

# Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector

Adam Cummings  
Todd Lewellen  
David McIntire  
Andrew P. Moore  
Randall Trzeciak

**July 2012**

**SPECIAL REPORT**  
CMU/SEI-2012-SR-004

**CERT Program**  
<http://www.sei.cmu.edu>



Copyright 2012 Carnegie Mellon University.

This material is based upon work funded and supported by the United States Department of Homeland Security Science and Technology Directorate under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Homeland Security or the United States Department of Defense.

This report was prepared for the

Contracting Officer  
ESC/CAA  
20 Shilling Circle  
Building 1305, 3rd Floor  
Hanscom AFB, MA 01731-2125

#### NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use:\* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:\* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

CERT<sup>®</sup> is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

---

# Table of Contents

|  |            |
|--|------------|
| <b>Foreword</b>  | <b>v</b>   |
| <b>Acknowledgments</b>   | <b>vi</b>  |
| <b>Executive Summary</b>   | <b>vii</b> |
| <b>Abstract</b>  | <b>xi</b>  |
| <b>1 Introduction</b>  | <b>1</b>   |
| 1.1 Terms and Definitions  | 1          |
| 1.2 Related Empirical Research   | 2          |
| 1.2.1 Surveys  | 2          |
| 1.2.2 Simulations  | 3          |
| 1.2.3 Case Studies and Other Empirical Research  | 3          |
| 1.3 Theory Related to the Insider Threat   | 5          |
| <b>2 Research Method</b>   | <b>6</b>   |
| 2.1 Case Identification and Selection  | 6          |
| 2.2 Coding Method and Database Description   | 7          |
| 2.3 Modeling and Analysis Approach   | 8          |
| <b>3 Crime Profile and Findings</b>  | <b>9</b>   |
| 3.1 Subject and Crime Description  | 9          |
| 3.2 FINDING ONE: Criminals who executed a “low and slow” approach accomplished more damage and escaped detection for longer. | 12         |
| 3.2.1 Description  | 12         |
| Case Example #1  | 15         |
| 3.2.2 Conclusions / Recommendations  | 15         |
| 3.3 FINDING TWO: Insiders’ means were not very technically sophisticated.  | 16         |
| 3.3.1 Description  | 16         |
| Case Example #2  | 18         |
| Case Example #3  | 19         |
| 3.3.2 Conclusions / Recommendations  | 19         |
| 3.4 FINDING THREE: Fraud by managers differs substantially from fraud by non-managers by damage and duration.                | 20         |
| 3.4.1 Description  | 20         |
| Case Example #4  | 22         |
| Case Example #5  | 22         |
| 3.4.2 Conclusions / Recommendations  | 22         |
| 3.5 FINDING FOUR: Most cases do not involve collusion.   | 23         |
| 3.5.1 Description  | 24         |
| Case Example #6  | 25         |
| 3.5.2 Conclusions / Recommendations  | 25         |
| 3.6 FINDING FIVE: Most incidents were detected through an audit, customer complaints, or co-worker suspicions.               | 25         |
| 3.6.1 Description  | 26         |
| Case Example #7  | 27         |
| 3.6.2 Conclusions / Recommendations  | 27         |
| 3.7 FINDING SIX—Personally identifiable information (PII) is a prominent target of those committing fraud.                   | 27         |
| 3.7.1 Description  | 28         |

|  |           |
|--|-----------|
| Case Example #8  | 31        |
| 3.7.2 Conclusions / Recommendations                                      | 31        |
| <b>4 Fraud Dynamics</b>  | <b>32</b> |
| 4.1 System Dynamics  | 32        |
| 4.2 Fraud Triangle   | 33        |
| 4.3 Manager Model  | 35        |
| 4.4 Non-Manager Model  | 38        |
| <b>5 Strategies for Prevention, Detection, and Response</b>              | <b>41</b> |
| 5.1 Behavioral and Business Process Recommendations                      | 43        |
| 5.2 Monitoring and Technical Recommendations                             | 44        |
| <b>6 Conclusion and Next Steps</b>                                       | <b>46</b> |
| 6.1 Considerations for Insider Threat Program Implementation             | 46        |
| 6.2 Identify Technical Gaps  | 47        |
| 6.3 Conclusion   | 48        |
| 6.4 Next Steps   | 48        |
| <b>Appendix A: The Insider Threat Center at CERT</b>                     | <b>49</b> |
| <b>Appendix B: The Structure of the CERT Insider Threat Database</b>     | <b>51</b> |
| <b>Appendix C: Other Insider Threat Concerns in the Financial Sector</b> | <b>54</b> |
| <b>Bibliography</b>  | <b>58</b> |

---

## List of Figures

|            |   |    |
|------------|---|----|
| Figure 1:  | Number of Insider Fraud Cases by Age                        | 9  |
| Figure 2:  | Average and Median Actual and Potential Damage (in Dollars) | 10 |
| Figure 3:  | Comparison of Damages for Internal and External Cases       | 11 |
| Figure 4:  | Average and Median Sentence Outcomes (in Years)             | 12 |
| Figure 5:  | Average Timeline of a Case (in Months)                      | 13 |
| Figure 6:  | Damages Compared to Crime Duration                          | 14 |
| Figure 7:  | Insider Position Types                                      | 17 |
| Figure 8:  | Actual Damages by Position Type                             | 20 |
| Figure 9:  | Cases by Type of Collusion                                  | 24 |
| Figure 10: | PII and Non-PII Cases by Type of Subject                    | 28 |
| Figure 11: | Average and Median Damage by PII and Non-PII Cases          | 29 |
| Figure 12: | Level of Seniority in Cases Involving PII                   | 30 |
| Figure 13: | System Dynamics Notation                                    | 33 |
| Figure 14: | Fraud Triangle  | 34 |
| Figure 15: | Manager Model   | 36 |
| Figure 16: | Non-Manager Model   | 39 |
| Figure 17: | High-Level Structure of the CERT Insider Threat Database    | 51 |

---

## List of Tables

|          |   |    |
|----------|---|----|
| Table 1: | Comparison of Damage and Crime Duration by Non-managers | 21 |
| Table 2: | Comparison of Crimes by Their Involvement of PII        | 30 |
| Table 3: | Comparison of Fraud by Managers and Non-Managers        | 40 |
| Table 4: | Summary of Recommended Controls                         | 42 |
| Table 5: | Organization Information Collected                      | 52 |
| Table 6: | Subject Information Collected                           | 52 |
| Table 7: | Incident Information Collected                          | 53 |

---

## Foreword

Cyber crimes committed by malicious insiders are among the most significant threats to networked systems and data. When developing policies and procedures for responding to cyber security events, it is important to consider the insider threat.

A malicious insider is a trusted insider who abuses his trust to disrupt operations, corrupt data, exfiltrate sensitive information, or compromise an IT (information technology) system, causing loss or damage. Left unchecked, their rogue actions may compromise the nation's ability to fend off future attacks and safeguard critical infrastructure assets, such as the electric power grid. In fact, some of the most damaging attacks against the government have been launched by trusted insiders. As increased information-sharing exposes sensitive information to more insiders, such attacks will become an increasingly serious threat. Their concerns are shared by the private sector, where corporations maintain valuable, highly sensitive information and financial institutions manage the flow of and access to electronic funds.

The research described in this report was sponsored by the Department of Homeland Security Science and Technology Directorate's Homeland Security Advanced Research Projects Agency Cyber Security Division. The work was conducted, and the report written, by members of the CERT<sup>®</sup> Insider Threat Center at Carnegie Mellon University's Software Engineering Institute. The authors built upon a previous S&T-funded 2004 report, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, to develop a greater understanding of the behavioral, technical, and organizational factors that lead to insider threat attacks [Randazzo 2004]. Drawing on case files provided by the United States Secret Service, they analyzed actual incidents of insider fraud, from inception to prosecution. As part of their effort, the authors compared the technical security controls commonly used to prevent internal and external attackers. Their findings can be used to inform risk management decisions being made by government and industry and to support law enforcement in cybercrime investigations.

I would like to specifically recognize the tremendous participation by the United States Secret Service in this effort. In granting the authors access to case files, the agency was instrumental in the development of this report.

Douglas Maughan, Director  
Cyber Security Division  
Homeland Security Advanced Research Projects Agency  
Science and Technology Directorate  
Department of Homeland Security



---

## Acknowledgments

We wish to thank Dr. Douglas Maughan, Cyber Security Division Director, and Megan Mahle from the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T), who made this study possible through their support and guidance. The United States Secret Service (USSS) provided invaluable and tireless assistance, specifically Deputy Special Agent in Charge Pablo Martinez, Assistant to the Special Agent in Charge Eduardo Cabrera, Special Agent Trae McAbee, and Special Agent Ryan Moore. We also appreciate the many other USSS agents who took time out of their busy schedules to discuss cases with us.

The U.S. Department of the Treasury helped us to identify opportunities to interact with the practitioners and thought leaders about this problem. The U.S. financial services sector opened its doors to us so that we could understand the challenges they face, and this assistance was instrumental to any insight we have provided. In particular, Bill Nelson (President & CEO) of the Financial Services - Information Sharing and Analysis Center (FS-ISAC), Leigh Williams (former President), Paul Smocer (President) and others at BITS, and Heather Wyson (Senior Director, Risk Management Policy) at the American Bankers Association (ABA), formerly with BITS, have offered much appreciated support in various forms.

Many Software Engineering Institute employees contributed to the report in myriad ways, so thank you to Dawn Cappelli, Dr. Eric Shaw, Lynda Pillage, Carly Huth, Derrick Spooner, Paul Ruggiero, and Barbara White. Finally, a sincere thanks is owed to numerous organizations and unnamed individuals from U.S. financial institutions, who provided advice and course corrections about business processes, technical controls, and individual cases.



---

## Executive Summary

This report describes a new insider threat study funded by DHS S&T in collaboration with the USSS and the CERT<sup>®</sup> Insider Threat Center, part of Carnegie Mellon University's Software Engineering Institute. The primary goal of the current research is to produce empirically derived findings from insider and outsider computer criminal activity within the banking and finance sector to help security professionals prevent, detect, and manage malicious insider activity and risk. The central question of this research is

*What are the observable technical and behavioral precursors of insider fraud in the financial sector and what mitigation strategies should be considered as a result?*

For the purposes of the current study, we focus on attacks rather than accidental acts and continue to define a *malicious insider* as

*a current or former employee, contractor, or other 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 [Cappelli 2009]*

Staff of the Insider Threat Center extracted technical and behavioral patterns from 67 insider fraud cases, as well as 13 external<sup>1</sup> fraud cases; all 80 cases occurred between 2005 and the present. Using this information and discussions with staff of other agencies, including the Department of the Treasury, and from some financial organizations, we developed insights and risk indicators of malicious insider activity within the financial services sector.

The majority of the 80 organizations impacted by these crimes are included in the banking and finance industry, including retail, commercial, and investment banks; accounting firms; credit card issuers; federal credit unions; and insurance providers; while some are financial departments of retail businesses (automobile, builders, employee benefit providers, employee staffing, engineering, fashion, home improvement, transportation) and federal, state, and local governments. This information is intended to help private industry, government, and law enforcement more effectively prevent, deter, detect, investigate, and manage insider threat in this sector.

Our research applied the multiple case study method described by Yin [Yin 2009]. USSS cases of insider fraud<sup>2</sup> were selected if they occurred against a U.S. organization, almost exclusively<sup>3</sup> re-

---

® CERT<sup>®</sup> is a registered trademark owned by Carnegie Mellon University.

<sup>1</sup> External fraud cases are those in which no malicious insiders were involved.

<sup>2</sup> USSS case types include criminal violations involving fraud against banks, savings and loan associations, credit unions, check cashers, stockbrokers, and other financial organizations.

<sup>3</sup> Of the 67 insider cases, only 1 did not result in being adjudicated guilty by a U.S. court of law. In that case, investigators found sufficient evidence of the crime to warrant prosecution, but other factors in the case resulted in it being declined for prosecution.

sulted in criminal conviction, and had a sufficient quantity and quality of behavioral and technical information available. A small set of external fraud cases were also studied to facilitate an informal comparison with the insider cases. The exploratory nature of this study and its method of case selection make it challenging to generalize our results to a larger population of insider fraud. Nevertheless, this study does help provide an understanding of the precursors and contextual factors that surround and influence a select sample of insider fraud cases in the financial services sector.

## Findings

The following six broad findings are based on analysis of the 80 cases selected and examined for this report.

**FINDING ONE**—Criminals who executed a “low and slow” approach accomplished more damage and escaped detection for longer.

- On average, over 5 years elapse between a subject’s hiring and the identified start of the fraud, and it takes an average of almost 32 months to be detected by the victim organization.
- The lower 50 percent of cases (under 32 months in length) had an average actual monetary impact of approximately \$382,750, while the upper 50 percent (at or over 32 months in length) had an average actual monetary impact of approximately \$479,000.

**FINDING TWO**—Insiders’ means were not very technically sophisticated.

- Very few subjects served in a technical role (e.g., database administrator) or conducted their fraud by using explicitly technical means.
- In more than half of the cases, the insider used some form of authorized access, whether current or authorized at an earlier time but subsequently withdrawn for any number of reasons, including change in job internally or a change in employer, and in a few of the cases, the insider used some non-technical method to bypass authorized processes.

**FINDING THREE**—Fraud by managers differs substantially from fraud by non-managers by damage and duration.

- Fraud committed by managers consistently caused more actual damage (\$200,105 on average) than fraud committed by non-managers (\$112,188 on average).
- Fraud committed by managers lasted almost twice as long (33 months) as compared to non-managers (18 months).
- Of all the non-managers, accountants cause the most damage from insider fraud (\$472,096 on average) and evade detection for the longest amount of time (41 months).

**FINDING FOUR**—Most cases do not involve collusion.

- Only 16 percent of the fraud incidents involved some type of collusion, with 69 percent of those involving collusion exclusively with outsiders.
- Only 1 case involved collusion with other insiders.

**FINDING FIVE**—Most incidents were detected through an audit, customer complaint, or co-worker suspicion.

- Routine or impromptu auditing was the most common way that an attack was detected (41 percent). In terms of who detected the attack, internal employees were the most common (54 percent) followed by customers (30 percent).
- Only 6 percent of the cases were known to involve the use of software and systems to detect the fraudulent activity.
- Transaction logs, database logs, and access logs were known to be used in the ensuing incident response for only 20 percent of the cases.

**FINDING SIX**—Personally identifiable information (PII) is a prominent target of those committing fraud.

- Roughly one-third (34 percent) of the cases involved PII being the target by the insider or external actor with younger, non-managers stealing PII more often than older employees.
- The average tenure of employees who stole PII was shorter than the tenure of malicious insiders who did not steal PII.

Our modeling and analysis of insider fraud cases revealed two scenarios: the manager scenario (51 percent) and the non-manager scenario (49 percent). In the manager scenario, the perpetrators of fraud are able to alter business processes, sometimes by manipulating subordinate employees, to profit financially. In the non-manager scenario, the perpetrators are often customer service representatives who alter accounts or steal customer account information or other PII to defraud the organization. These two scenarios share many patterns, but each has key distinguishing characteristics regarding timeline, incentives, the organization's trust in the insider, others' suspicions, outsider facilitation, and concealment. Fraud cases examined in previous CERT studies were more similar to the fraud committed by non-managers than that committed by managers.

## **Recommendations**

The following behavioral and/or business process recommendations, and monitoring and technical recommendations are provided in response to the six findings described above. These recommendations are intended to be implemented in conjunction with other organizational controls targeted at preventing, detecting, or responding to malicious insider activity. Be sure to consult with legal counsel prior to implementing any recommendations to ensure compliance with federal, state, and local laws.

### **Behavioral and/or Business Process**

- Clearly document and consistently enforce policies and controls.
- Institute periodic security awareness training for all employees.

### **Monitoring and Technical**

- Include unexplained financial gain in any periodic reinvestigations of employees.
- Log, monitor, and audit employee online actions.
- Pay special attention to those in special positions of trust and authority with relatively easy ability to perpetrate high value crimes (e.g., accountants and managers).

- Restrict access to PII.
- Develop an insider incident response plan to control the damage from malicious insider activity, assist in the investigative process, and incorporate lessons learned to continually improve the plan.

---

## Abstract

This report describes a new insider threat study funded by the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) in collaboration with the U.S. Secret Service (USSS) and the CERT Insider Threat Center, part of Carnegie Mellon University's Software Engineering Institute. Researchers extracted technical and behavioral patterns from 67 insider and 13 external fraud cases; all 80 cases occurred between 2005 and the present. Using this information, we developed insights and risk indicators of malicious insider activity within the banking and finance sector. This information is intended to help private industry, government, and law enforcement more effectively prevent, deter, detect, investigate, and manage insider threats in this sector.

---

# 1 Introduction

This report describes a new insider threat study funded by DHS S&T. The CERT<sup>®</sup> Insider Threat Center<sup>4</sup> completed the study in collaboration with the USSS. This effort extracted technical and behavioral patterns from 80 fraud cases—67 insider and 13 external<sup>5</sup>—that occurred between 2005 and the present. These cases were used to develop insights and risk indicators to help private industry, government, and law enforcement more effectively prevent, deter, detect, investigate, and manage malicious insider activity within the banking and finance sector. This study updates an initial study of insider threats in the banking and finance sector [Randazzo 2004].

The report starts by providing definitions, an overview of selected current literature on insider threats, and the study research methodology, which may be of greater interest to researchers than financial sector practitioners. It then covers the findings we derived from an analysis of selected cases and describes a system dynamics model of the crime of fraud. Finally, we compare this crime profile, including the system dynamics model, with other crimes, provide mitigation strategies, and describe additional steps that could be taken by researchers or information security practitioners in this area who hope to reduce the occurrence of individuals committing illegal acts against their organization.

## 1.1 Terms and Definitions

A number of authors have defined insider attacks and characterized insider subjects. Predd and colleagues define an insider generally as someone with legitimate access to an organization's information assets, including contractors, auditors, temporary employees, former workers, and non-malicious subjects who cause damage unintentionally [Predd 2008]. This definition is broader than many others, but it generally reflects a consensus in the literature that, in addition to current employees, insiders may include other personnel with past or current authorized access, including contractors or even customers. For the purposes of the current study, we concentrated on insiders who caused harm to an organization through deliberate actions.

The following definitions are critical to our study:

- A *malicious insider* is a current or former employee, contractor, or other 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 [Cappelli 2009].

---

<sup>®</sup> CERT is a registered trademark owned by Carnegie Mellon University.

