access by the Ambitious Leader*

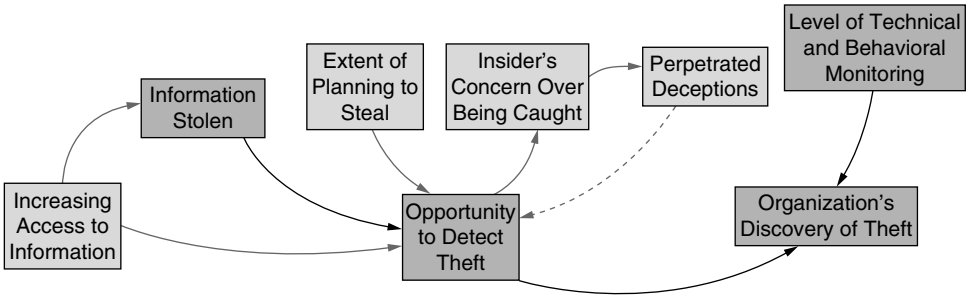


Figure 3-8 *Organization's discovery of theft of IP in Ambitious Leader cases*

In some of the cases we reviewed, the organization only found out about the theft when the insider took his competing product to market or solicited business from his previous employer's customers. While this detection is later than one would prefer, it is still not too late to take action and prevent further losses. However, we strongly suggest that you consider the countermeasures at the end of this chapter to facilitate earlier detection. Many of the incidents in our database were detected by nontechnical means, such as the following:

- Notification by a customer or other informant
- Detection by law enforcement investigating the reports of the theft
- By victims
- Reporting of suspicious activity by coworkers
- Sudden emergence of new competing organizations

You can use technical monitoring systems to detect insider theft of IP. More than one-half of the Entitled Independents and almost two-thirds of the Ambitious Leaders stole information within one month of resignation. Many of these involved large downloads of information outside the patterns of normal behavior by those employees. In more than one-quarter of the Ambitious Leader cases, an insider emailed or otherwise electronically transmitted information or plans from an organizational computer.

Keeping track of backups of critical information is also important—in one case an insider took the backup media from his computer on his last day of work. Understanding the potential relevance of these types of precursors

provides a window of opportunity for you to detect theft prior to employee termination.

Of course, the earlier you can become aware of illicit plans the better. Early awareness depends on behavioral as well as technical monitoring and is more likely to catch incidents involving Ambitious Leaders than Entitled Independents. In Ambitious Leader scenarios, you need to look for evolving plans and collusion by insiders to steal information, including attempts to gain access to information over and above that for which an employee is authorized. There were behavioral or technical precursors to the crime in all of the Ambitious Leader cases.

One insider, over a period of several years, exhibited suspicious patterns of foreign travel and remote access to organizational systems while claiming medical sick leave. It is not always this blatant, but signs are often observable if you are vigilant.

Theft of IP inside the United States Involving Foreign Governments or Organizations

This section focuses on cases of malicious insiders who misused a company's systems, data, or network to steal intellectual property from an organization inside the United States for the benefit of a foreign entity—either an existing foreign organization or a new company that the insiders established in a foreign country.[13] These cases fit the problem described in the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07* prepared by the Office of the National Counterintelligence Executive.

> The United States remains the prime target for foreign economic collection and industrial espionage as a result of its worldwide technological and business leadership. Indeed, strong US international competitiveness underlies the continuing drive by foreign collectors to target US information and technology.[14]

13. Material in this section includes portions from a previously published work. Specifically, a joint CyLab and CERT Program article was published as "Spotlight On: Insider Theft of Intellectual Property inside the U.S. Involving Foreign Governments or Organizations" by Derrick Spooner, Dawn Cappelli, Andrew Moore, and Randy Trzeciak [Spooner 2008].

14. See www.ncix.gov/publications/reports/fecie_all/fecie_2007/FECIE_2007.pdf.

These cases also include activities defined by the Office of the National Counterintelligence Executive as economic espionage or industrial espionage.