<sup>4</sup> More information about the CERT Insider Threat Center is available in Appendix A.

<sup>5</sup> External fraud cases are those in which no malicious insiders were involved.

- *Insider fraud* is a malicious 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 the theft of information leading to an *identity crime* [Weiland 2010].
- An *identity crime* is "the misuse of personal or financial identifiers in order to gain something of value and/or facilitate some other criminal activity."<sup>6</sup>
- A *victim organization* is a business entity that was impacted by the actions of a malicious insider.
- A *precursor* is an action, event, or condition that precedes the insider crime and is hypothesized to be associated with that crime. If the hypothesized association can be confirmed with a comparison to case controls, then those observable precursors indicate increased risk of the crime [Band 2006].

## 1.2 Related Empirical Research

Empirical insider threat research generally falls into one of three categories:

- surveys of violation frequency by type as reported anonymously by victim organizations
- simulations of insider actions by experimental groups
- post-hoc reviews of actual cases

The rest of this section provides a high-level overview of each of these three areas of empirical research.

### 1.2.1 Surveys

For years researchers have surveyed organizations to gather data on the frequency and types of computer-related crimes and violations they have experienced. Two of the most prominent surveys are the Computer Security Institute (CSI) survey, conducted in collaboration with the Federal Bureau of Investigation (FBI), and the *CSO Magazine* survey, conducted in collaboration with the USSS and the CERT Insider Threat Center. This critical information has

- established the frequency, types, costs, and countermeasures involved in a range of computer crimes experienced by a range of government, private, and other participating organizations
- documented important trends in computer crimes such as an apparent increase in the sophistication of insider crimes [CSO 2011]<sup>7</sup>

Similar surveys by Verizon have documented the variety and seriousness of these breaches [Verizon 2011]. This research has reconfirmed the continued impact of insider acts within the banking and finance sector.

---

<sup>6</sup> This definition comes from the USSS website (<http://www.secretservice.gov/criminal.shtml>).

<sup>7</sup> For more information, see the article titled "2011 Cybersecurity Watch Survey: Organizations Need More Skilled Cyber Professionals to Stay Secure" [CSO 2011].

## 1.2.2 Simulations

Computer scientists have often simulated insider activity to test different insider activity detection methods. Maybury and colleagues performed one of the most thoroughly reported simulations of this kind [Maybury 2005]. They assessed the timeliness and accuracy of several prototype techniques to provide early warning of malicious insider activity in an operational setting. More recently, Caputo and colleagues employed a blind control group format to an insider simulation. In a double-blind, control-group experimental design, Caputo and colleagues compared volunteer MITRE employees acting as highly motivated malicious versus benign insiders in pursuit of similar information targets [Caputo 2009a, Caputo 2009b]. The study's design addressed a critical deficiency in the insider threat literature: the lack of control groups involving insiders who violate policies or laws with versus without malicious intent. The research revealed that these groups used somewhat different approaches that could distinguish their motivation for security professionals.

While simulations are excellent for conducting exploratory research, testing detection methods, and overcoming gaps in more naturalistic research designs, researchers and practitioners should work closely together to generalize the results to actual insider activity within the banking and finance sector. Empirically derived lessons learned need to be interpreted and evaluated by security personnel in this area.

## 1.2.3 Case Studies and Other Empirical Research

The Defense Personnel Security Research Center (PERSEREC) compiled information related to espionage and insider events and produced two data sets that are available for research. The National Security Espionage Database contains publicly available information on espionage against the United States and includes 200 case variables describing more than 150 criminal events [Herbig 2002]. While this data set provides an invaluable overview of these cases over time, it does not provide the level of information available from more in-depth case studies with additional data sources, such as interviews with investigators, suspects, and their co-workers and legal records. This detailed information is critical to deriving practical lessons for security practitioners. However, the PERSEREC did compile more detailed data on 80 cases involving insiders who targeted the U.S. Department of Defense, military contractors, and other components of the U.S. critical infrastructure [Fischer 2003]. Shaw, Ruby, and Post reported more detailed data on a subset of these cases [Shaw 1998].

Shaw and Fischer used a multiple-source, case-study approach to examine 10 cases of malicious insider information technology (IT) activity in critical infrastructure industries [Shaw 2005]. For each case, they examined the background of the event, the environment in which it occurred, the specifics of the event, the motivations of the subject, the investigative and legal actions taken, and the lessons learned.

CERT Insider Threat Center research has focused on malicious insider threat compromises that have been adjudicated in the United States. In 2002, the Insider Threat Study Team, composed of USSS behavioral psychologists and CERT information security experts, collected approximately 150 insider threat cases that occurred in U.S. critical infrastructure sectors between 1996 and 2002 and examined them from both a technical and a behavioral perspective. The USSS and DHS S&T



funded this project. A subsequent study examined 23 incidents of illicit insider activity in the banking and finance sector and reported the following key findings [Randazzo 2004]:

- In 87 percent of the cases, the insider used legitimate system commands in committing the malicious activity. The insiders needed little technical sophistication because they tended to exploit known or newly discovered design flaws in systems used to enforce business rules or policies.
- Of the perpetrators, 81 percent planned their actions in advance.
- In 85 percent of the cases, someone else knew about the insider's actions before or during the malicious acts.
- In 81 percent of the cases, financial gain motivated the perpetrators. Revenge was the motivator in 23 percent of the cases, and 27 percent of the perpetrators were experiencing financial difficulties at the time they committed the acts.
- Perpetrators came from a variety of positions and backgrounds within the victim organization, but management had identified 33 percent of them as "difficult" and 17 percent as "disgruntled."
- Audit logs helped to identify the insiders in 74 percent of the cases.
- Of the victim organizations, 91 percent suffered financial loss, with amounts ranging from hundreds to hundreds of millions of dollars.
- Of the perpetrators, 80 percent committed the malicious acts while at work, during working hours.

The USSS and the CERT Insider Threat Center published the results of the study in a series of case analyses in the banking and finance sector [Randazzo 2004], the IT sector [Kowalski 2008a], the government sector [Kowalski 2008b], and IT sabotage across all critical infrastructure sectors [Keeney 2005]. The 2004 USSS/CERT Insider Threat Study laid the foundation for extensive follow-on research within the CERT Insider Threat Center, including the development of models, reports, training, and tools to accomplish the following:

- raise awareness of the risks of insider threat
- help identify the factors influencing an insider's decision to act
- help identify the indicators and precursors of malicious acts
- identify countermeasures that will improve the survivability and resiliency of the organization

Over the past seven years, Carnegie Mellon's CyLab,<sup>8</sup> followed by DHS National Cyber Security Division Federal Network Security Branch, funded the CERT Insider Threat Center to update its case library with more recent cases. Over 550 additional cases were collected and coded in the CERT insider threat database, bringing the case library total to over 700. The general structure of the database, depicted in Figure 17 on page 51, includes 30 major constructs and is operationalized by hundreds of specific variables.

---

<sup>8</sup> For more information, visit the CyLab website (<http://www.cylab.cmu.edu/>).

### 1.3 Theory Related to the Insider Threat

There is an abundance of literature on counterproductive work behavior (CWB), which Sackett defines as “any intentional behavior on the part of an organizational member viewed by the organization as contrary to its legitimate interests” [Sackett 2002a]. CWB includes a wide variety of both self-destructive and retaliatory behaviors, but it specifically encompasses sabotage, stealing, fraud, and vandalism. Sackett also provides a thorough review of the CWB literature and groups the antecedents of CWB into personality variables, job characteristics, work group characteristics, organizational culture, control systems, and perceived injustice [Sackett 2002b]. This work supports Shaw’s research and the CERT Insider Threat Center’s previous research findings on personal predispositions and organizational and individual stressors as antecedents of a range of malicious activity [Shaw 2006, Band 2006].

The primary personality model used in CWB research is the Five Factor Model (FFM), which includes dimensions of openness to experience, extraversion, conscientiousness, agreeableness, and emotional stability. After reviewing the literature on the FFM dimensions and CWBs, Salgado found 44 studies conducted between 1990 and 1999 that examine the relationships between the FFM dimensions and deviant behaviors (17), absenteeism (13), work-related accidents (9), and turnover (5) [Salgado 2002]. This work showed that low levels of conscientiousness and agreeableness were significant, valid predictors of workplace deviance. Related work showed that workplace stress and the perceived status of the insider within the organization were correlated with CWBs [Mount 2006, Stamper 2002].

---

## 2 Research Method

The primary goal of the current research is to produce empirically derived findings from insider and outsider computer criminal activity within the banking and finance sector to help security professionals prevent, detect, and manage malicious insider activity and risk. This section provides an overview of the research method, including subject or case selection criteria and sources, case coding procedures, and the system dynamics modeling approach.

The central question addressed by this research is

*What are the observable technical and behavioral precursors of insider fraud in the cases examined for this study, which are drawn from the financial sector, and what mitigation strategies should be considered as a result?*

This research applied the multiple (or comparative) case study method described by Yin, Kaarbo, and Beasley [Yin 2009, Kaarbo 1999]. This approach supports analytical generalizations and hypothesis testing of available data rather than statistical comparisons across groups or populations (e.g., subjects with various levels of risk factors who do and do not commit insider acts). Because it is difficult to get separate samples of individuals with hypothesized risk characteristics who do and do not commit insider acts, our study sought general patterns among demonstrated insider subjects, especially personal characteristics and behavioral and technical steps associated with insider attacks.

### 2.1 Case Identification and Selection

The following criteria guided the selection of insider cases:

1. The case subject is a malicious insider who committed fraud using some form of information technology. This explicitly excluded many cases where the insider defrauded a financial institution by means of simple cash drawer theft.<sup>9</sup>
2. The victim organization is U.S. based.
3. The subject's actions were confirmed by criminal conviction, confession, or other independent, reliable, and verifiable means.
4. Sufficient quantity and quality of information is available to ensure that cases are of comparable depth and have the appropriate amount of behavioral and technical details.

In addition, a small set of external fraud cases—cases in which no malicious insiders were involved—were also studied to facilitate an informal comparison with the insider cases. This study's selection of prosecuted cases, including cases that ended in a plea bargain, may have

---

<sup>9</sup> Two cases that more closely resembled IT sabotage and theft of IP were retained because of their impact and relevance to the concerns of the financial sector.

caused a selection bias toward insider events that are not typical of all insider offenses. It is generally acknowledged that many insider offenders are not prosecuted due to

1. the difficulty of prosecuting these cases
2. the costs of pursuing small-value crimes or crimes where recovery of misappropriated funds is unlikely
3. the relatively mild sentences that often result from conviction
4. the potentially negative impact on the victim organization's public image

Prosecuted cases may represent a distinct subset of insider events in which the victim organization

- was highly motivated to work with law enforcement by the extent of the offense and the real and reasonable likelihood of a successful outcome, such as recovery of funds
- needed an agency's police powers (e.g., search, forensic investigation, arrest) to terminate the activity or gain redress

Nonetheless, these cases offered the study team an added measure of data reliability.

While information from USSS case files was the starting point for our research, we also searched other sources for information on these cases, including various media outlets (found through searches on LexisNexis news databases and internet search engines such as Google) and criminal justice databases (found through searches on LexisNexis court databases). Finally, we conducted interviews with principal parties involved in investigating the incident, primarily the law enforcement or bank investigators involved.

## **2.2 Coding Method and Database Description**

Case coding is a critical process in which information gathered through case file document review and interviews is entered into the CERT insider threat database according to a prescribed methodology that is documented in a codebook. Appendix B shows the structure of the database used in this project, which is the same as the structure of the codebook that guided the coding process. The codebook provides operational definitions and examples of all the required items.

Because reliability is important for all types of data collection, we develop, test, and follow specific procedures to ensure that data are collected and coded in a consistent and predictable manner. To address consistency in coding, coders were 1) trained by more experienced coders and 2) briefed on the codebook's conceptual framework and typology to help them gain a clear understanding of the contents. Once trained coders completed cases, a second coder examined the coding results to ensure that details in the original source documents were not inadvertently missed by the first coder. Furthermore, a record quality index is automatically calculated for each case; in doing so, missing or blank fields are flagged so that a coder either has to indicate that field as explicitly unknown or enter the information found in the sources.

## 2.3 Modeling and Analysis Approach

The primary purpose of our modeling effort is to clarify the complex nature of the insider fraud threat. Our models evolved through a series of group data analysis sessions with individuals experienced in both the behavioral and technical aspects of insider crimes. We used system dynamics, a method for modeling and analyzing the holistic behavior of complex problems as they evolve over time [Sterman 2000]. System dynamics model boundaries encompass all the variables necessary to generate and understand problematic behavior. This approach encourages the inclusion of soft factors in the model, such as policy-related, procedural, administrator, or cultural factors.

The system dynamics models for this project were developed during a group modeling session and presented to several financial organizations prior to the publication of this report. System dynamics modeling involves identifying the primary variables of interest, the influences between these variables, and the feedback loops that are critical for understanding the complex behavior associated with insider fraud. Our group modeling session brought together people from various specialty areas, including clinical psychology, behavioral science, computing science, and cybersecurity. The group studied the details associated with and identified patterns in the insider fraud data. The group modeling process enabled the team to step back and consider the big picture at times and focus on individual concepts at other times. The goal was not to represent all cases with perfect accuracy but to paint a broad picture that represents key dynamic aspects of a preponderance of the case findings.

---

### 3 Crime Profile and Findings

Our case analysis yielded six findings based on trends and descriptive statistics observed in the case files, which are detailed in this section; however, a more general characterization of the subjects and the crimes will hopefully provide additional insights. The crime profile describes variables such as sex and age of the subject, but do not presume that this establishes a clear individual profile that could be acted upon. In fact, it most likely describes a profile of a large number of individuals who work in this industry. Rather than infer that the characteristics we describe below could be used for targeting in your workplace, compare them to your own organization to determine if and why the same characteristics may or may not depart from what we found in this set of cases. Eighty cases are included in the analyses below. The 13 external cases were not considered when calculating the statistics if they were not included in many of the analyses relevant mainly to insider issues.

#### 3.1 Subject and Crime Description

##### Age at the Beginning of the Offense

Data on age at the time of the offense were available for 58 of the insider fraud cases. The average age at the initiation of the crime was 39 and the median age was 38. Figure 1 shows the distribution of cases by age ranges.

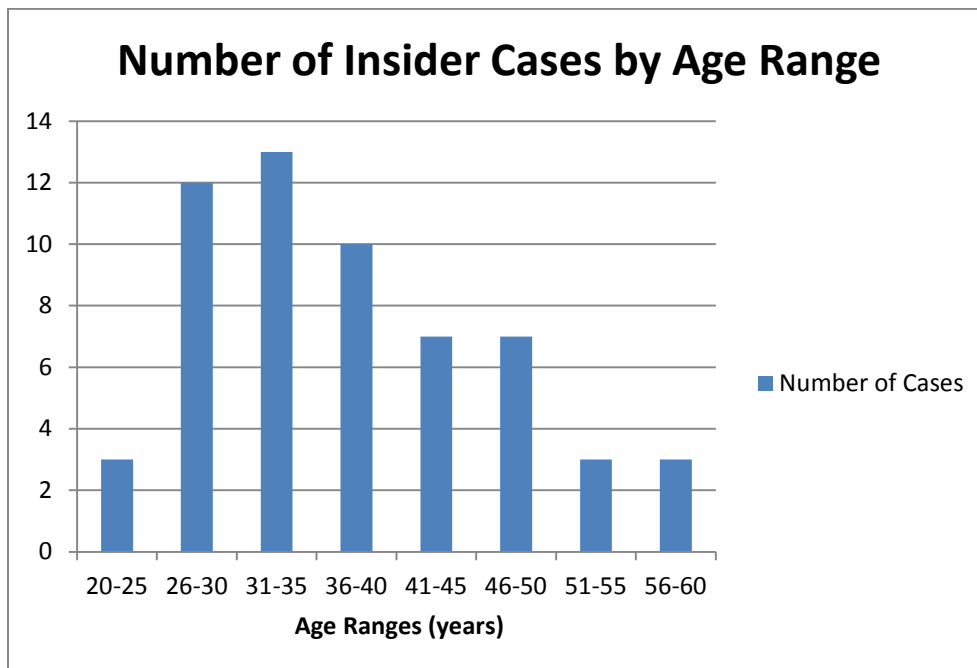


Figure 1: Number of Insider Fraud Cases by Age

## Gender

Twenty-three (31 percent) of the 67 insider fraud subjects were male and 44 (69 percent) were female. This finding departs from our previous case research on fraud, which found gender more evenly split between male and female subjects [Randazzo 2004]. The high incidence of female perpetrators in this data does not indicate a greater likelihood for females to commit fraud as much as it may reflect the distribution of women in these roles within the organizations studied. For example, 52 percent of the female subjects were in non-management positions, while only 30 percent of the male subjects were in non-management positions. This finding may reflect the fact that women were simply over-represented in our sample.

## Subject's Country of Origin

Data on national origin were available for 46 of the 67 insider cases. Eight subjects out of 46 (17 percent) were citizens of a foreign country. No single country or region was consistently represented, with Nigeria being the only country to occur more than once. Others involved subjects from China, Guatemala, Venezuela, Vietnam, Jamaica, Guyana, and the Bahamas. Data on national origin were available for 6 of the 13 external cases. Of those 6 cases, 3 were U.S. citizens and 3 were from foreign countries.

## Monetary Impact and Sentence

Actual damages are indicated in every USSS case file as the dollar amount the victim organization lost as a result of the subject's activities, while potential damages are the monetary damages that the subject had the ability to cause had he not been caught. Figure 2 shows the actual and potential damages for all 80 cases—the significant difference between the average and median was in large part due to the largest case with an actual and potential damage amount of 28 million dollars.

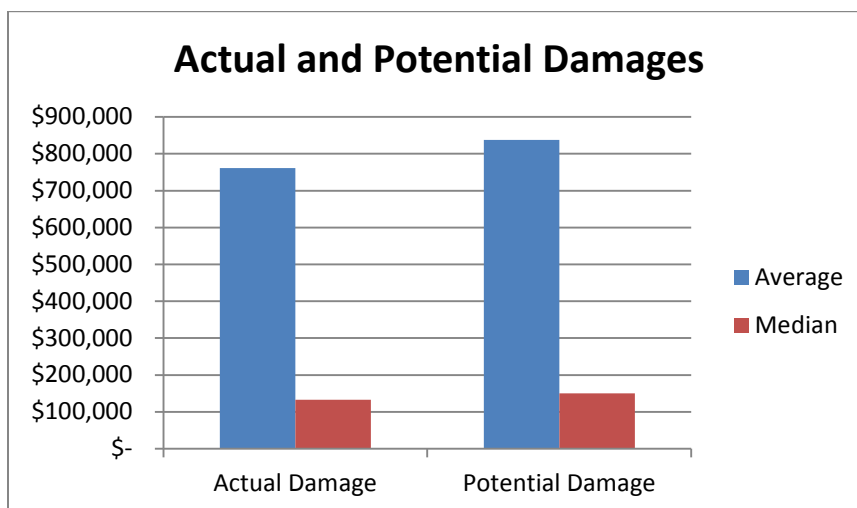


Figure 2: Average and Median Actual and Potential Damage (in Dollars)

Though we examined a smaller number of external cases, Figure 3 shows the difference in damages, both average and median, between our 67 internal cases and the 13 external cases.

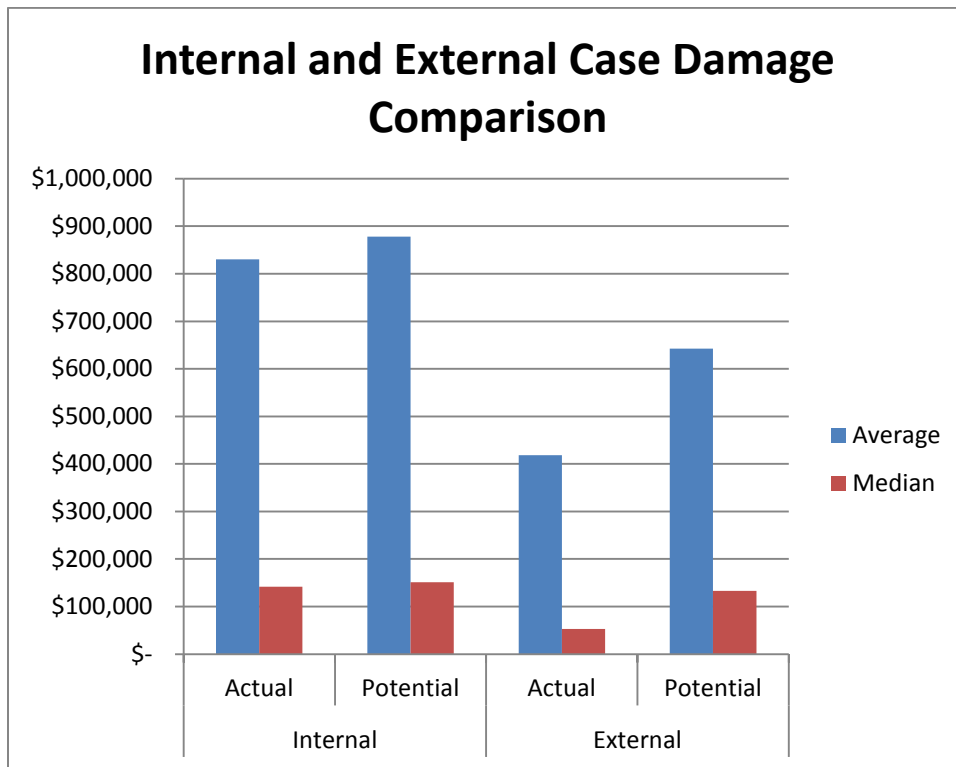


Figure 3: Comparison of Damages for Internal and External Cases

Figure 4 reflects the length of the sentence, both in terms of the jail time and the probation or supervised release. Because of the amount of larger sentences, the average time was higher than the median by about 9 months. Subjects were, on average, sentenced to 2.3 years of jail time, while they were given 3.2 years of supervised release. It is limiting to have a felony on one's record in addition to stipulations that prohibit one from working in a fiduciary role; however, consistent pre-employment screening should be followed to reduce the chance that a previous violation is not identified during the hiring process.



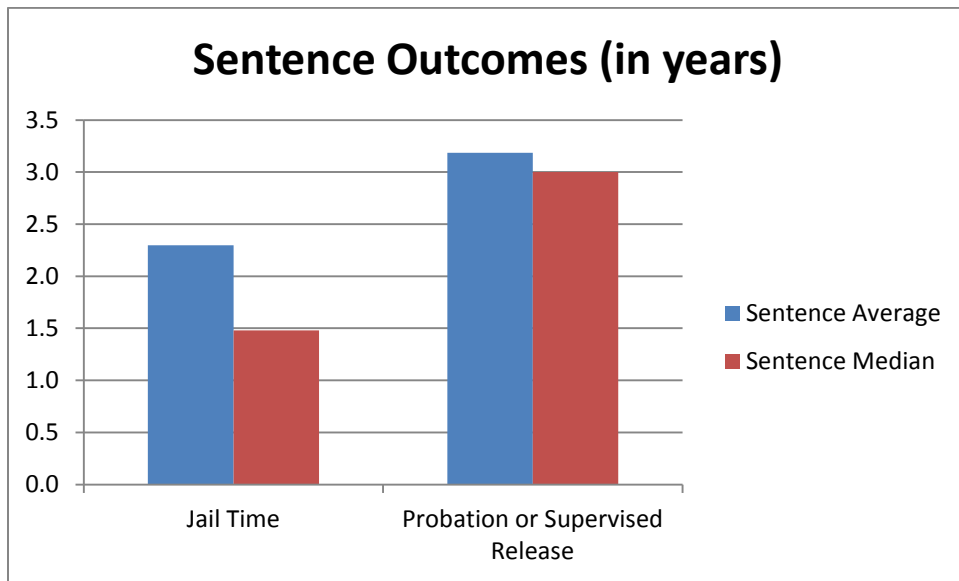


Figure 4: Average and Median Sentence Outcomes (in Years)

The remainder of this section will detail six findings that we derived from an analysis of 80 cases.

### 3.2 FINDING ONE: Criminals who executed a “low and slow” approach accomplished more damage and escaped detection for longer.

This finding addresses the chronological relationships among important, common events in our cases. We calculated average times between those events to determine the window during which the victim organization(s) might have been able to detect and respond to the incident.

#### 3.2.1 Description

The milestones we examined were the point at which

1. the subject was hired
2. the subject began the fraud activities
3. the victim organization detected the fraud
4. the victim organization reported the fraud to law enforcement (LE)

Data were available for the milestones from 47 insider cases. The available case information yields an interesting and somewhat consistent trend regarding the amount of time between these milestones. Examining only these milestones provides only part of a case chronology, since it does not take into account other potentially significant events in the life of the subject or developments within the victim organization. However, it may suggest windows of opportunity during which specific measures may prevent or disrupt the fraud activities or lessen their ultimate impact. Figure 5 shows the average timeline for the 47 cases where this data were available.

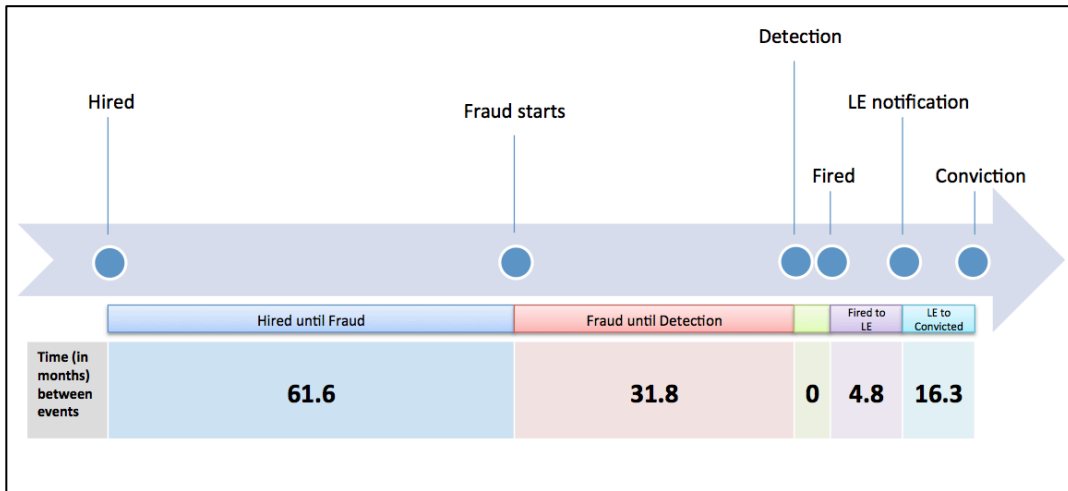


Figure 5: Average Timeline of a Case (in Months)

There are, on average, over 5 years between a subject’s hiring and the start of the fraud. Though some subjects may have started planning and even executing their fraud before the first *known* instance of fraud captured in the case, this analysis indicates that subjects worked for a long period of time without conducting any fraudulent activities. Though we observed personal and/or financial struggles in individual cases that led to those subjects committing their fraud, there was not a known, common event (e.g., divorce, personal bankruptcy, change of work assignment) that immediately preceded or triggered the fraud.

More concerning are the 32 months between the beginning of the fraud and its detection by the victim organization or law enforcement. This period suggests another lengthy period during which organizations may be able to counter the fraud, if not prevent it. Stopping the fraud during this period could lessen its impact on the victim organization.

Comparing potential and actual monetary damages to the duration of the crime may suggest what controls may have been effective at detecting fraud activities. Figure 6 shows an interesting, although not entirely consistent, picture of this comparison.

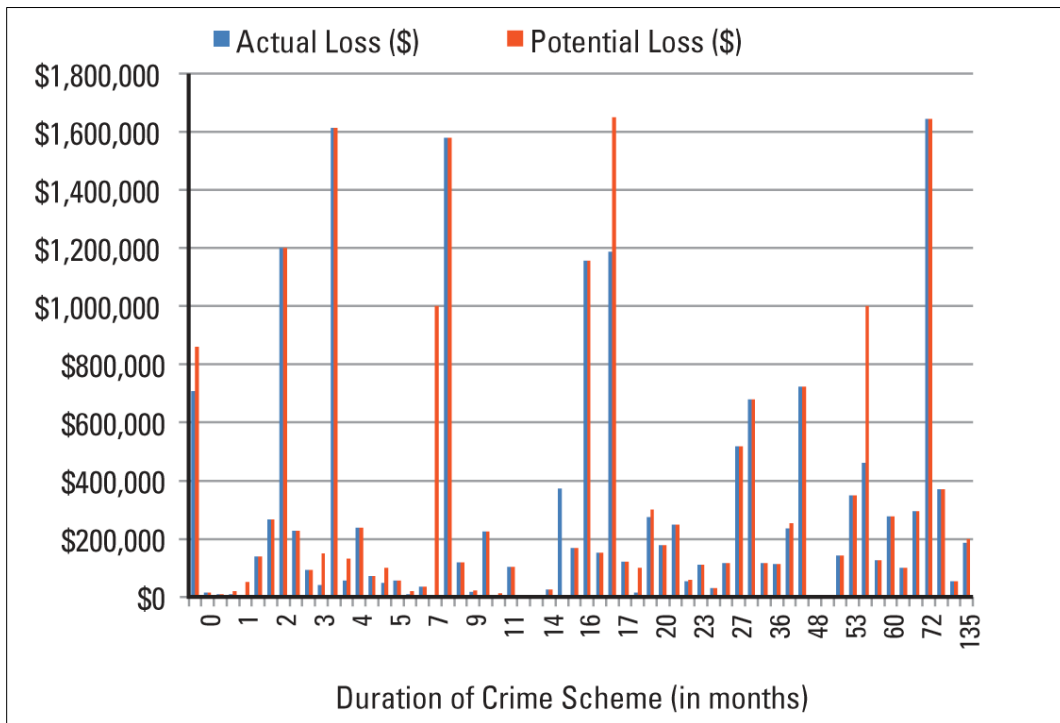


Figure 6: Damages Compared to Crime Duration

Though the data do not show a definitive correlation where the longer duration crimes clearly cause more financial impact, they do show some interesting trends. The lower 50 percent of cases (under 32 months in length) had an average actual monetary impact of approximately \$382,750, while the upper 50 percent (at or over 32 months in length) had an average actual monetary impact of approximately \$479,000. The “low and slow” crimes had, on average, 132 fraud events over the course of the crime. The highest number of fraud events during a crime was 756 over a duration of 47 months. Cases with durations of 32 months or longer and a known number of fraud events always had over a dozen theft events, with the lowest number of theft events for a case being 18. Excluding an upper outlier of 756, the average number of thefts for a case 32 months or longer is 58 theft events.

Victim organizations were apparently effective at detecting the crimes that took place for a short period of time, even though the subjects were still able to cause significant financial damage. Victim organizations were not as effective at detecting the longer term crimes, and the incremental damage (i.e., monthly, weekly amount stolen) was much lower in these cases, which may not have drawn as much attention. We recommend that financial organizations examine areas of their business in which an insider may be able to defeat controls where thresholds of activity (e.g., manager approval for transactions exceeding \$10,000) may not be reached.

Organizations should attempt to address fraud crimes by deploying controls that would be effective for the large thefts that occur in short periods of time as well as the small thefts that continue for long periods of time.

Finally, an average of nearly five months elapsed between the victim organizations' discovery of the fraud (and usually the termination of the accused insider) and their request to law enforcement personnel for investigative and legal assistance. Some of these victim organizations may have waited to gather the required evidence before involving external parties. But involving law enforcement earlier in this period may have permitted the victim organizations to at least recover from the incident more quickly.

#### Case Example #1

The insider worked as an accountant for a certified public accounting firm. Due to her good performance, her employer decided to make her solely responsible for the accounts of two client companies, one of which was her supervisor's other business, a staffing agency. The insider eventually created a fake employee on the payroll of her supervisor's business. Over the course of 6 years, the insider used this fake identity to pay herself money from the staffing agency. Several times she also issued fraudulent checks on behalf of the business and had them deposited to her personal accounts. The insider was finally caught when her supervisor was preparing to buy a house and discovered a large amount of cash missing from one of the staffing agency's accounts. She confronted the insider about the situation, and the insider admitted to the crime. According to the insider, she stole the money for daily expenses and to pay her credit card debt. While she had stolen more than \$100,000, she had already paid back approximately \$23,000. The insider was indicted on charges of wire fraud and check fraud and eventually pled guilty. She was sentenced to 15 months in prison and 3 years' probation and was ordered to repay the remaining \$77,000 of the stolen money.

### 3.2.2 Conclusions / Recommendations

This finding indicates that there may be several points in the evolution of fraud crimes that organizations can take advantage of to prevent, detect, or respond to fraud. As such, organizations should examine current or potential business practices, policies, or procedures and the extent to which those are or might be effective to prevent, detect, or respond to fraudulent activities. The fraud event durations might also provide a benchmark timeline to members of the financial services community.

However, we believe organizations could take this information one step further. They could compare their own practices, such as Employee Assistance Programs, to the timeline to determine what might deter an employee who may be considering engaging in illegal acts. Before the perpetrator's personal and/or financial struggles get the best of them, reach out to them with assistance or some will find illegal means of solving their problems. Additionally, to ensure that their financial obligations are not putting them at risk, for some employees it might be worthwhile to repeat a subset of pre-employment screening practices.

Employing tactics such as these could have helped to identify employee risk factors, the presence of which could have justified closer examination of some or all of the employee's transactions. Finally, this finding suggests that it would be prudent to develop and maintain a proactive relationship with members of law enforcement so that they can be meaningfully involved as soon as it is appropriate.

### 3.3 FINDING TWO: Insiders' means were not very technically sophisticated.

Very few of the subjects served in a technical role (e.g., database administrator) or conducted their fraud by using explicitly technical means. The data suggest that most subjects who used information systems used them, however fraudulently, for their intended purpose. For example, numerous subjects executed fraudulent wire transfers using information systems. This fraud did not require a high degree of technical sophistication or extensive knowledge of the control mechanisms. It was merely the system that everyone used to complete that particular transaction.

One important question this study sought to answer was “What kind of employees in the banking and finance industry are most likely to commit fraud?” The data in our research overwhelmingly point to employees in non-technical positions. For example, if fake vendors have been added to a payroll system, the fraud is far less likely to have been committed by a database administrator hacking into the payroll systems than a payroll administrator, responsible for paying vendors, with legitimate access to the system.

#### 3.3.1 Description

In the majority of the fraud cases studied, subjects had no need for technical sophistication or subterfuge to carry out their fraud-related activities. If a case involved a subject who performed business operations commensurate with their normal duties and involved no technical attack methods, it was categorized as an *Authorized Use* case. Of the 80 fraud cases coded, 57 (71 percent) cases relied on some form of authorized use or non-technical bypass of authorized processes. Of the 57 cases, 52 involved subjects using some form of previously authorized access to carry out the fraud. Finally, in 5 of the 57 cases, the subject used some non-technical method to bypass authorized processes and commit the fraud. For example, more than one insider altered bank statements to cover up the fraudulent transfers that had been completed and then hand-delivered those bank statements to the customer.

While the insiders' methods were largely non-technical, the insiders themselves also held non-technical positions. Organizations can focus on implementing controls that monitor non-technical insiders whose activities and system usage patterns may be inherently different than those of IT personnel.

Of the 80 cases in the data set, only 6 involved subjects with some kind of technical position. Of those 6 cases, half were helpdesk employees and half were programmers. In 9 of the cases, we were either unable to conclusively determine if the person committing the crime (whether an insider or outsider) was technical or we were unable to determine the exact identity of the criminal.

Non-technical subjects were responsible for the remaining 65 (81 percent) incidents. Seven of those subjects were external attackers, but their methods were non-technical. Figure 7 represents the distribution of technical versus non-technical positions held by insider fraudsters.

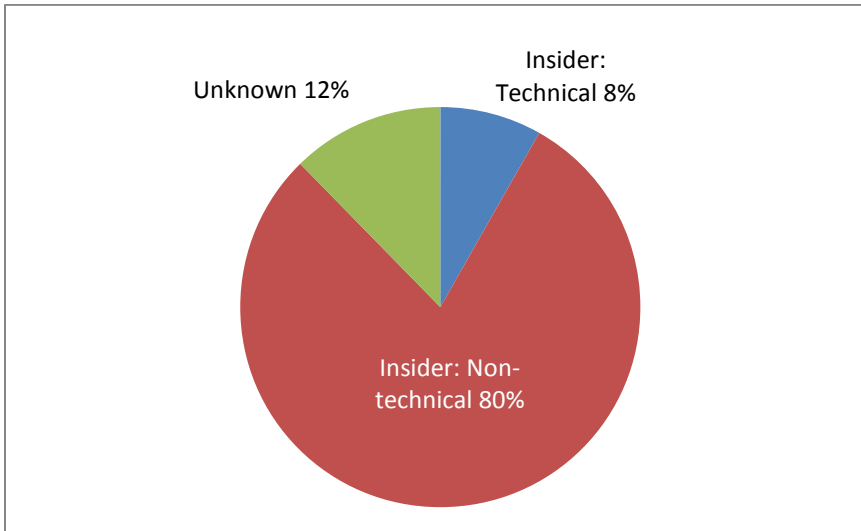


Figure 7: Insider Position Types

The few technical cases yielded some interesting observations. The three cases that were conducted by helpdesk employees were motivated strictly by financial gain. In two of the cases, the insiders stole PII using their authorized access; one sold the information, and one used the information to directly steal funds. The third helpdesk employee also used her authorized access as a means to directly siphon funds, but rather than steal customers' legitimate information, she modified the information by setting herself up as an authorized user.