> ***Economic Espionage***—*the conscious and willful misappropriation of trade secrets with the knowledge or intent that the offense will benefit a foreign government, foreign instrumentality, or foreign agent.*[15]
>
> ***Industrial Espionage***—*the conscious and willful misappropriation of trade secrets related to, or included in, a product that is produced for, or placed in, interstate or foreign commerce to the economic benefit of anyone other than the owner, with the knowledge or intent that the offense will injure the owner of that trade secret.*[16]

NOTE

We have not included any cases of national security espionage in this book.

Cases that involve foreign beneficiaries can differ from other theft of IP cases because the insiders may have a sense of duty or loyalty to their countries of origin that overrides any loyalty to their employer. Moreover, some of these cases suggest that some foreign entities appear to be interested in recruiting insiders to steal IP to advance businesses in that particular country. Competing loyalties, coupled with recruitment of employees in U.S. businesses by foreign nations or organizations, make this type of crime a potent threat for organizations that rely on IP for competitive advantage.

There are several reasons for heightened concern about this kind of crime. The impact of a crime that extends outside the jurisdiction of U.S. law enforcement on an organization can be substantially greater than a case that remains within U.S. jurisdiction. Insiders who leave the United States may be difficult or impossible to locate and arrest. And even if the insider were located and arrested, extradition to the United States would be required. Therefore, there can be more risk from an employee who intends to leave the United States following the theft than from employees contemplating criminal acts against their employer who remain in the United States.

15. Ibid.

16. Ibid.

In addition, it can be very difficult to recover stolen IP once it leaves the United States. In cases within U.S. borders, companies that receive the stolen IP can suffer similar consequences under the same laws as the insiders if they use the stolen IP for their own advantage. Thus, domestic organizations are under greater obligation to cooperate with authorities and return all stolen IP than foreign organizations might be.

Who They Are

The majority of the insiders worked as either a scientist or an engineer. Males committed most of the incidents. Of the cases that identify citizenship, about half were foreign nationals, about 40% were naturalized U.S. citizens, two were U.S. citizens, and the rest were resident aliens or had dual citizenship.

The insiders' countries of origin, for cases in which the information was available, are shown in Table 3-1.

About one-fourth of the cases involved at least one accomplice who was also an insider. Some of those involved multiple insiders; one case involved 14 insiders in all! Almost 40% had at least one external accomplice.

Table 3-1 *Countries of Origin (When Known)*

Country	Number of Cases
China	13
United States	2
Taiwan	2
Canada (naturalized citizen from China)	2
South Korea	1
Germany	1
Russia	1
Iran	1
Ecuador	1
India	1
Dual citizenship, China and United States	1

Note that when multiple insiders are involved in a case we only code it as a single case, and code details for the primary insider. Additional information about conspirators is also coded for the case. If you are interested in a detailed description of the information coded for each case, please see Appendix D, Insider Threat Database Structure.

What They Stole

All of these insiders stole intellectual property in digital form, physical form, or both. The methods used were consistent with those described elsewhere in this chapter.

Table 3-2 contains the details known for these cases. Damage amounts are supplied when they were available. We only used the term *trade secrets* when that term was used in the case file; otherwise, we used the description supplied in the case file.

Table 3-2 *Breakdown of Cases*

Sector	Number of Cases	Damages[17]	What Was Stolen
Information and telecommunications	11	1 case, $1 billion	Trade secrets (4 cases)
		1 case, $600 million	Source code (3 cases)
		1 case, $1 million	Confidential product information (3 cases)
		1 case, $100,000	
		1 case, $5,000	Confidential manufacturing information (1 case)
		6 cases, Unknown	Proprietary documents and source code (1 case)

17. In the majority of the cases, damages reported were in the form of potential loss to the organization as reported in court documents.

Chemical industry and hazardous materials	7	1 case, $400 million 1 case, $100 million 1 case, $50 million to $60 million 4 cases, Unknown	Trade secrets (5 cases) Sensitive product information (1 case) Confidential documents (1 case)
Manufacturing	3	1 case, $40 million 1 case, $32 million	Trade secrets (2 cases) Confidential documents (1 case)
Banking and finance	1	$5,000	Source code
Commercial facilities	1	Unknown	Trade secrets
Defense industrial base	1	Unknown	Source code
Education	1	$3 million	Patentable proprietary information
Energy	1	Unknown	Sensitive software
Government–Federal	1	Unknown	Government restricted information
Public health	1	$500 million	Trade secrets
Water	1	$1 million	Trade secrets and source code

Why They Stole

The specific motives fall into several categories.

- **To form a new competing business:** One-third of the insiders stole the IP to establish a new business venture in a foreign country that would compete with their current employer. In all of these cases, the insiders had at least one accomplice who assisted them with their theft, with forming and/or running the new business, or with both. All but one of these insiders had already started their business before they left the victim organization; in fact, some of them had already established the business and had made money for quite some time.
- **To take to a new employer in a competing business:** More than 40% of these insiders stole IP to take to their new employers, businesses located outside the United States that competed with their current employer. In all but two of these cases, the insiders had already accepted jobs with the competitors before leaving the victim organization.
- **To take to their home country:** In three of the cases, this was the somewhat vague reason they gave for their theft. In another case, the insider stated he wanted to "benefit the homeland."
- **To sell to a competitor:** In two cases, the insider stole the information to sell to a competitor in another country outside the United States.

Mitigation strategies for these cases are the same as for any other cases of insider theft of intellectual property, which is covered in the next section.

Mitigation Strategies for All Theft of Intellectual Property Cases

The intent of the MERIT models is to identify the common patterns of each type of insider threat over time based on our analysis of the cases in our database. We have found that the models suggest key mitigation strategies for you to defend yourself against these types of threats. We therefore propose countermeasures based on expert opinions in behavioral psychology, organizational management, and information security.

Your insider threat mitigation strategies should involve more than technical controls. An overall solution should include policies, business processes, and technical solutions that are endorsed by senior leadership in HR,

legal, data owners, physical security, information security/information technology, and other relevant areas of the organization. It is critical that all levels of management recognize and acknowledge the threat posed by their current and former employees, contractors, and business partners, and take appropriate steps to mitigate the associated risk. It may not be realistic to expect that all intellectual property exfiltrated by insiders will be stopped before the information leaves your network, but it is realistic to expect that you can implement countermeasures into your infrastructure and business processes to allow you to detect as many incidents as possible, thereby minimizing the financial impact on your organization.

> An overall solution should include policies, business processes, and technical solutions that are endorsed by senior leadership in HR, legal, data owners, physical security, information security/information technology, and other relevant areas of the organization.

The remainder of this chapter describes potential countermeasures that we believe could be effective in mitigating insider theft of intellectual property.

Exfiltration Methods

We begin this section by providing more in-depth details of the technical methods used by insiders to steal IP in our database. Methods varied widely, but the top three methods used were email from work, removable media, and remote network access. Table 3-3 describes the primary methods of exfiltration.

Table 3-3 *Exfiltration Methods*

Exfiltration Method	Description
Email	Insiders exfiltrated information through their work email account. The email may have been sent to a personal email account or directly to a competitor or foreign government or organization. Insiders used email attachments or the body of the email to transmit the sensitive information out of the network.

Continues

Table 3-3 *Exfiltration Methods (Continued)*

Exfiltration Method	Description
Removable media	Common removable media types were USB devices, CDs, and removable hard drives.
Printed documents	Insiders printed documents or screenshots of sensitive information, and then physically removed the hard copies from the organization.
Remote network access	Insiders remotely accessed the network through a virtual private network (VPN) or other remote channel to download sensitive information from an off-site location.
File transfer	The insider was at work, on the company network, and transferred a file outside of the network using the Web, **File Transfer Protocol (FTP),**[18] or other methods. Although email could potentially fit this category, we thought that email should be considered separately due to the large number of crimes that used email.
Laptops	Insiders exfiltrated data by downloading IP onto a laptop at work and bringing it outside the workplace. For example, one insider was developing an application for his company on a laptop and later purposely leaked the source code. In other cases the insiders simply downloaded sensitive files onto their laptops for personal or business use later.

We dug a little deeper into those methods to determine where our mitigation strategies need to be focused—on the host, the network, or the physical removal of information—and found that more than half involved the network, 42% involved the host, and only 6% involved physical removal.