The three cases involving programmers were more diverse and driven by different motives. One programmer conducted fraud for personal financial gain by using his abilities and privileges to bypass security controls. Another programmer sabotaged her organization because she was disgruntled. The final case involved the theft of intellectual property (IP) by two programmers who were dissatisfied with their positions and desired positions at a competing organization. Though these two crimes were not as closely aligned with fraud activities as the majority of our other cases, we included them in this analysis because of their impact and because we heard from several financial sector representatives that this type of crime concerns them as well.

In four of these six cases, the insiders did not need any technical methods to conduct their crime; they used the access privileges afforded to them by their positions. In the case where the programmer conducted fraud, he used a compromised co-worker's account with an easily guessed password to bypass an authorized process. In the single case of sabotage, the recently terminated insider used social engineering to get her remote access account reactivated and used the account's privileges to conduct the fraud.

To some extent, the inherently greater level of privilege granted to these technical insiders enabled their crimes. These privileges were often necessary for the insiders to perform their legitimate job duties, so organizations must ensure that technical insiders are using their privileges appropriately.

### Case Example #2

#### Non-Technical

The subject worked as a vice president for a federal credit union. As part of his job, he was given a corporate credit card to use for business purposes only. Soon after being hired and continuing throughout his employment, the insider used this corporate credit card to pay for personal expenses. The insider also used the card to take out cash advances on a few occasions, even though doing so violated company policy. To justify the cash advances, the insider created fake invoices on his business laptop and forwarded them to the appropriate departments within the organization. He also falsely claimed that the personal expenses on the card were for legitimate business purposes. For example, the insider used the card to pay restaurant bills and later claimed that the meals were for his employees; however, later investigations revealed that the subject had not treated any employees to meals. The subject was able to continue his fraudulent scheme by creating a fake contract with his wife's third-party organization and then paying the organization for fake services via wire transfer.

### Case Example #3

#### Technical

The insider was employed as a lead software developer at a prominent credit card company, which offered a rewards program where customers could earn points based on the volume and frequency of their credit card usage. These points could later be redeemed for gift cards, services, and other items of monetary value. Due to the high transaction volume of corporate accounts, a typical corporate account could hypothetically accumulate an immense number of rewards points. Therefore, the rewards points program was configured in such a way that the back-end software would not allow corporate accounts to earn points. At an unknown date, the insider devised a scheme by which he could earn fraudulent rewards points by bypassing the back-end checks in the software and linking his personal accounts to corporate business credit card accounts of third-party companies. After compromising a co-worker's domain account by guessing the password, he was able to implement a backdoor that allowed him to successfully link his personal accounts to several corporate accounts. The insider cashed in the rewards points for items of value, such as gift cards to popular chain stores, and sold them in online auctions for cash. In all, the insider was able to accumulate approximately 46 million rewards points, \$300,000 of which he was able to convert into cash before being caught by internal fraud investigators. The insider admitted to the scheme and bargained with investigators for a reduced sentence if he agreed to provide information on his technical backdoor and offer insight as to how organizations might prevent a similar occurrence from happening in the future.

### 3.3.2 Conclusions / Recommendations

The most important lesson from this finding is that the seemingly least-threatening employees—the ones without technical knowledge or privileged access to organizational systems—can still use organizational systems to cause significant damage. This finding reinforces our recommendation that organizations must adhere to good security principles when developing policies and controls to protect themselves from malicious insiders. In the large majority of the studied cases, the insiders did not require technical knowledge to commit their crimes. They easily bypassed security controls or concealed their actions with non-technical actions and exploited insufficient access controls that were put in place by their organization.

We recommend that organizations guide their policies and practices by commonly accepted security principles, such as access control, least privilege, and separation of duties. Restricting the level of employee access to that necessary to perform job duties may have prevented several of the cases described in this section.

Organizations should assume that ill-intentioned employees will leverage the most easily exploitable vulnerabilities first; often, such vulnerabilities are within the reach of most non-technical personnel. No amount of intrusion detection systems, database triggers, or host system hardening



procedures will defend against an insider with authorized access to data. Therefore, an organization can only begin to minimize or prevent costly insider attacks if it continually builds its policies and procedures on the foundation of trusted information security principles.

### 3.4 FINDING THREE: Fraud by managers differs substantially from fraud by non-managers by damage and duration.

Previous insider threat research into fraud activities indicated that non-managers were the primary perpetrators of malicious activity. In this study, we observed two main types of fraudsters: those who occupied senior positions (e.g., executives, branch managers) and those who were more junior in the organizational structure. The crimes of these two types of insiders show substantial differences, and organizations can use this information to identify alternate measures of detection or even prevention.

#### 3.4.1 Description

Of the 67 insider cases used for this study, all but 6 documented the subjects' workplace role (e.g., teller, teller manager, vice-president [VP]). Of these 61 subjects, 31 (51 percent) were managers, VPs, supervisors, or bank officers. The remaining 30 subjects (49 percent) did not hold supervisory positions, though they often served in fiduciary roles and may have had sufficient tenure at the victim organization to have been very trusted. Since more than half of the insiders were serving in supervisory roles, it is worth examining some of the other case criteria about managers and non-managers, such as differences in monetary impact and how they executed their crimes.

Figure 8 shows the actual monetary damages caused by managers and non-managers.

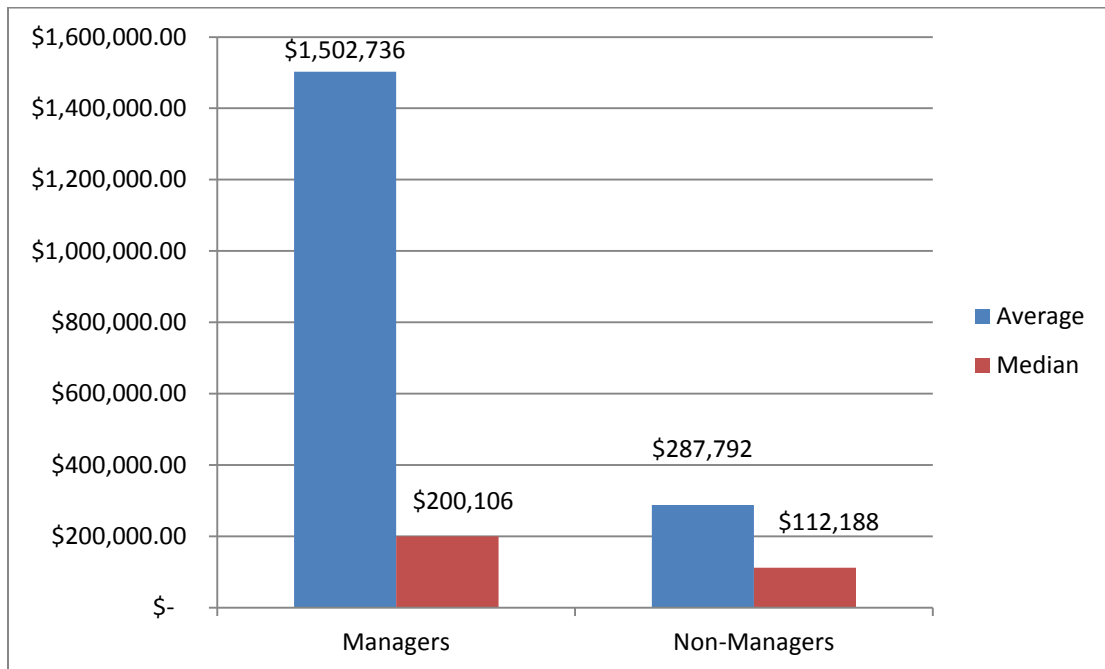


Figure 8: Actual Damages by Position Type

The average monetary damage by managers seems very high, but it is skewed by one large outlier. The median values, which address outliers both high and low, may give a better sense of these numbers. The median results show that managers consistently cause more actual damage (\$200,106) than non-managers (\$112,188).

Crime duration also shows an interesting difference. Non-managers’ crimes lasted an average of 18 months, while managers’ crimes almost doubled to an average of 33 months. One explanation of this disparity in crime duration is that managers took advantage of their superior access to information and relative lack of supervision to sustain longer crimes.

Our analysis categorized the non-managers into the following employment types:

- accounting (6 subjects)—employee whose primary responsibility is that of an accountant or equivalent
- customer service (14 subjects)—employee whose primary responsibility is interacting with the victim organization’s customers
- analyst (3 subjects)—employee whose duties deal with some sort of analysis other than accounting activities
- technical (4 subjects)—employee whose duties deal with some technical facet of operations, such as engineers or other IT personnel
- other (3 subjects)—anything that could not be accurately categorized as one of the above

Table 1 shows the crime duration (in months), average actual damage (in dollars), and damage per month (in dollars) for the first four categories of non-managers. The “other” category is not included because the associated job roles were too disparate to be considered a coherent group.

*Table 1: Comparison of Damage and Crime Duration by Non-managers*

|                            | Categories |                  |            |           |
|----------------------------|------------|------------------|------------|-----------|
|                            | Accounting | Customer Service | Technical  | Analysis  |
| Duration Average, (Months) | 41         | 10               | 26         | 20        |
| Average Damages, Actual    | \$ 472,096 | \$ 191,338       | \$ 104,430 | \$ 54,785 |
| Damage per Month, Average  | \$ 11,627  | \$ 18,350        | \$ 4,041   | \$ 2,785  |

On average, accounting employees did the most actual damage, followed by customer service employees and, with much less damage, technical and analysis employees. These numbers make sense, given that the accounting employees had the ability to illegally transfer funds and often had access to PII. It also follows that they were able to continue their schemes for the longest amount of time since they were often the first and last line of defense for proper accounting procedures. Though customer service representatives were also able to cause significant damage on average, their schemes did not go on nearly as long; in fact, their schemes had the shortest duration of all. This may have been because their activities were more easily audited and detected, and also perhaps because they were generally not in supervisory roles and were thus able to hide or explain their actions with exception handling.

#### Case Example #4

##### Manager

The insider worked as a branch manager of a national banking institution. The insider's father had a criminal history and while in prison had met a man who, after he was released, eventually started running an identity theft scheme. Sometime after being released, the father put his prison friend (the outsider) in touch with his son (the insider) in the hopes that the insider would help steal account information using his privileged access. The outsider offered to pay the insider \$1,000 for each account. While the insider initially refused, his father was eventually able to persuade him to take part in the fraud scheme. Over a three-month period, the outsider asked the insider for the account information of 25 specific people. The insider divulged this information over the phone at work and on paper documents outside of work. The outsider made fake identifications using the account information and had a team of complicit cashiers who walked into banks and made fraudulent withdrawals. In total, \$228,000 was stolen. Once investigators received reports from customers whose accounts had been compromised, they were able to use the access logs of customer records to trace the fraud to the insider. The insider admitted to the scheme, and even helped investigators conduct a sting operation to apprehend the outsider. Considering that he helped to catch the outsider, who had an extensive criminal history and numerous charges, the insider was sentenced to time served and two years of supervised release.

#### Case Example #5

##### Non-Manager

The insider worked as the loan processor for a banking institution. As part of her job responsibilities, she had full privileges to read and modify loan information within the organization. She took out two legitimate loans totaling \$39,000 from her employer organization for her own personal expenses, which in itself was not a violation of company policy. However, to help pay for additional personal expenses, she used her privileged access several times to fraudulently increase her personal loan amounts. She then withdrew the resulting difference, thereby committing embezzlement. She was discovered when a routine audit revealed that essential loan documentation was missing from her loan account, which the insider had removed to cover up the fraud. By the end of her scheme, she had stolen approximately \$112,000. She was sentenced to 18 months in prison and 5 years' probation and was ordered to pay full restitution.

### 3.4.2 Conclusions / Recommendations

Though their activities and access may have differed at times, managers and accountants caused the most damage from insider fraud and evaded detection for the longest amount of time. Prevention strategies for these two types of employees may not be the same, but they both require that the organization closely check, at least occasionally, even those who are in charge of certain criti-

cal business processes. Many of the victim organizations in this study tended to blindly trust that the lead accountant or branch manager must be doing things for the right reason, even if their actions violated policies and procedures. Organizations should consider auditing the activities of accountants and managers on a more detailed level or more frequent basis than other employees.

It is essential for financial organizations to develop enforceable policies and clearly communicate them to all employees, not just those responsible for enforcing the rules. Despite this communication, non-managers may be reluctant to report when their supervisors violate rules, especially rules that seem to have little association with malicious or criminal conduct. Therefore, a corollary practice should be put in place to disallow regular exception handling. For example, there was more than one case in which, against the rules, a manager insisted that he deliver customer account statements by hand in the name of good customer service. The manager did this because he had altered the statements and thought this exception would help him to avoid detection.

Employees in general and those with greater privilege, in particular, should be greatly limited in what actions they can perform on their own accounts, as well as the accounts of their immediate family members. We found that using scripts to notify fraud-prevention specialists and using access-control mechanisms to prevent fraud in the first place, would have been effective in several of the cases in this study.

Finally, financial organizations must ensure that access control is granular enough to provide only necessary access to those in senior or supervisory positions. For fraud as well as other types of insider crimes, we often see privileges accumulate over years of employment without employee accesses being closely examined by the victim organization until it is too late. If tellers or teller managers can complete account transfers, then should a branch manager be able to perform the same activities? Perhaps the answer is yes; however, the actions of managers should be scrutinized at a more detailed level than the actions of other employees.

### **3.5 FINDING FOUR: Most cases do not involve collusion.**

There was not a significant number of cases involving collusion, but those that did occur generally involved external collusion (i.e., a bank insider colluding with an external party to facilitate the crime). The external collusions often involved an insider who wanted or needed an external party to act as a conduit to sell stolen PII or pose as a legitimate account holder. Further, there was only one case of collusion that involved someone in a supervisory or management position. This indicates that collusion was not necessary for those individuals to commit the fraud. In the cases in this study, managers involved non-managers in their crime largely without the non-managers' knowledge.

The lack of internal collusion departs from some of our previous research and findings about fraud collusion. For example, we have previously captured several instances of rings of insiders completing malicious activities together—one such collusion was a ring of individuals at a government agency issuing fraudulent identification cards. Nonetheless, the collusion cases in this study did exhibit some trends that may inform collusion controls.

### 3.5.1 Description

We categorized and tracked three types of collusion for this study:

- *inside*—An insider recruited or was recruited by other victim organization employees.
- *outside*—An insider recruited or was recruited by parties completely external to the victim organization.
- *both*—The crime involved inside and outside parties. Either party could have done the recruitment.

Figure 9 shows the distribution of the different types of collusion.

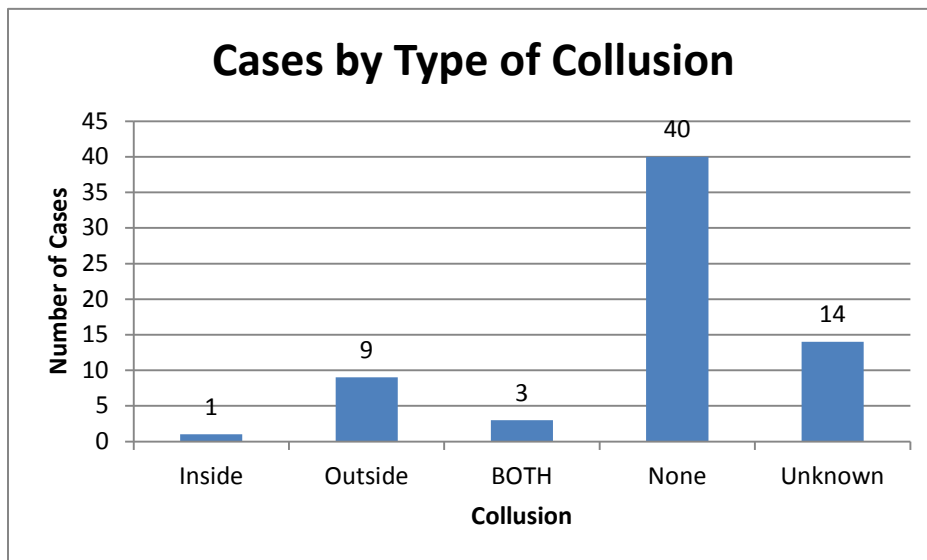


Figure 9: Cases by Type of Collusion

For all insider cases, only 13 (16 percent) involved any collusion. This relatively small number departs from some of our previous findings, both in other specific sectors and across all sectors [Cappelli 2012]. Since the majority of fraud collusion in the financial sector involved outside actors, it also seems that the malicious insiders often required external assistance to complete their crimes. For example, two cases involved inside employees paying outside entities (one of which posed as a vendor), who promptly withdrew money and shared it with the insider. Seven additional cases involving external collusion dealt with the sale of PII. The safeguarding of PII, or lack thereof, was a common theme and is addressed in Finding Six (see page 27).

In other sectors, internal collusion often occurs when it facilitates the crime or makes it more profitable. This was the case in the single financial-sector case involving only internal collusion. The two insiders had separate access to IP, and their collaboration facilitated the crime.

### Case Example #6

The subject, a financial institution employee, accessed and printed account information belonging to multiple individuals. This information was then provided to an outsider, her boyfriend. The outsider provided the information to associates in New York who then recruited homeless or indigent people to enter financial branches, pose as legitimate account holders, and withdraw funds from the financial institution. The financial institution began investigating the missing funds and interviewed the subject, who confessed that she had printed the account information and passed it to an outside source. The subject was sentenced to probation (2 years) with home detention (6 months), random drug testing, and 50 hours of community service. The subject was also ordered to repay part of the stolen funds. The total losses experienced by the victims exceeded \$235,000.

### 3.5.2 Conclusions / Recommendations

The vast majority of cases that involve collusion also involve the improper use of customer information or PII. Clearly, the black-market value of such information motivates employees to undertake risky and illegal activities. Properly controlling access to PII has already emerged as a critical issue for businesses, both to maintain trusted relationships with customers and to avoid fines and undue attention from regulators and law enforcement.