Network Data Exfiltration

Data exfiltration over the network was the most common method of removing information from an organization, used by more than half of

18. **File Transfer Protocol (FTP):** a communication standard used to transfer files from one host to another over a network, such as the Internet (Wikipedia).

the insiders in the database who stole IP. Removal methods included in this category were email, a remote network access channel (originating externally), and network file transfer (originating outside the network).

About one-fourth of the insiders used their work email account to send the IP outside the network, either sending IP to their personal email account, or directly emailing the IP to a competitor or foreign government or organization.

About one-fourth of the insiders used their work email account to send the IP outside the network.

For example, an insider in one case sent customer lists and source code he had written from his work email account to his personal email account. During this time, he was being recruited by a competing organization. He accepted the competitor's offer and took the customer lists and source code to his new job to help him get a head start there.

In another case, an insider asked his superiors for confidential data about their product costs and materials. Two months later, he accepted a new job with a competitor. The original employer warned him against taking or distributing any of its proprietary information. However, the insider emailed internal business information from his work email account to two of his new supervisors before he started at the new company.

Interestingly, almost half of the cases involving email exfiltration also involved another type of exfiltration. This suggests that if you suspect an insider is stealing information you should check other communication channels for similar activity. Most frequently, the additional exfiltration path involved stealing information on a laptop, but use of remote access channels and theft of printed documents each happened a few times in combination with theft via email.

The second most frequent network exfiltration method was remote network access. As in the MERIT model, many of these cases occurred immediately before resignation or shortly after acceptance of a new job at a competitor. In more than one-third of these cases, the remote connections were established after normal work hours; in almost one-third of the cases, the time of exfiltration was unknown.

During the remote sessions, insiders downloaded sensitive documents to their remote computers. In one case, an insider and a coworker were

employed as contract software developers for the victim organization. Their contracts were periodically renewed when modifications to the software were needed. Each time their contracts ended, the victim organization neglected to disable their remote access to the network since the organization knew they would be contracted again in the near future. However, at one point both insiders suddenly claimed that the programs they developed belonged to them, and requested that the organization cease using them. The company continued to use the applications, and the insider and accomplice were able to remotely access and download the proprietary source code they claimed to own.

The least common method of network data exfiltration was transferring data outside the network through outbound channels such as FTP, the Web, or instant messaging. These crimes were all perpetrated by more technically skilled insiders. Examples include the following.

- A computer programmer at an investment banking organization submitted his letter of resignation to his manager. He then used a script that copied, compressed, and merged files containing source code, and then encrypted, renamed, and uploaded the files using FTP to an external file hosting server.
- An insider transferred trade secrets and source code to a password-protected Web site using standard HTTP. The insider intended to start a side business with the company's stolen IP.
- An insider who failed to receive a raise and whose request for transfer was rejected submitted his resignation and downloaded proprietary information from his organization for potential use in a new job. He used FTP to transfer the data to his home computer.

What Can You Do?

Most cases that involved use of the network to perpetrate the theft involved email and remote access over VPN. Given that several cases involved email to a direct competitor, you should consider at least tracking, if not blocking, email to and from competing organizations. Our cases did not explicitly show sophisticated concealment methods, such as use of **proxies**[19] or extensive use of personal, Web-based email services. However, we did find that insiders periodically leverage their personal, Web-based email as an

19. **Proxies:** A proxy server, more commonly known as a proxy, is a server that routes network traffic through itself, thereby masking the origins of the network traffic.

exfiltration method. You should carefully consider the balance between security and personal use of email and Web services from your network.

As mentioned, most insiders steal IP within 30 days of leaving an organization. You should consider a more targeted monitoring strategy for employees and contractors when they give notice of their exit. For instance, check your email logs for emails they sent to competitors or foreign governments or organizations. Also check for large email attachments they sent to Gmail, Hotmail, and similar email accounts.

Further, you should consider inspecting available log traffic for any indicators of suspicious access, large file transfers, suspicious email traffic, after-hours access, or use of removable media by resigning employees. Central logging appliances and **event correlation**[20] engines may help craft automated queries that reduce an analyst's workload for routinely inspecting this data.

Host Data Exfiltration

Host-based exfiltration was the second most common method of removing IP from organizations; close to half of the cases involved an insider removing data from a host computer and leaving the organization with it. In these cases, insiders often used their laptops to remove data from the organization. We had difficulty determining the exact ownership and authorization of the laptops used. However, we do know that about one-sixth of the insiders who stole IP used laptops taken from the organization's site during normal work hours. Half of them transferred proprietary software and source code; the other half removed sensitive documents from the organization.

In one case, the insider worked for a consulting company and stole proprietary software programs from a customer by downloading them to a laptop. He attempted to disguise the theft by deleting references to the victim organization contained in the program, and then attempted to sell portions of the program to a third party for a large sum of money.

Another case involved an insider who accessed and downloaded trade secrets to his laptop after he accepted an offer from a foreign competitor. He gave his employer two weeks' notice, and continued to steal information until he left.

20. **Event correlation:** a technique for making sense of a large number of events and pinpointing the few events that are really important in that mass of information (Wikipedia).

By far, the most common method of host-based exfiltration in the database was removable media; 80% of these cases involved trade secrets, and the majority of those insiders took the stolen trade secrets to a competitor. The type of removable media used varied. Where information was available, we determined that insiders most often used writable CDs. Thumb drives and external hard disks were used in just 30% of the cases. However, the type of removable media used has changed over time. Insiders primarily used CDs prior to 2005. Since 2005, however, most insiders using removable media to steal IP use thumb drives and external hard drives. This trend indicates that changes in technology are providing new and easier methods of stealing data from host computers.

In one case, an insider resigned from his organization after accepting a position at another organization. He downloaded personal files as well as the organization's proprietary information onto CDs. Despite signing a nondisclosure agreement, the insider took the trade secrets to a competitor.

In a similar example, an insider received an offer from a competitor three months prior to resignation. He lied about his new position and employment status to coworkers. Only days before leaving the organization, he convinced a coworker to download his files to an external hard drive, supposedly to free up disk space. He came into work at unusual hours to download additional proprietary information onto a CD. Finally, he took this information with him to his new position at a competing organization.

What Can You Do?

It is unlikely that the victim organizations in our database prohibited removable media in their daily computing environments. You should consider carefully who in your organization really needs to use removable media. Perhaps access to removable media is a privilege granted only to users in certain roles. Along with that privilege could come enhanced monitoring of all files copied onto such devices. In addition, understanding who requires removable media and for what purposes can help you to determine what may constitute normal and healthy business use, and to monitor for usage patterns that deviate from that. Inventory control, as it pertains to removable media, may also be helpful. For example, you could allow use of removable media only on company-owned devices prohibited from leaving your facility. Organizations requiring the highest-assurance environment should consider disallowing removable media completely, or allowing it only in special situations that are carefully audited.

Finally, recall the 30-day window in our theft of IP cases. Can you log all file transfers to removable media? You might not have the resources to review all of those logs (depending on how restricted your use of such media is). However, if the logs exist, you can audit them immediately on the hosts accessed by any employee who has announced his resignation. This would provide one quick mechanism for detecting IP that might be exfiltrated by an employee on his way out the door.

Physical Exfiltration

Only 6% of the theft of IP cases involved some sort of physical exfiltration. We found that physical exfiltration usually occurs in conjunction with some other form of exfiltration that would have produced a more obvious network or host-based observable event.

Exfiltration of Specific Types of IP

Once we determined what kinds of IP were stolen and how, we determined what methods of exfiltration were associated with the different types of IP. Several interesting findings surfaced. In particular, business plans were stolen almost exclusively through network methods, particularly using remote access. Conversely, proprietary software and source code involve a much higher use of non-network methods. This may be due in part to the volume of data associated with different asset types. Software and source code files are often large, but business plans are usually smaller documents that are easier to move over a VPN or as an email attachment. Enumerating the most frequent methods by which particular assets are exfiltrated may help steer monitoring strategies with respect to computers that house particular types of assets or are allowed to access given assets over the network.