Some of the insiders who colluded with others used particularly low-tech means of exfiltrating the information, such as reciting the information over the phone or handwriting it on paper. In these cases, it seems there is virtually no technical detection measure relating to the data exfiltration. The fraudsters' use of the customer account information was only caught with forensic audits after several of the accounts they had accessed were manually flagged for unusual activity. Another group of cases involved the use of technology, but not necessarily in a particularly inventive or unique way. For example, one subject used screen captures, another copied and pasted PII into text files, and many more printed the information. Though these may seem like normal business activities, organizations should strongly consider restricting such activities on workstations that regularly process PII.

These cases may indicate that organizations must implement extremely stringent controls to adequately control employees with legitimate and regular access to customer PII. For example, we know of one financial institution that restricts its helpdesk and customer service representatives from printing anything from their desktops or bringing pencil and paper into the environment; additionally, supervisors physically watch these employees from a raised floor above the employees at all times. Though this might be perceived by some as extreme, our cases clearly indicate the need to strongly protect access to PII and prevent abuse.

### 3.6 FINDING FIVE: Most incidents were detected through an audit, customer complaints, or co-worker suspicions.

This finding addresses how victim organizations in the study detected and responded to incidents. When the data were available, we recorded the actors involved with detecting the incident and the

methods they used. We reveal the most common and effective methods of discovering an insider's fraud.

### 3.6.1 Description

Data about the detection and response phases proved scarce at times. Of the 80 cases in the study, just under half (45 percent) lacked information on how the incident was detected and by whom, and just over half (51 percent) lacked information about the type of logs used during the detection and incident response phases. A fifth of the cases did not identify the primary actors involved with incident response.

#### **How was the attack detected?**

The most common way attacks were detected was through routine or impromptu audits. An audit detected the insider's fraudulent activities in 41 percent of the cases where detection methods were known. Other non-technical methods, such as customer complaints and co-workers noticing suspicious behaviors, were used to detect 39 percent of the insiders. Only 6 percent of the cases involved fraud-monitoring software and systems, while the remaining cases used unknown detection methods.

#### **Who detected the attack?**

Over half of the insiders were detected by other victim organization employees, though none of the employees were members of the IT staff. This, in conjunction with the mere 6 percent of cases where software and systems were used in detection, seems to indicate that fraud-detection technology was either ineffective or absent. Most of the remaining cases were detected by customers, an unfortunate yet likely source of detection in cases of bank fraud.

#### **What logs were used to detect the incident?**

The case data contained limited information regarding the logs that were used during the detection and response phases. However, of the 62 cases with sufficient information, transaction logs, database logs, and access logs were utilized in 20 percent of the cases. About 10 percent of the cases showed strong evidence that no logs were used during detection, often because the insider readily admitted to the crime before the evidence was analyzed. The remaining 70 percent of cases presented evidence of log usage without specifying the type or exhibited a mixture of evidence, such as surveillance footage, phone records, print server logs, and system file logs.

#### **Who responded to the incident?**

As expected, most initial responders to the incidents were managers and/or internal investigators (75 percent). Some cases (13 percent) also involved state or local law enforcement officials in addition to the Secret Service.

### Case Example #7

The insider, a temporary bank employee, was responsible for processing large cash deposits and placing them in the vault in bank-issued deposit bags. On site and during work hours, the insider created fake deposit bags using the company-issued system, put them in the vault in place of legitimate deposit bags, and stole the money from the legitimate deposit bags. In total, during a three-month period, the insider stole 12 deposit bags containing more than \$92,000. Even though each of the 12 customers complained of their deposits not being credited to their accounts, it was not until the 12th customer's complaint that the victim organization conducted an investigation. Using surveillance footage and transaction logs, the victim organization discovered the insider's scheme.

### 3.6.2 Conclusions / Recommendations

The case data seem to indicate that technology played a very small role in enabling victim organizations to detect fraud. However, by itself, this finding could be explained or skewed by other factors. Perhaps technology was largely successful at preventing or detecting fraud before any damage occurred, thereby preventing the incident or checking it before law enforcement became involved. Additionally, even if security systems had been collecting useful information to detect fraud, the tools necessary to correlate the data may have been absent. Furthermore, the victim organization's IT staff may have been too busy with other tasks to adequately monitor the logs.

The large majority of cases were detected by non-technical methods. The victim organizations involved in the 80 cases were much more successful at detecting fraud by conducting audits, monitoring suspicious behaviors, and questioning abnormal activities. Organizations should provide open and anonymous communication channels for their employees to use if they suspect their co-workers of conducting fraudulent activity. Additionally, routine and impromptu audits to inspect the activities of all employees should take place frequently. No process, especially exception processes, should go unchecked. No employee, no matter how senior, should be exempt.

### 3.7 FINDING SIX—Personally identifiable information (PII) is a prominent target of those committing fraud.

While selecting cases for this study, the research team reviewed many USSS case files. One of the criteria for including a case was that the subject had used some form of technology in the commission of the fraud. We excluded quite a few cases involving bank tellers and a few teller managers who pocketed money from their cash drawer. These tellers and managers often falsified documents about the true balance to avoid detection. Once we completed our case selection, we realized that many other employees perform similar crimes—the difference is that these employees raid information systems instead of cash drawers and PII is the commodity of value.

Clearly, stealing cash from a drawer yields the insider immediate and tangible benefits, but it also leaves a trail that offenders must cover. Given the large market for stolen user and account credentials that can be used to encode a credit card or automated teller machine (ATM) card for im-



mediate use, PII is only slightly less liquid an asset than cash. Compared to cash drawer theft, the trail of evidence in inappropriate use of PII may not always be as clear. The insider may have merely completed a normal activity (e.g., printing customer records) and used its outcome to profit externally. Because the PII audit trail is more difficult to trace, financial institutions must restrict insiders' ability to indiscriminately access and export such sensitive information.

To reveal any differences and better specify how PII misuse might be combatted, this section separates and compares cases that involve PII and those that do not.

### 3.7.1 Description

Because PII is such a sensitive and critical organizational resource, to better understand this type of crime, this analysis includes all cases of fraud committed by subjects internal and external to the victim organization. Of the 80 cases, 34 percent involved PII and 66 percent did not (see Figure 10). The external cases were evenly split between PII cases and non-PII cases.

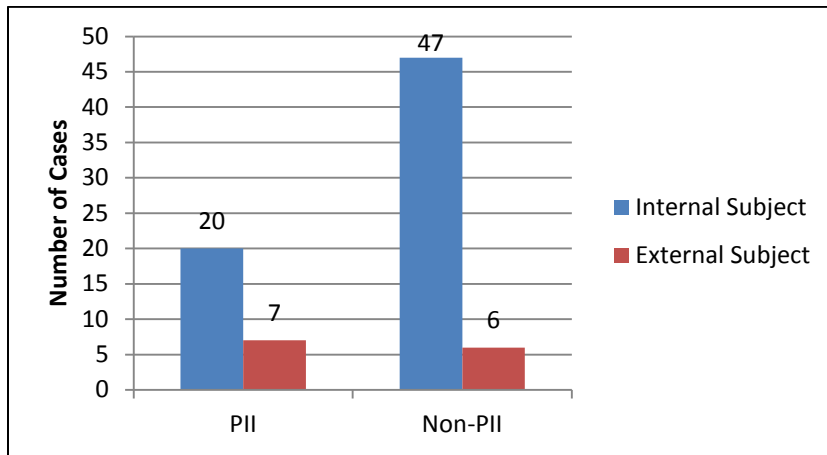


Figure 10: PII and Non-PII Cases by Type of Subject

Though monetary damages are only one measure of a crime's severity, we compared actual monetary damages in the two categories of cases (PII and non-PII). As with other findings and analysis, there are several cases with extremely high damages that skew the numbers when calculating the average, so we also computed the median. For cases involving PII, the average damage per case was \$222,896 and the median damage was \$52,339, as seen in Figure 11. The non-PII cases involved damages roughly four times as large, both for the average (\$1,046,670) and the median (\$186,000). The difference might suggest that the PII cases were insignificant or not worthy of concern. However, 10 PII cases involved damages that exceeded \$100,000 and 2 involved damages of more than one million dollars.

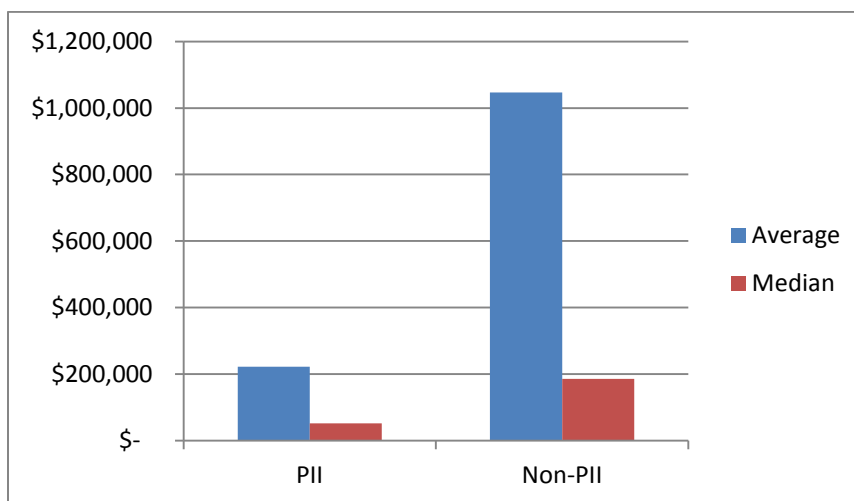


Figure 11: Average and Median Damage by PII and Non-PII Cases

A potential explanation for the lower damages of PII cases is that they were detected and stopped earlier than non-PII cases. The cases included several crimes of unknown duration in both categories, which reduced the number of cases with known duration to 18 PII cases and 43 non-PII cases. The crimes involving PII were consistently shorter in duration. The median durations were 6 months for PII cases and 19 months for non-PII cases. The averages were much closer, at 19 months for PII cases and 27 months for non-PII cases. Even when accounting for the long-duration PII cases bringing the average up, more than 80 percent of the subjects committing crimes involving PII did so for less than 2 years before being caught.

Perhaps the detection mechanisms worked better in these cases, or perhaps these criminals were not as good at concealing their crimes. No matter the explanation, these cases still caused significant financial damage and potentially exposed the victim organizations to unwanted consequences, such as disclosure requirements and potential regulatory penalties and fines.

Finally, characterizing the type of employee that committed acts of fraud with PII may provide some insight into mitigation strategies. As in Finding 3 (see page 20), we gleaned information about the age, tenure, and seniority of the subjects from our case data and used it to compare PII cases to non-PII cases. The differences are described below and summarized in Table 2.

- *Age*—A noticeable difference emerged for this variable. The average age of subjects (at the beginning of the crime) who misused PII was 32 years, while subjects who did not use PII were, on average, 40 years old. Though there were 16 cases with unknown ages and several subjects on the extreme ends of the age scale, the median values are similar to the averages: 30 years for PII cases and 40 years for non-PII cases. Clearly, those who used PII in the commission of their crimes were more likely to be closer to entry into the workforce than on the road to retirement.
- *Tenure*—For this variable, we excluded the external cases and unknowns from the calculations, leaving 47 cases where tenure was applicable or known. Consistent with the finding about age, the subjects who were involved with PII crimes had not been with the victim or-

ganization as long as non-PII subjects. PII subjects spent an average of less than 8 years (7.5 years) with their organization before being fired for their actions. Non-PII subjects had spent, on average, over 11 years (11.2) with the victim organization.

- *Level of Seniority*—Finally, we examined level of seniority. As shown in Figure 12, PII cases involved both managers and non-managers, but the number of non-managers involved with trafficking PII was more than twice the number of managers.

Taken together, these variables paint a fairly consistent picture of insiders committing crimes involving PII—such crimes tend to be committed by younger, less experienced non-managers. The crimes involving PII were also caught more quickly than non-PII crimes and, on average, resulted in less damage. However, some PII crimes caused damages as large as non-PII crimes, so the potential financial impact of these crimes should not be ignored.

Table 2: Comparison of Crimes by Their Involvement of PII

|  | Crimes Involving PII                                     | Crimes Not Involving PII                                |
|--|--|---|
| <b>Age</b>   | 32 years   | 40 years  |
| <b>Tenure</b>  | 7.5 years  | 11.2 years  |
| <b>Position of Seniority<br/>(unknowns excluded from<br/>calculated percentages)</b> | Managers—22%<br>Non-managers—48%<br>External Parties—30% | Managers—53%<br>Non-managers—44%<br>External Parties—2% |

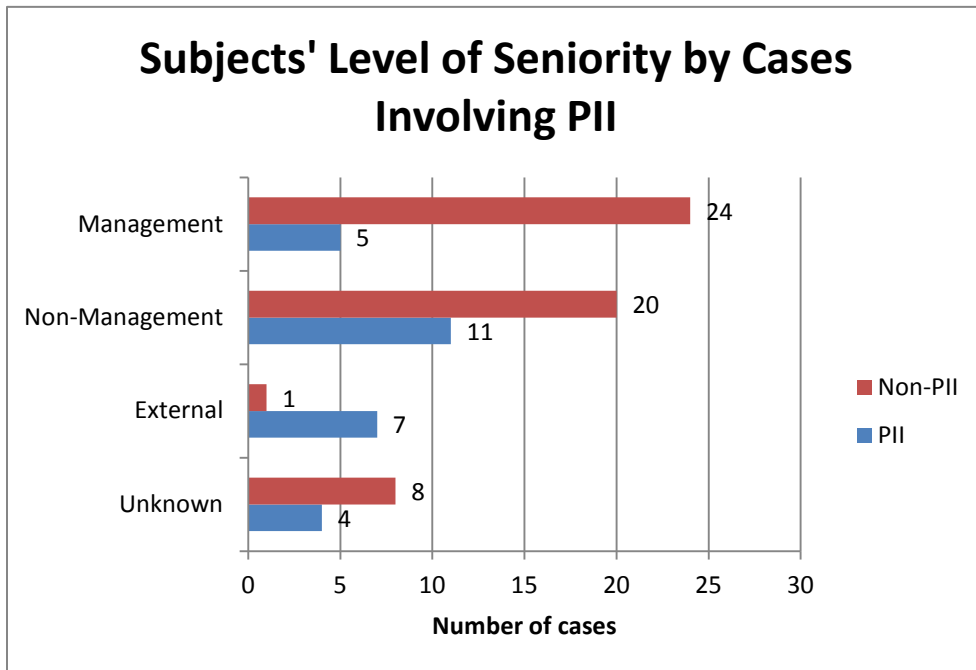


Figure 12: Level of Seniority in Cases Involving PII

### Case Example #8

The insider and his accomplices were customer service employees at a financial institution's call center. These employees had access to customer information, which included PII. While accessing customer accounts during the normal course of business, the insider and his accomplices printed screen captures of customer records and gave them to an outsider to make fraudulent purchases. Sometimes the insiders modified customer records to have a credit card sent to an address to which they had access, and they would use these newly issued cards to make fraudulent purchases. One insider even purchased a wedding dress with a fraudulent card. The organization's total losses exceeded \$2.2 million.

### 3.7.2 Conclusions / Recommendations

In every case involving PII, the insiders had to export the data to a format that was acceptable to those who ultimately consumed the PII. Some insiders used creative methods of exfiltration to avoid detection. In several cases, audits of the subject's information system usage revealed that the subject had violated policy, though it was not clear if the audit was random or not.

Financial institutions must consider more tightly restricting what customer PII and account credentials their employees can access, print, or save electronically. Though employees require some base level of access to do their jobs, granting them unfettered access can lead to costly information exposure that could entail fines and litigation. Financial institutions must place strong restrictions on employees' access to customer PII and account credentials that, at the very least, meet their regulatory requirements. If they do not already, they may also want to consider regularly auditing the use of information systems that process customer PII and account credentials.

Whenever fraudulent insider activity is detected, whether or not such activity involves PII, organizations should perform analyses to determine how to prevent or detect similar fraud in the future. Organizations should evaluate the fraud and ask the following questions:

- What business processes need to change?
- What new controls could be implemented to prevent similar activity in the future?
- What automated scripts are available that might detect similar activity?

Organizations should then take the necessary steps, such as creating and running fraud-detection scripts, to help identify similar or ongoing fraud activity.

---

## 4 Fraud Dynamics

To complement the previous section's characterization of insider fraud, this section describes prominent patterns in the dynamic behavior of fraud over time. We take a step back from the details of the individual findings and paint a larger picture of the crime. Not all aspects of the fraud model developed have detailed case frequencies associated with them. There were gaps in the data that would not allow a coherent behavior-over-time model to be developed if we required hard numbers for all aspects. Nevertheless, the model does represent many aspects of the cases we reviewed quite well. The model embodies a set of hypotheses about fraud in the banking and finance sector that can be tested in future research.

While analyzing insider fraud cases, we discovered two dominant scenarios: the Manager Scenario (32 cases) and the Non-Manager Employee Scenario (30 cases). In the Manager Scenario, the perpetrators of fraud are typically branch managers or vice presidents who realize they are able to alter business processes, including influencing subordinate employees, in a way that suits their desire to profit financially. In the Non-Manager Employee Scenario, the perpetrators are often customer service representatives who alter accounts or steal customer accounts or other personally identifiable information (PII) to defraud the victim organization for money. These scenarios share many patterns, but they each have key distinguishing characteristics.

As was mentioned in Section 2, we used a technique called *system dynamics*, which is a method for modeling and analyzing the holistic nature of complex problems as they evolve over time [Sterman 2000]. This section provides an overview of the approach and its notation, describes the Fraud Triangle as a starting point for organizing the model, and presents system dynamics models for the two fraud scenarios.

### 4.1 System Dynamics

A powerful tenet of system dynamics is that the underlying feedback structure of problematic behavior captures the behavior's dynamic complexity. System dynamics models consist of variables connected by causal relationships. Every relationship represents either a positive or negative influence of one variable on another. A positive influence (shown as a solid arrow between two variables) indicates that the values of the variables move in the same direction, and a negative influence (shown as a dotted arrow between two variables) indicates that they move in opposite directions. A relationship's polarity assumes that all other variables in the model remain constant.

A connected group of variables can create two types of feedback loops:

- Balancing loops, indicated by the label *B* and a number within the loop symbol, describe system behaviors that oppose change and tend to drive variables to some goal state. Balancing loops often represent actions that an organization takes to mitigate a problem.
- Reinforcing loops, indicated by the label *R* and a number within the loop symbol, describe system behaviors that tend to drive variable values consistently upward or downward. Rein-

forcing loops often represent the escalation of problems but may include problem-mitigation behaviors.

Within a model, a loop symbol containing an italicized loop name indicates a significant feedback loop. The number of negative influences along the path of the loop determines the loop’s type: an odd number of negative influences indicates a balancing loop, and an even (or zero) number of negative influences indicates a reinforcing loop.

Figure 13 summarizes the notation used in this report. Our modeling is restricted to a portion of the notation that does not involve simulation. Models using this notation are often referred to as *qualitative system dynamics models* or *causal loop diagrams*.



|   |   |
|---|---|
| Var1  | <b>Variable</b> – anything of interest in the problem being modeled   |
| Var1 $\longrightarrow$ Var2   | <b>Positive Influence (solid arrow)</b> – values of variables move in the same direction (e.g., source increases, target increases)                 |
| Var1 $\text{---} \longrightarrow$ Var2  | <b>Negative Influence (dotted arrow)</b> – values of variables move in the opposite direction (e.g., source increases, the target decreases)        |
| <br><i>Loop Characterization</i> | <b>Balancing Loop</b> – a feedback loop that moves variable values to a goal state; color loop identifies circular influence path                   |
| <br><i>Loop Characterization</i> | <b>Reinforcing Loop</b> – a feedback loop that moves variable values consistently upward or downward; loop color identifies circular influence path |

Figure 13: System Dynamics Notation

## 4.2 Fraud Triangle

The system dynamics model we developed in this research has as an organizing structure similar to the Fraud Triangle, one of the most famous fraud-specific models, developed by the criminologist Donald Cressey in the early 1950s [Cressey 1974]. We summarize the Fraud Triangle in this section.

Cressey interviewed imprisoned bank embezzlers and observed that many of these formerly law-abiding citizens had a “non-sharable financial problem” [Cressey 1974]. This observation led him to develop the Fraud Triangle, depicted in Figure 14.

Cressey's theory holds that for fraud to occur, three dimensions must all be present: pressure, opportunity, and rationalization.

- *Pressure* is what causes a person to commit fraud. It often stems from a significant financial need or problem. This problem or need can arise due to external pressures, such as medical bills, addiction problems, or even just expensive taste. While some fraud is committed purely out of greed, Cressey observed that perpetrators often need to resolve their problem in secret, making it “non-sharable.”
- *Opportunity* is the ability to commit fraud. It may be the result of weak internal controls or poor management oversight. Organizations have more control over the opportunity dimension than the other two dimensions. Organizations can build processes, procedures, and controls that inhibit or deter an employees' ability to commit fraud and then effectively detect it when it occurs.
- *Rationalization* is a perpetrator's process of overcoming any personal or ethical hesitations to commit the fraud. It involves reconciling the bad behavior with commonly accepted notions of decency or trust. Rationalizing individuals may believe that, due to perceived mistreatment, the organization owes them something or that committing the fraud is the only way to save their family from devastation. Rationalization may incorporate beliefs that the fraudster is merely borrowing money until he or she can repay it. At the other end of the spectrum, rationalization incorporates misunderstanding of the severity of the fraudulent acts or apathy about their consequences.

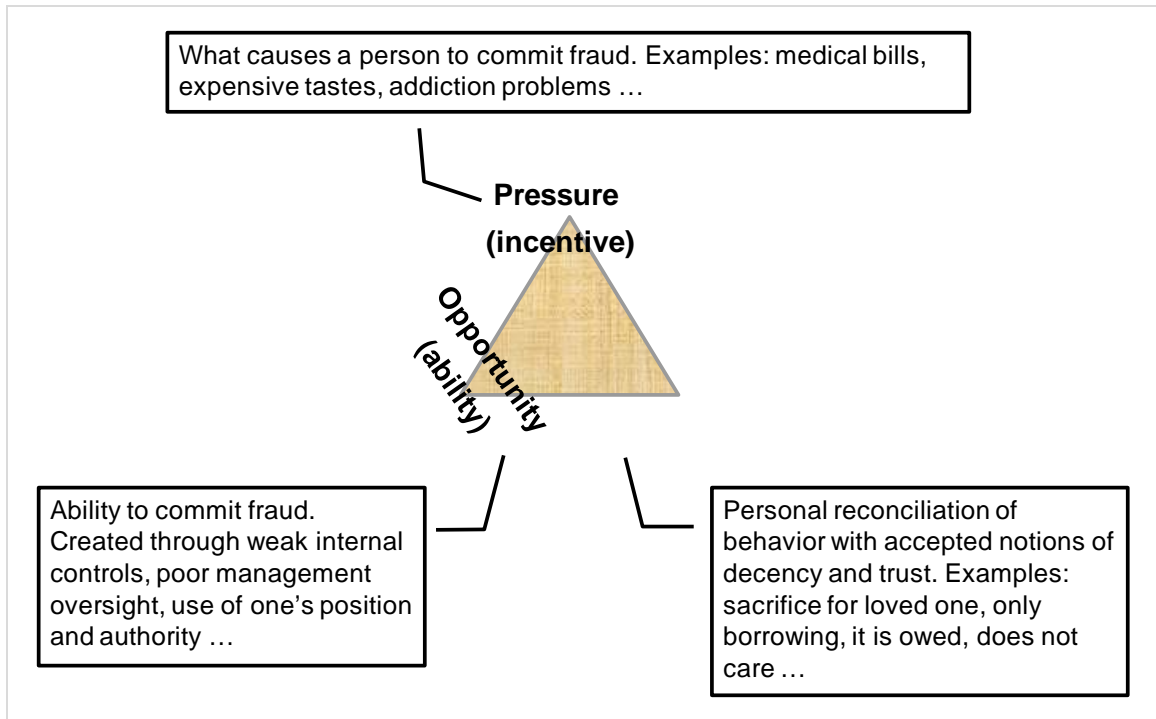


Figure 14: Fraud Triangle

The Fraud Triangle has gained widespread support, most prominently from the document titled “Consideration of Fraud in Financial Statement Fraud,” published by the American Institute for Certified Public Accountants (AICPA) [AICPA 2002]. Multiple studies have shown the value of considering the Fraud Triangle’s dimensions when conducting organizational audits [Wilks 2002, 2004, Favere-Marchesi 2009]. Other authors have suggested that the Fraud Triangle is more appropriate for employee asset misappropriations than it is for “‘major’ (million-dollar-plus) management fraud, particularly the corruption schemes” [O’Gara 2004]. Nevertheless, we find it useful as a basis for modeling the primary patterns of insider fraud.

### **4.3 Manager Model**

Figure 15 shows the system dynamics model of manager fraud. The red variables in the upper middle portion of the model represent the vertices of the Fraud Triangle. As shown, the insider’s incentive, opportunity, and rationalization all contribute to the insider’s fraud-related activities. The insider’s incentive and opportunity are incorporated in major feedback loops within the model and will be described in the next sections. The limited information on rationalization suggests that some insiders rationalized that their actions were only temporary and that they would eventually make things right. Another common feeling was that the insider was at a turning point in his or her life and had no option but to commit the crime.



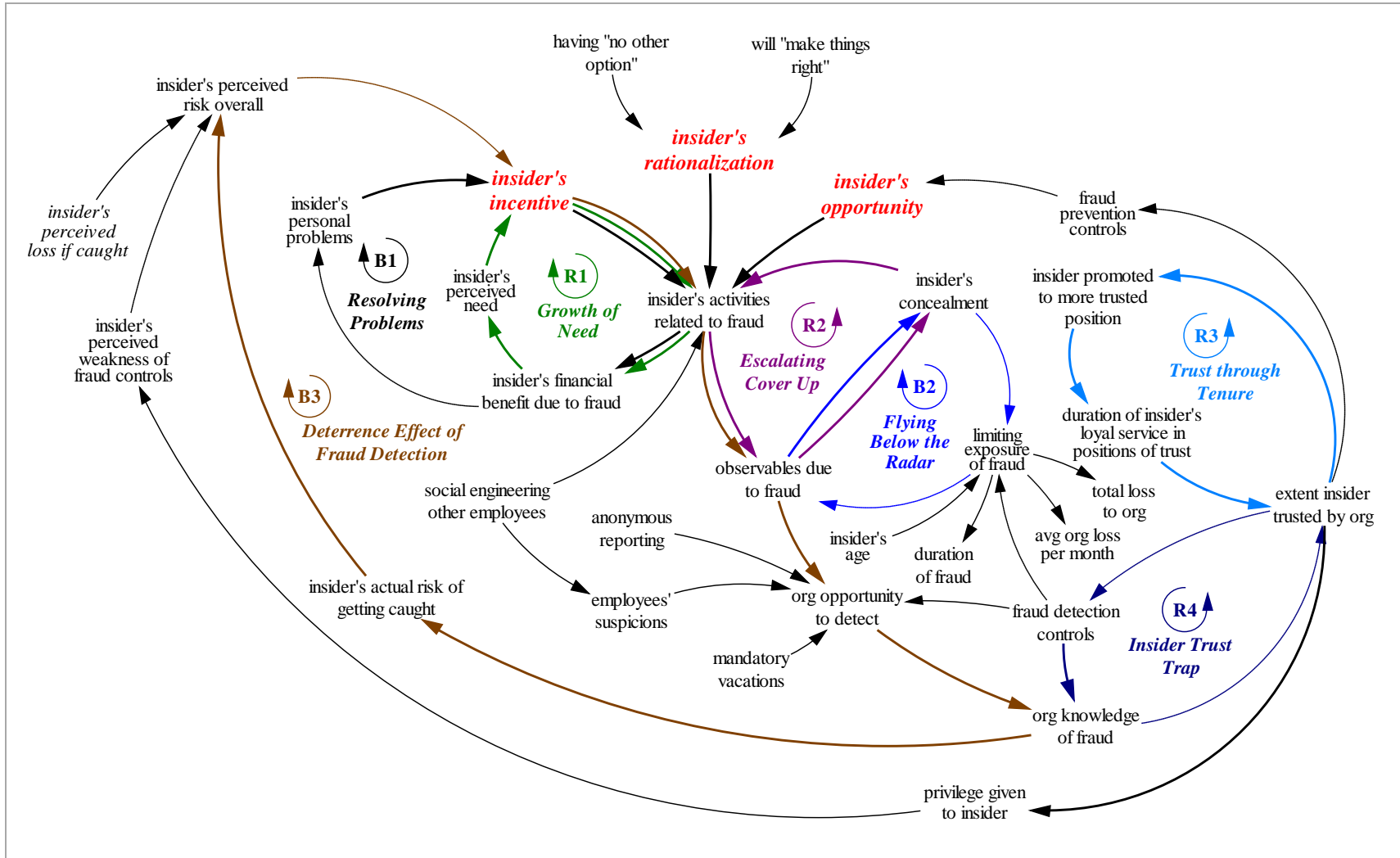


Figure 15: Manager Model

The model includes the following significant feedback loops:

- *Resolving Problems* (loop B1, in black) and *Growth of Need* (loop R1, in green): The insider's primary motivation was financial gain to resolve a variety of personal problems. However, even if the insider's personal problems are resolved, the crime typically does not end. Fraud crimes are typically longer in duration than other types of insider crimes. The case data indicate that the average manager fraud spanned 33 months. Even if the fraud resolves the insider's original problems, the additional income is too great to resist and the fraud takes on a life of its own.
- *Escalating Cover-Up* (loop R2, in purple) and *Flying Below the Radar* (loop B2, in light blue): The victim organization may observe the insider's fraud activities if it looks in the right places. An insider's unexplained financial gain is a red flag. But insiders' online or social attempts to conceal their actions can provide the victim organization with further observables of an escalating cover-up. There is evidence in manager fraud cases that insiders were able to reduce the observables of their crime, and thus conceal their activities, by keeping the victim organization's per-month fraud losses low. While "flying below the radar" resulted in slower losses, the longer duration of these crimes led to greater losses by the victim organization.
- *Deterrence Effect of Fraud Detection* (loop B3, in brown): Observables provide an opportunity for a victim organization to detect insider fraud. Many cases involved managers socially engineering their subordinates to conduct activities that may have appeared to be legitimate but in fact contributed to the fraud. Irregularities in such requests could have raised the subordinates' suspicions. An anonymous reporting vehicle may have been all that was necessary to alert the victim organization to the fraudulent activities. Fraud-detection controls can increase an organization's knowledge of fraud and the chances of catching the fraudster. The greater strength the insider perceives in the controls, the greater risk the insider will perceive in perpetrating the fraud, which may be enough to deter the fraud altogether. Deterrence also depends on the insider's perceived loss if caught.
- *Trust through Tenure* (loop R3, in aqua) and *Insider Trust Trap* (loop R4, in dark blue): Managers committing fraud often had a significant period of loyal service to the victim organization prior to the crime. During this time, the managers gained prominence and a commensurate level of trust by others in the victim organization. Excessive trust can lead the victim organization (possibly inadvertently) to
  - disable fraud-detection controls, leading to reduced knowledge of fraud activities and even more trust in the insider (the *Insider Trust Trap*)
  - disable fraud-prevention controls, creating the opportunity to commit the fraud
  - increase the privilege given to the insider, giving him or her knowledge of potential weaknesses in the victim organization's fraud-control system
  - lead co-workers, especially subordinates, to ignore or fail to report behaviors considered policy violations

*Trust through Tenure* and the *Insider Trust Trap* can reduce an organization's ability to prevent, detect, and respond to fraud activities.

#### 4.4 Non-Manager Model

The system dynamics model of the non-manager, shown in Figure 16, shares much of the dynamics exhibited in feedback loops B1 (*Resolving Problems*, in black), R1 (*Growth of Need*, in green), and B3 (*Deterrence Effect of Fraud Detection*, in brown) of the manager model. According to the case data, non-managers were sometimes motivated to commit fraud by a need to help family or friends financially. Co-workers collaborating on joint tasks with the non-manager insiders, or simply working in close proximity, may suspect the insider of committing fraud. This contrasts with suspicions of managers, which are less likely to be raised by subordinates the insider has socially engineered to engage in activities that seem irregular.

The *Deterrence Effect on Fraud Detection* (loop B3, in brown) has two paths, one indicating organizational knowledge that comes from outsider facilitation of the fraud (e.g., through the discovery that employees have had their identities stolen) and one indicating knowledge coming directly from insider activities). The potential for detecting suspicious or malicious insider activities generally allows earlier detection of criminal activities than detecting outsider facilitation of the fraud, since outsider facilitation usually exhibits itself as identity crimes perpetrated using insider information. While organizations would like to prevent crimes before they happen, monitoring for the illicit use of the organization's information externally can limit damage if internal detection is insufficient to prevent it.

Additional aspects of the model include the *Growth of the Fraud Business* (loop R5, in navy blue) and the *Growing Pressure from Outsiders* (loop R6, in aqua). Outsiders' financial benefit from insider fraud encourages the outsiders to continue and perhaps increase their facilitation of the fraud activities. This increases the incentive for insiders to continue and perhaps grow their insider fraud activities. Further, when outsiders know the details of insider activities, the insiders may feel pressured to continue or grow their fraud activities even if they would prefer not to. Thus, this dynamic affects not only the insider's opportunity but their incentive as well.

Table 3 presents the primary differences between manager fraud and non-manager fraud.

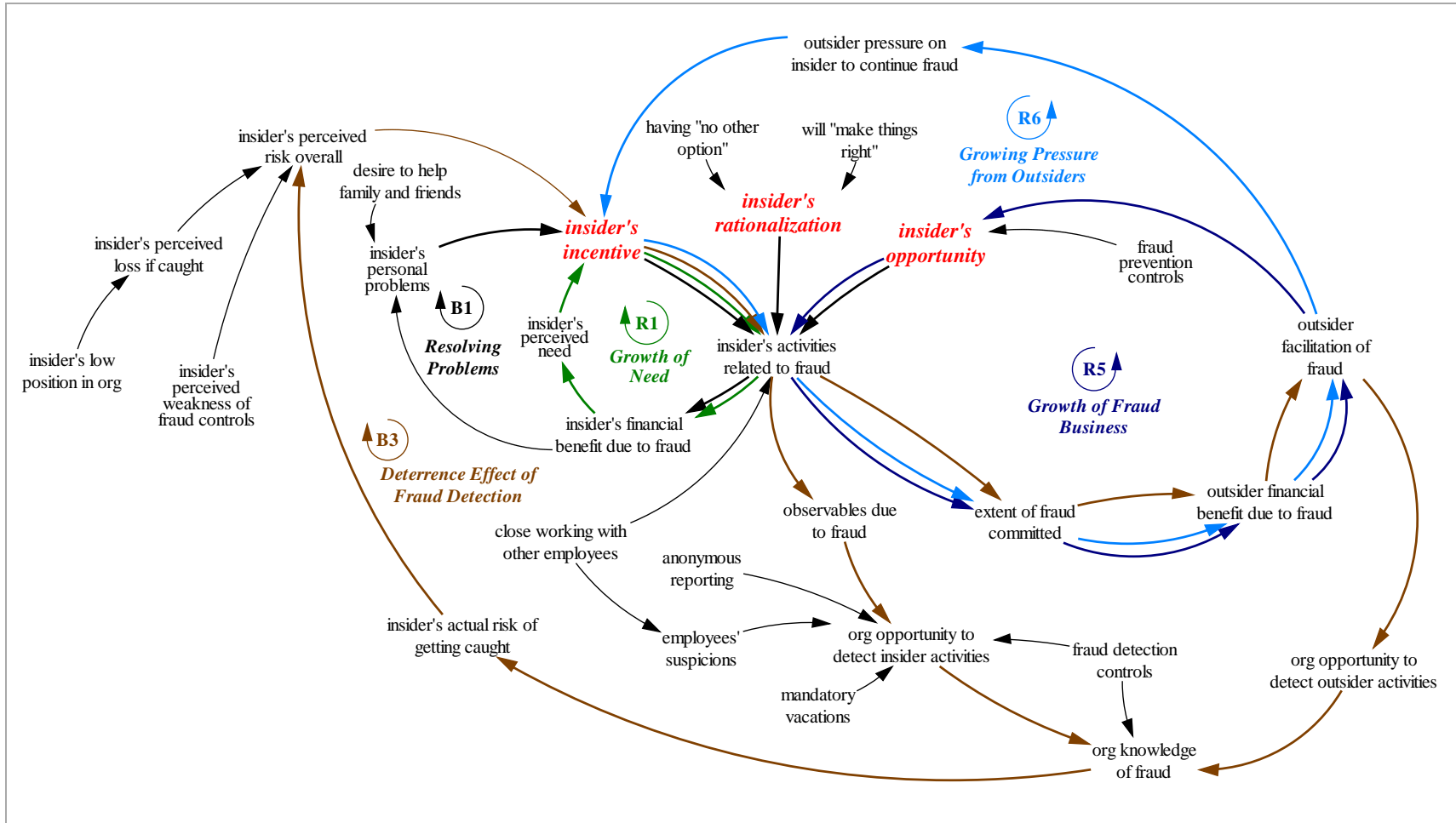


Figure 16: Non-Manager Model

Table 3: Comparison of Fraud by Managers and Non-Managers

| <b>Attribute</b>                             | <b>Manager Fraud</b>           | <b>Non-Manager Fraud</b>                         |
|--|--------------------------------|--|
| <b>Number of Cases</b>                       | 31                             | 30   |
| <b>Position Held</b>                         | branch manager, vice president | helpdesk employee, accountant, bank teller       |
| <b>Median Age</b>                            | 38                             | 31   |
| <b>Timeline</b>                              | extended duration              | comparatively short                              |
| <b>Origin of Trust</b>                       | period of loyal service        | inherent in duties and position                  |
| <b>Possible Source of Others' Suspicions</b> | subordinate social engineering | co-worker proximity to fraud acts                |
| <b>Outsider Facilitation</b>                 | nearly nonexistent             | financial source from perpetrated identity crime |
| <b>Concealment</b>                           | flying below the radar         | unsophisticated deceptions                       |