Concealment

Some insiders attempted to conceal their theft of IP through various actions. These cases signify a clear intent to operate covertly, implying the insiders may have known their actions were wrong. In one case, an insider was arrested by federal authorities after stealing product design documents and transferring them to a foreign company where he was to be employed. After being arrested, he asked a friend to log in to his personal email account, which was used in the exfiltration, and delete hundreds of emails related to the incident.

Another case involved an insider who used an encryption suite to mask the data he had stolen when moving it off the network.

Trusted Business Partners

Trusted business partners accounted for only 16% of our theft of IP cases, but this is still a complicated insider threat that you need to consider in your contracting vehicles and technical security strategies.

For example, a telecommunications company was involved in a lawsuit, and had to hand over all of its applicable proprietary information to its attorneys, which it did in hard-copy form. The law firm subcontracted with a document imaging company to make copies of all of the information. One of the employees of the document imaging company asked his nephew, a student, if he would like to make a little extra spending money by helping him make the copies at the law firm. The nephew realized that he had access to proprietary access control technology that the telecommunications company used to restrict its services based on fees paid by each individual customer. He felt, like many others, that the company unfairly overcharged for these services, so he posted the information online to the Internet underground. This basically released the telecommunications company's "secret sauce," and now it was easy for members of that community to obtain free services. When the post was discovered, law enforcement investigated the source of the post and traced the activity back to the student.

It is important that you consider these types of threats when drawing up contracts with your business partners. Could that scenario happen to you? Do you write legal language into your contracts that dictates how your confidential and proprietary information can and cannot be handled?

It is important that you understand the policies and procedures of your trusted business partners. You establish policies and procedures in order to protect your information. When you enlist the support of a trusted business partner, you should ensure that their policies and procedures are at least as effective as your safeguards. This includes physical security, staff education, personnel background checks, security procedures, termination, and other safeguards.

In addition, you should monitor intellectual property to which access is provided. When you establish an agreement with a trusted business partner, you need assurance that IP you provide access to is protected. You need to get assurances that access to and distribution of this data will be monitored. You should verify that there are mechanisms for logging the dissemination of data, and review their procedures for investigating possible disclosure of your information.

These are just a few recommendations. We detail eight recommendations in Chapter 9, Conclusion and Miscellaneous Issues, regarding trusted business partners.

Mitigation Strategies: Final Thoughts

We devoted a good deal of this chapter to technical countermeasures. Figure 3-9 depicts organizational issues of concern in the theft of intellectual property cases in our database. We addressed the technical issues in the previous section, but there are nontechnical issues worth noting as well. For instance, notice that the most prevalent issue of concern is an employee who went to work for a competitor. Therefore, you might want