---

## 5 Strategies for Prevention, Detection, and Response

Because the majority of the incidents included in this study were categorized as insider fraud, this section focuses primarily on summarizing the technical and non-technical controls that may be effective in preventing, detecting, and responding to that activity. Organizations should, of course, remain concerned about IT sabotage and theft of IP, but this section focuses on the issues identified in Section 2 of this report. The CERT report, *Common Sense Guide to the Prevention and Detection of Insider Threats*, may provide useful guidance for addressing the wide range of threats posed by insiders [Cappelli 2009]. Table 4 below recaps the findings outlined in Section 2.<sup>10</sup>

Preventive controls for insider fraud should be designed to take away the insider's opportunity to commit the crime. (For more information, refer to Section 4.2, Fraud Triangle, on page 33.) For example, as part of the hiring process, in an attempt to reduce the number of high-risk employees entering the organization, an organization's Human Resource (HR) department often implements screening and identification of at-risk employees; this screening reduces the incidence of fraud. Individuals that have a criminal history of fraud may be more likely to commit fraud against their employer. Individuals with chronic financial problems may also be more at risk, as was evidenced in a number of incidents included in this study. In addition, financial problems sometimes arise years after an employee is hired; this suggests that for employees in positions that could commit fraud, financial organizations should consider repeating financial background investigations periodically—every three to five years.

Since fraud crimes often involved database transactions, either viewing or modifying data, some level of role-based access control or multi-person transaction verification may help to prevent some insider fraud crimes. These measures will make it more difficult to perpetrate the crime and may deter individuals from getting involved, or at least may make them think twice about it.

However, as evidenced in some of the cases in this study, motivated fraudsters may find ways around these measures. Cases exist in which insiders recruited others inside the victim organization precisely to get around role-based access controls. In addition, the crimes where managers were involved in the fraud scheme may have continued as long as they did because of the trust the victim organization had in the manager, which may have resulted in less monitoring of their online activity or auditing of their financial transactions. Therefore, for most organizations, detection of ongoing fraud activities is essential.

The fact that insider fraud crimes are often long and ongoing does not bode well for the victim organizations. However, it does afford the victim organization ample opportunity to discover the crime and possibly curtail the activity to limit damage. The goal is to prevent the unauthorized activity; but if that is not possible, then the organization should strive to detect it as early as possible to minimize damage.

---

<sup>10</sup> Many of the recommendations in this section are adapted from the book titled *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes* [Cappelli 2012].

There are two primary means for detecting insider fraud. The first is external discovery of the crime, potentially as a result of investigation into financial losses incurred by customers of the financial institution or noticed by law enforcement as it related to another criminal matter. In some of the incidents in this study, the actual fraud crime is conducted by an outsider to the victim organization, so they have a very limited ability to monitor and detect the crime. The second is the discovery of the internal crime (i.e., discovery of the malicious actions of the insider or accomplice). In these situations, the victim organization typically has an opportunity to detect the illicit insider activity at any point from planning, to insider recruitment, to execution.

*Table 4: Summary of Recommended Controls*

| <b>Practice Areas to Consider</b>   |  |
|---|--|
| <b>Finding 1: Criminals who executed a “low and slow” approach accomplished more damage and escaped detection for longer.</b>                   |  |
| Considerations  | Justification from Cases Studied   |
| 1. Consider fraud levels and durations when setting audit and investigation thresholds.   | The nature of the fraud levels and durations provide a potential benchmark timeline to members of the financial services community.  |
| 2. Consider policies and practices regarding the timing of employee assistance.   | Employee assistance offered when employees are facing difficult times may help resolve the employee’s issues or otherwise deter an employee from engaging in illegal acts.       |
| <b>Finding 2: Insiders did not generally have technical responsibilities.</b>   |  |
| Considerations  | Justification from Cases Studied   |
| 1. Consider good security principles regarding access control, least privilege, and separation of duties when developing policies and controls. | Restricting the level of employee access to that necessary to perform job duties may have limited or prevented the damage incurred in several of the cases.                      |
| 2. Consider all employees, regardless of their technical expertise, when defining security practices and controls.                              | Ill-intentioned employees will leverage the most easily exploitable vulnerabilities first, and often; such vulnerabilities are within the reach of most non-technical personnel. |
| <b>Finding 3: Fraud by managers differs substantially from fraud by non-managers by damage and duration.</b>                                    |  |
| Considerations  | Justification from Cases Studied   |
| 1. Consider auditing activities of accountants and managers on a more detailed level or a more frequent basis than other employees.             | Accountants and managers cause the most damage from insider fraud and evade detection for the longest amount of time.  |
| 2. Consider the enforceability of organizational policies; clearly communicate policies to all employees.                                       | Non-managers may be reluctant to report when their supervisors violate rules, especially in regard to exceptions to the usual process that seem innocent.                        |
| 3. Consider restricting the ability of employees to perform actions on their own, or a family member’s, account.                                | Several cases involved the use of an insider’s account, or that of a family member, in the perpetration of fraud.  |
| 4. Consider the need for access provided to those in senior or supervisory positions.   | Privileges often accumulate over years of employment without employee access being closely examined by the victim organization.  |

Table 4: Summary of Recommended Controls (continued)

| <b>Finding 4: Most cases do not involve collusion, but external collusion is much more common than internal collusion.</b>   |   |
|--|---|
| Considerations   | Justification from Cases Studied  |
| 1. Consider alerting employees to watch out for external parties who might want access to PII; educate employees on the penalties involved with illicit use of that information. | External parties were often involved as a conduit to sell stolen PII or pose as a legitimate account holder.  |
| <b>Finding 5: Most incidents were detected through an audit, customer complaints, or co-worker suspicions.</b>   |   |
| Considerations   | Justification from Cases Studied  |
| 1. Consider instituting an open and anonymous communication channel for employees to use if they have reason to suspect their co-workers of engaging in fraud.                   | Co-workers were unwittingly involved in activity related to the fraud. Co-worker suspicions, if reported, may have allowed the fraud to be detected earlier.                            |
| 2. Consider increasing the frequency of audits conducted in an impromptu fashion.  | While audits were often useful to detect fraudulent activity, greater frequency may have permitted earlier detection.   |
| <b>Finding 6: Personally identifiable information (PII) is a prominent target of those committing fraud.</b>   |   |
| Considerations   | Justification from Cases Studied  |
| 1. Consider access restrictions on workstations that process PII.  | Theft of PII often involved low-tech methods such as simple printing, screen captures, cutting and pasting into text files, or even copying PII to paper or reciting it over the phone. |
| 2. Consider increasing the frequency of audits conducted on information systems that process customer PII.   | While audits were often useful to detect fraudulent activity, greater frequency may have permitted earlier detection.   |
| 3. Consider performing analyses of fraud incidents to determine how to prevent or detect similar fraud crimes in the future.   | Gaps in an organization's fraud prevention and detection measures are apparent from the methods used by fraud perpetrators.   |

## 5.1 Behavioral and Business Process Recommendations

The following behavioral and/or business process recommendations are provided in response to the six findings described in Table 4. These recommendations are intended to be implemented in conjunction with other organization controls targeted at preventing, detecting, or responding to malicious insider activity. Be sure to consult with legal counsel prior to implementing any recommendations to ensure compliance with federal, state, and local laws.

### *Clearly document and consistently enforce policies and controls.*

Clear documentation and communication of technical and organizational policies and controls could have mitigated some of the insider incidents of fraud. Consistent policy enforcement is important; inconsistent policy enforcement may lead some employees to feel they are being treated differently than other employees and provide a potential motivation to retaliate against this perceived unfairness. Some insiders in this study were able to commit fraud against their organization due to inconsistent or unenforced policies and/or inconsistent monitoring and auditing of transactions.



***Institute periodic security awareness training for all employees.***

A culture of security awareness should be instilled in every organization so that all employees understand the need for policies, procedures, and technical controls. All employees must be made aware that security policies and procedures exist, that there is a good reason why they exist, that they must be enforced, and that there can be serious consequences for infractions. Employees also need to be aware that individuals, either inside or outside the organization, may try to co-opt them into activities that are counter to the organization's mission, including committing fraud. Each employee needs to understand the security policies and the process for reporting policy violations.

## **5.2 Monitoring and Technical Recommendations**

The following monitoring and technical recommendations are provided in response to the six findings described in Table 4. These recommendations are intended to be implemented in conjunction with other organization controls targeted at preventing, detecting, or responding to malicious insider activity. Be sure to consult with legal counsel prior to implementing any controls to ensure compliance with federal, state, and local laws.

***Include unexplained financial gain in any periodic reinvestigations of employees.***

Many organizations use screening mechanisms in their hiring process to determine the financial status of potential employees. This helps organizations to determine the trustworthiness of potential employees. However, few organizations do this on a regular basis after an employee is hired. If possible, organizations should institute a periodic reinvestigation process for employees in positions of trust. Attempts should be made to determine whether employees are under significant financial stress; such stress may make them more likely to participate in fraud or make them susceptible to recruitment into a fraud scheme. In addition to determining negative financial stressors, organizations should attempt to determine unexplained wealth or living beyond ones means since this may also indicate participation in a fraud scheme.

***Log, monitor, and audit employee online actions.***

If account and password policies and procedures are enforced, online actions can be associated with the employee who performed them. Logging, periodic monitoring, and auditing provide an organization the opportunity to discover and investigate suspicious insider actions before more serious consequences occur. Organizations can use data-leakage tools to detect unauthorized changes to the system and the downloading of confidential or sensitive information, such as IP, customer or client data, and PII.

***Pay special attention to accountants and managers.***

Instituting separation of duties into critical business processes is one way to prevent fraudulent transactions from occurring. In addition, in the event the separation of duties was unsuccessful at preventing suspicious events, audit programs can be put in place to identify such transactions. However, what if a manager or someone in the auditing or accounting process is also involved in a fraud scheme? Organizations should consider implementing processes that "check-the-checker," allowing an objective third party to verify the transactions of managers or others involved in a transaction's approval process. Finally, the auditing function in many organizations has become very predictable in terms of schedule, frequency, and what is audited. Instituting unpredictability into the auditing function may be a deterrent for some employees, including accountants, auditors, and managers, or others in positions of trust.

***Restrict access to PII.***

IT groups face the constant struggle of least privilege when managing access to digital assets. Many organizations struggle with identifying the organization's critical assets, determining where they are located, and deciding who should have access to them. All too often, organizations allow employees to accumulate privileges over time—privileges build up as users move across projects, between departments, or take new positions. To the best extent possible, employee privileges should be commensurate with the employee's current job responsibilities—the organization should strive to ensure that employees have appropriate privileges to do their job duties, but not more than they need. Having more privileges than necessary may provide an avenue for an employee to harm the organization. PII should always be treated as a critical asset. Protection strategies should be put in place to protect PII from unauthorized access, and controls should alert proper personnel when PII is accessed, modified, or transmitted within the organization as well as outside the organization.

***Develop an insider incident response plan.***

Organizations should develop an insider incident response plan to control the damage that results from malicious insider activity. This is challenging because the same people assigned to a response team may be the insiders who could use their knowledge of controls and skills against the organization. Only those responsible for carrying out the plan need to understand and be trained on its execution. Should an insider be suspected of committing fraud, it is important that the organization have evidence in hand to identify the insider and follow up appropriately. Lessons learned should be used to continually improve the plan.

---

## 6 Conclusion and Next Steps

This report describes six findings of a study of insider fraud in the U.S. Financial Services Sector:

- **FINDING ONE:** Criminals who executed a “low and slow” approach accomplished more damage and escaped detection for longer.
- **FINDING TWO:** Insiders’ means were not very technically sophisticated.
- **FINDING THREE:** Fraud by managers differs substantially from fraud by non-managers by damage and duration.
- **FINDING FOUR:** Most cases do not involve collusion.
- **FINDING FIVE:** Most incidents were detected through an audit, customer complaints, or co-worker suspicions.
- **FINDING SIX—**Personally identifiable information (PII) is a prominent target of those committing fraud.

The description of each finding includes frequency statistics on important aspects of the finding, case examples illustrating the finding, and preliminary recommendations. The recommendations discussed are fairly general in nature, but are the start of what we hope will be a fruitful discussion with organizations to elaborate what members of the financial services community should do in the face of these findings.

### 6.1 Considerations for Insider Threat Program Implementation

In their enterprise-wide risk assessments, organizations should consider the threat posed by insiders to the organization’s critical assets, people, technology, information, and facilities. The first step is to identify and prioritize assets, followed immediately by locating the critical assets and determining who has, or should have, authorized access. Many organizations fail during this step when they allow authorized access to extend beyond what is required for employees to fulfill their job responsibilities. Privileges tend to accumulate over time as employees migrate among departments and accept new job responsibilities. It is imperative that

- employees have only the appropriate privileges with critical assets
- employee privileges are known by the organization
- the organization can modify or disable access if an employee changes roles, responsibilities, or employment status

If an organization asks what an employee has access to or where critical assets exist when an employee is walking out the door, it is too late. Diligent access control to critical assets is essential and organizations should not allow this control to degrade over time; recovery from lapses in control can be time consuming.

Most organizations begin assessing an employee or contractor’s trustworthiness as part of the hiring process. Background checks, employment and personal references checks, and individual screenings are valuable; however, organizations should continue to assess trustworthiness after

the individual is hired. Organizations should regularly evaluate employees for potential motivators of malicious insider activity, including detecting the presence of financial and professional stressors and employee disgruntlement. Individuals showing such signs are at greater risk for committing a malicious act. Additionally, organizations should similarly scrutinize their contractors, subcontractors, suppliers, and other trusted business partners.

Finally, separation of duties is an effective way to prevent unauthorized transactions in financial systems. Organizations should extend the “separation of duties” model from their business process to their IT processes. There should not be a single point of failure in any IT operation. Also, when possible, more than one person should be required to complete critical IT functions, including creating and deactivating accounts and modifying privileges. Consistent enforcement of such monitoring and auditing strategies in critical business processes may help to prevent or detect malicious insider activity. Recall that approximately 50 percent of the fraud crimes included in this study was committed by someone in a management-related position; therefore, someone outside an employee’s management chain should audit such transactions. Organizations should implement the same type of consistent auditing in IT processes.

## 6.2 Identify Technical Gaps

Most organizations face the challenge of differentiating anomalous and normal network activity. Many IT tools exist to meet this challenge, but it takes significant effort to customize these tools to a specific organization’s business processes. In addition, organizations often struggle to determine and maintain baseline behavior at the individual level and scale it across the enterprise. It is time consuming to achieve a degree of confidence in distinguishing normal variations in baseline behavior from abnormal variations.

Relying on technical controls alone to differentiate anomalous but acceptable behavior from malicious behavior may not be the most effective way to address the threat posed by insiders. Organizations should consider combining the results of IT log aggregation and analysis tools with non-technical indicators that may be derived from internal and external data sources such as those listed below:

- results of employee and contractor performance management processes
- employee dispute resolution processes
- employee assistance processes
- credit rating systems
- law enforcement and criminal history databases
- facility-tracking systems

Such tools may help organizations to identify 1) individuals who are susceptible to recruitment into a fraud scheme and 2) disgruntled employees who may be more likely to sabotage an IT system or steal critical data when they leave.

The topic of employee monitoring draws together a mixture from different areas of the law, from labor to constitutional. As technology continues to evolve, legislators and the judiciary will continue to be confronted with new questions. Employers will need to keep a watchful eye on this process to avoid violating internal policy, regulatory requirements, or legal statutes. Collaboration

among staff, including legal staff, will widen your knowledge base and lead to a more informed set of policies and processes.<sup>11</sup>

### 6.3 Conclusion

As long as there are institutions that hold money, internal and external adversaries will make every attempt to subvert control mechanisms to illegally profit. To defeat those who are defrauding financial services companies, security professionals in this sector must master both the technical and behavioral aspects of the problem as well as ensure compliance with external regulators and internal governance initiatives, all while protecting their organizations' profits, shareholders, and customers. This report will not solve the problem entirely or give the financial sector a set of procedures guaranteed to prevent employees from conducting illegal activities. Rather, it paints a relatively complete picture of 80 recent cases of insider fraud and provides important insights into those cases.

The insider fraud models presented in this report round out the CERT series of insider threat models. Security professionals have used our previous models to establish countermeasures in dealing with insider IT sabotage, insider theft of IP, and national security espionage. We hope that these previous models and this new insider fraud model have a similar impact on the financial sector. Certainly the study of future cases may yield different insights, but we have found that our past models have stood the test of time. Although we published our other insider threat models quite some time ago (beginning in 2005), we have discovered that in the interim the overarching patterns in the cases have not changed.

We also hope this report will encourage the continued dialog between public, private, and research entities. Conversations about these findings will help us to learn even more and supplement the community's collective knowledge. The CERT Insider Threat Center has been conducting research into the problem of malicious insiders for more than a decade. In that time, we have seen progress in some areas of the problem; we have also seen other issues repeatedly resurface. Perhaps the most important message we can convey to those who are unfamiliar with the issue is that defeating insider threats is not solely the problem of IT, HR, or security—it's *everyone's* problem.