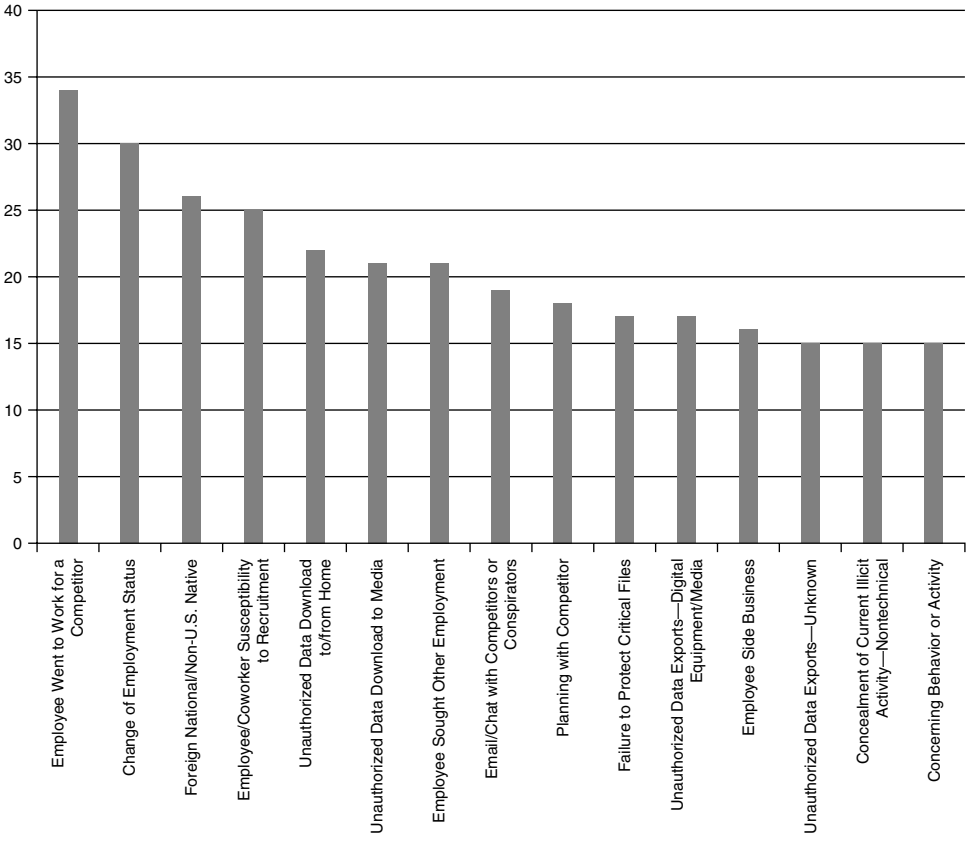


Figure 3-9 *Issues of concern*

to monitor emails going to a competitor. We provide a control for doing that in Chapter 7, Technical Insider Threat Controls. Also, note the second most prevalent issue of concern: change in employment status, which would account for the insiders who stole information within 30 days of resignation. The third most prevalent issue is foreign national/non-U.S. native, which we covered in depth in the section Theft of IP inside the United States Involving Foreign Governments or Organizations earlier in this chapter. The fourth issue, employee/coworker susceptibility to recruitment, applies in all of the Ambitious Leader cases.

One final thought regarding the 30-day window: You should review your access-termination procedures associated with employee and contractor exit procedures. Several cases provided evidence that insiders remotely accessed systems by using previously authorized accounts that were not disabled upon the employee's exit. Precautions against this kind of incident seem to be common sense, but this trend continues to manifest in newly cataloged cases.

NOTE

For more details of technical controls you can implement to prevent or detect insider theft of IP, see Chapter 7, where we describe new technical controls from our insider threat lab.

Summary

Insiders who steal intellectual property are usually scientists, engineers, salespeople, or programmers. The IP stolen includes trade secrets, proprietary information such as scientific formulas, engineering drawings, source code, and customer information. These insiders typically steal information that they have access to, and helped to create. They rarely steal it for financial gain, but rather they take it with them as they leave the organization to take to a new job, give to a foreign government or organization, or start their own business.

These insider threats fall into two groups. The first is the Entitled Independent, an insider who acts alone to take the information with him as he leaves the organization. The second is the Ambitious Leader, an insider who creates a "ring" of insiders who work together to steal the information. Ambitious Leaders want to steal more than just the information they created—they want the entire product line, or whole suite of source code, for example.

A portion of this chapter was devoted to insiders who stole IP to take to a foreign government or organization. These crimes can be particularly disastrous, since it is much more difficult to recover the information once it leaves the United States. We described the countries involved, the positions of the employees, and the methods of theft.

The most useful pattern we found in modeling these crimes was that most of the insiders stole at least some of the information within 30 days of resignation. That time frame actually encompasses a 60-day window: 30 days before turning in their resignation, and 30 days after. Our mitigation strategies use that time frame; we recommend logging of all potential exfiltration methods, especially emails off of the network and use of removable media, so that you can audit the information when an employee who has access to your critical information resigns. You need to be able to go backward in time when such an employee resigns to make sure he has not emailed your IP outside the network—for example, to competitors, to governments or organizations outside the United States, or to Gmail or Hotmail accounts. You also need to be able to identify information that was copied to removable media during that time frame. Finally, you need to do real-time alerting when such online activity takes place in that period between when the insider resigns and when his employment actually terminates.

The next chapter turns to insider fraud. Insider fraud involves theft as well, but theft of a different type of information: Personally Identifiable Information (PII), credit card information, and other data that could be used to commit fraud. It also includes crimes in which an insider modified information for financial gain, often for pay by outsiders.

This page intentionally left blank

This page intentionally left blank

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X