### 6.4 Next Steps

Upon publication of this report, the USSS and the CERT Insider Threat Center will present its findings at financial service sector venues as well as at Secret Service Electronic Crime Task Force (ECTF) chapter meetings across the country. We gladly accept comments and suggestions, which we may incorporate into an addendum to this report. We welcome ongoing feedback on any practices and technical solutions that members of the financial sector have implemented to successfully counter insider threats. Finally, we will attempt to answer any questions not covered in this report by querying and further analyzing our database of insider incidents. Contact us at [insider-threat-feedback@cert.org](mailto:insider-threat-feedback@cert.org).

---

<sup>11</sup> CERT Insider Threat Center internal publication.

---

## Appendix A: The Insider Threat Center at CERT

The text in this section was excerpted from the book titled *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)* [Cappelli 2012].

### The Software Engineering Institute's 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 percent 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).

While CERT continues to respond to major security incidents and analyze product vulnerabilities, the 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.

### The CERT Insider Threat Center

The CERT Insider Threat Center, part of the CERT Program, began research in 2000 and has continued to grow. The original insider threat research was sponsored by the U.S. Department of Defense (DoD) and focused on insider threats in the military services and defense agencies. The research ramped up in 2001, when the Secret Service National Threat Assessment Center (NTAC) and the CERT Insider Threat Center joined efforts to conduct a unique study of insider incidents. DHS S&T provided financial support for the completion of the study in 2003 and 2004. Four reports were produced as a result of that effort focusing on the banking and finance sector [Randazzo 2004], the information technology sector [Kowalski 2008a], the government [Kowalski 2008b], and the analysis of insider IT sabotage across all critical infrastructure sectors [Keeney 2005]. Since 2005, DHS Federal Network Security (FNS) has provided funding to allow CERT to continue its insider threat research.

The objective of the CERT Insider Threat Center is to assist organizations in preventing, detecting, and responding to insider compromises. The foundation of the work is the CERT database of more than 700 insider threat cases. System dynamics modeling is used 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 ex-

tension of the modeling efforts. In addition to the models, the team has developed an assessment framework, based on fraud, theft of intellectual property, and IT sabotage case data, to assist organizations in identifying their technical and non-technical 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 ongoing research.

---

## Appendix B: The Structure of the CERT Insider Threat Database

At a high level, the CERT insider threat database involves three entities: the organization(s) involved, the insider (subject), and the details of the incident. Figure 17 shows the primary relationships among these three entities.

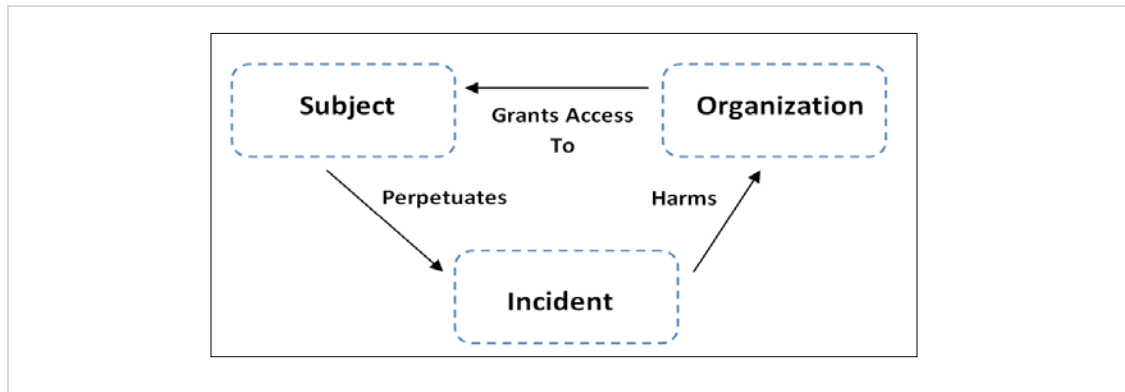


Figure 17: High-Level Structure of the CERT Insider Threat Database

### Organization Data

Multiple organizations can be involved in a single incident. An organization that is negatively impacted by an incident is designated as a victim organization. Incidents may also involve the victim organization's trusted business partner. In these incidents, the malicious insider is not directly employed by the victim organization, but is able to attack the victim organization via access authorized by a contractual relationship with the insider's employer.

Incidents, particularly those involving theft of IP, may also involve a beneficiary organization—an organization that knowingly or unknowingly benefits from the incident to the detriment of the victim organization. When entering case data into the CERT insider threat database, we identify the organization and any organizational issues relevant to the case, as shown in Table 5.<sup>12</sup>

---

<sup>12</sup> The tables in this appendix do not represent the CERT insider threat database's data dictionary. They merely provide insight into the type of information collected for each incident and a few sample values for each case.



Table 5: Organization Information Collected

| Organization Subcategory        | Information Collected in the Database  |
|---------------------------------|--|
| Organization Descriptors        | name, address, relation to insider   |
| Organization Type               | victim, beneficiary, trusted business partner, other   |
| Organization Description        | description of the organization  |
| Industry Sector                 | critical infrastructure sector of the organization   |
| Based in the United States?     | location of the organization; based in the united states?  |
| Organization Issues             | work environment, such as hostile work environment or culture of mistrust, and layoffs, mergers, and acquisitions, reorganizations, and other workplace events that may have contributed to an insider's decision to act   |
| Opportunity Provided to Insider | actions taken by an organization that may have contributed to the insider's decision to take action (such as demotions or transfers of employees); failure on the part of the organization to take action based on concerning behaviors or other events, actions, or conditions; or vulnerabilities, for example, insufficient monitoring of external access |

## Subject Data

We collect as many details as possible about the insider, including details regarding planning activities. These details are generally discovered after an incident has already occurred, but they are essential to preventing future insider threats. We also collect information about the insider's accomplices, including demographic data, the accomplice's relationship to the insider and the victim organization, and the accomplice's role in the incident.

We do not make any judgments about the insider or attempt to diagnose his or her behavior; we code exactly what we find in the source materials.

Table 6 describes the subject attributes in more detail.

Table 6: Subject Information Collected

| Subject Subcategory            | Information Collected in the Database   |
|--------------------------------|---|
| Descriptors                    | name, gender, age, citizenship, residence, education, employee title/type/status, departure date, tenure, access, position  |
| Motives and Unmet Expectations | motives (financial, curiosity, ideology, recognition, external benefit), unmet expectations (promotion, workload, financial, usage)   |
| Concerning Behaviors           | tardiness, insubordination, absences, complaints, drug/alcohol abuse, disgruntlement, co-worker/supervisor conflict, violence, harassment, poor performance, poor hygiene, etc. |
| Violation History              | security violations, resource misuse, complaints, deception about background  |
| Consequences                   | reprimands, transfers, demotion, HR reports, termination, suspension, access revocation, counseling   |
| Substance Abuse                | alcohol, hallucinogens, marijuana, amphetamines, cocaine, sedatives, heroin, inhalants  |
| Planning and Deception         | prior planning activities, explicit deceptions  |

## Incident Data

The information we collect about an incident includes individual actions taken to set up the attack, vulnerabilities exploited during the attack, steps taken to conceal it, the way the incident was detected, and the impact on the victim organization. In addition, we also collect data on the victim organization's response to the incident and events and conditions that may have contributed to an insider's decision to attack. Table 7 describes the incident attributes in more detail.

*Table 7: Incident Information Collected*

| <b>Incident Subcategory</b> | <b>Information Collected in the Database</b>  |
|-----------------------------|---|
| Case Summary                | incident dates, duration, prosecution   |
| Conspirators                | accomplices, type of collusion, relationships to insider  |
| Information Sources         | origin type   |
| Incident Chronology         | sequence, date, place, event  |
| Investigation and Capture   | how the insider was identified and caught   |
| Prosecution Result          | indictment, subject's story, sentence, case outcome   |
| Recruitment                 | outside/competitor induced, insider collusion, outsider collusion, acted alone, reasons for collusion   |
| IT Accounts Used            | subject's, organization's, system administrator's, database administrator's, co-worker's, authorized third party's, shared, back door   |
| Outcome                     | data copied/deleted/read/modified/created/disclosed, identity theft, creation of unauthorized document, denial of service   |
| Impact                      | description, financial  |
| How Detected                | software, information system, audit, non-technical, system failure  |
| Who Detected                | self-reported, it staff, other internal; customer, law enforcement, competitor, other external  |
| Log Files Used              | system files, email, remote access, internet service provider   |
| Who Responded               | incident response team, management, other internal  |
| Vulnerabilities Exploited   | sequence of exploit, description, vulnerability grouping  |
| Technical Methods           | technical methods used to set up and/or carry out the attack (e.g., hardware device, malicious code, modified logs, compromised account, sabotaged backups, modified backups) |
| Concealment Methods         | concealment methods used to hide technical and non-technical methods  |

---

## Appendix C: Other Insider Threat Concerns in the Financial Sector

No single pattern describes all malicious insider activity. The CERT Insider Threat Center's analysis of individual insider crimes has identified three distinct crime profiles, based on the motivations of the insider and the impact to the victim organization. This section compares insider crimes in the financial sector against our existing crime profiles and other types of insider crimes.

### Insider IT Sabotage in the Financial Services

*Insider IT sabotage is typically committed by technical users with privileged access, such as system administrators, database administrators, and programmers. The motivation in these crimes is usually revenge for a negative workplace event, and the crimes are often set up while still employed, but executed following termination. [Cappelli 2012]*

The crime of IT sabotage is typically motivated primarily by revenge against the victim organization for a perceived injustice done to the insider. Examples of perceived injustices, pulled from actual incidents in the CERT insider threat database, include

- being passed over for a promotion
- losing control of a critical system or application
- failure to receive a bonus or raise
- the hiring of a new supervisor
- demotions

When these insiders experienced some degree of unmet expectations, they typically became disgruntled. As the disgruntlement increased, they began to demonstrate non-technical observables in the workplace, such as conflicts with co-workers or supervisors, performance problems, and time and attendance problems. As victim organizations observed this behavior, they reprimanded the insiders, which, in many of the incidents, contributed to the escalation of the insider's disgruntlement and his or her decision to seek revenge against the victim organization by sabotaging a critical system, service, or data.

Disgruntlement is frequently exhibited in non-technical ways prior to the insider using technology to set up or carry out their attack. Once an insider decides to disrupt data or a critical system or service, he or she typically uses a privileged account to create an unknown access path into the victim organization's network. The unknown access paths can take the form of an unauthorized account, malicious code, or some other method of inflicting harm without detection. In most instances, insiders set up their attack prior to leaving the victim organization, often via remote access after normal working hours, and the impact to the victim organization is realized after voluntary or involuntary termination.

In our larger database of over 700 cases, there are 145 cases of IT sabotage and 15 of those were in the financial sector. Of the 80 incidents included in this study, 2 are categorized as IT sabotage. In both incidents, the insiders had been reprimanded for poor performance, the victim organiza-

tions attempted to implement sanctions to correct the behavior, the sanctions resulted in termination, and, prior to leaving the victim organization, the insiders set up their attack, which eventually disrupted a critical system or service. These two incidents are consistent with the MERIT model's description of IT sabotage [Moore 2008].

### **Insider Theft of IP in the Financial Services**

*Insider theft of intellectual property (IP) is usually committed by scientists, engineers, programmers, and salespeople. These insiders usually steal the information they worked on, and take it with them as they leave the victim organization to start their own business, take with them to a new job, or give to a foreign government or organization. [Cappelli 2012]*

The crime of IP theft is motivated primarily by the insider's desire to obtain or retain a competitive advantage as he or she leaves a victim organization to work for a competing organization, to start a competing organization, or to provide information to a foreign government or organization. While it could be argued that theft of IP benefits the insider financially, the insiders who take IP tend to have longer term aspirations than immediate financial gain. The crime allows the insider to advance his or her career.

The relevant cases in the CERT insider threat database indicate the following types of stolen IP [Cappelli 2012]:

- proprietary software and source code
- business plans, proposals, and strategic plans
- customer information
- product information (e.g., designs, formulas, schematics)

The insiders typically stole information to which they had regular, authorized access as part of their job responsibilities. Many of the insiders stole the information while at work and during normal working hours. These patterns make it very difficult for an organization to distinguish normal behavior from abnormal or illicit behavior.

Previous CERT research has identified two prominent types of IP thieves [Moore 2009]:

- *entitled independent*—An insider acting primarily alone to steal information to take to a new job or to his or her own side business. The entitled independent tends to believe that he or she owns the IP. This sense of ownership increases with the amount of time and effort the individual spends developing the IP. The insider usually has authorized access to the entire product suite or information. An event or condition in the workplace usually creates dissatisfaction on the part of the individual and increases his or her desire to leave and take information prior to departure.
- *ambitious leader*—A leader of an insider crime who recruits insiders to steal information for some larger purpose. Ambitious leaders are different from entitled independents in that they tend to not have authorized access to all the information they need, which is why they involve others in the scheme. A second difference is that ambitious leaders tend not to be dissatisfied with the victim organization. Instead they tend to steal the information primarily to benefit personally in a future business opportunity.

The majority of insiders who steal IP do so relatively close to announcing their resignation. This provides a window of opportunity for the victim organization to detect the unauthorized access or exfiltration of information.

In our database of over 700 cases, there are 98 cases of theft of IP and 11 of those were in the financial sector. Of the 80 incidents included in this study, only 1 is categorized as theft of IP. This incident involved two insiders, both of whom were dissatisfied with their jobs; one was unhappy with his compensation and the other no longer considered his job challenging. Both individuals resigned and went to work for a competitor, which the victim organization discovered only after their resignation. The victim organization became suspicious and conducted forensic examinations of the insiders' computers. They found that both individuals had downloaded all of the software modules for the victim organization's critical application. Both insiders fit the profile of an entitled independent.

### **Comparing Insider Fraud in the Financial Services to Other Insider Crimes**

The CERT Insider Threat Center defines insider fraud as 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 the theft of information that leads to an identity crime (e.g., identity theft, credit card fraud). The insider's potential for financial gain motivates these crimes. All incidents of insider fraud in the CERT insider threat database, across all sectors, and therefore including incidents not examined in this study, suggest the following pattern of behavior for this crime:

*Insider fraud is usually committed by non-managers such as help desk, customer service, and data entry clerks. The crimes are motivated by financial need or greed, and they typically continue for a long period of time. Many of these insiders are recruited by outsiders to steal information. Collusion with other insiders is very common in crimes involving modification of information for payment from the outside [Cappelli 2012].*

Insider fraud and insider theft of IP share many characteristics. Perpetrators of both types of fraud usually

- are current employees of the victim organization with authorized access at the time of the crime<sup>13</sup>
- target PII or customer information
- tend to commit their crimes while at work and during normal working hours
- are assisted by outsiders a minority of the time. In about one-third of fraud cases and 44 percent in the theft of IP cases, outsiders had recruited the insider to commit the crime [Cappelli 2012].
- colluded with one or more individuals in the victim organization in nearly half the fraud and IP theft incidents in the database. We speculate that insider crimes often require collusion to

---

<sup>13</sup> This pattern differs from insiders who commit IT sabotage, who are typically former employees without authorized access.

overcome the separation of duties that organizations enforce in attempts to prevent insider crime.

The incidents of insider fraud examined in this study differed starkly from the overall behavioral pattern of insider fraud in one respect. Whereas insider fraudsters are typically non-managers, approximately half of the cases examined in this study involved insiders in a managerial position, including account manager, customer service manager, branch manager, operations manager, assistant manager, vice president, senior vice president, and president.

---

## Bibliography

URLs are valid as of the publication date of this document.

### [AICPA 2002]

American Institute for CPA. *Consideration of Fraud in a Financial Statement Audit* (AU 316.02). American Institute for CPA, 2002. <http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00316.pdf>

### [Band 2006]

Band, S. R.; Cappelli, Dawn; Fischer, Lynn F.; Moore, Andrew P.; Shaw, Eric D. & Trzeciak, Randall F. *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis* (CMU/SEI-2006-TR-026). Software Engineering Institute, Carnegie Mellon University, 2006. <http://www.sei.cmu.edu/library/abstracts/reports/06tr026.cfm>

### [Cappelli 2006]

Cappelli, D. M.; Desai, Akash, G.; Moore, Andrew P.; Shimeall, Timothy J.; Weaver, Elise A.; & Willke, Bradford J. "Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information, Systems, or Networks." *Proceedings of the 24th International System Dynamics Conference*. Nijmegen, The Netherlands, July 23-27, 2006. <http://www.systemdynamics.org/conferences/2006/proceed/papers/MOORE333.pdf>

### [Cappelli 2009]

Cappelli, D. M.; Moore, A. P.; Trzeciak, R. F.; & Shimeall, T. J. *Common Sense Guide to Prevention and Detection of Insider Threat, 3rd Edition—Version 3.1*. Software Engineering Institute, Carnegie Mellon University and CyLab, 2009. <http://www.cert.org/archive/pdf/CSG-V3.pdf>

### [Cappelli 2012]

Cappelli, D. M.; Moore, A. P.; & Trzeciak, R. F. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Addison-Wesley, 2012. <http://www.sei.cmu.edu/library/abstracts/books/9780321812575.cfm>

### [Caputo 2009a]

Caputo, D. D.; Stephens, G. D.; & Maloof, M. A. "Detecting Insider Theft of Trade Secrets." *IEEE Security and Privacy* 7, 6 (November/December 2009): 14-21. <http://www.computer.org/csdl/mags/sp/2009/06/msp2009060014-abs.html>

### [Caputo 2009b]

Caputo, D.; Stephens, G.; Stephenson, B.; & Kim, M. *Human Behavior, Insider Threat, and Awareness: An Empirical Study of Insider Threat Behavior* (Research Report No. 16). Institute for Information Infrastructure Protection, MITRE Corporation, July 31, 2009. [http://www.mitre.org/work/tech\\_papers/2010/09\\_3130/09\\_3130.pdf](http://www.mitre.org/work/tech_papers/2010/09_3130/09_3130.pdf)

### [Charney 2010]

Charney, D. L. "True Psychology of the Insider Spy." *Intelligencer: Journal of the U.S. Intelligence Studies* 18, 1 (Fall/Winter 2010): 47-54.

**[Cressey 1974]**

Cressey, D. R. *Other People's Money*. Wadsworth, 1974. <http://www.amazon.com/Other-Peoples-Money-Embezzlement-ethnography/dp/0534001424>

**[CSO 2011]**

*CSO Magazine*, U.S. Secret Service, Software Engineering Institute, and Deloitte. *2011 Cybersecurity Watch Survey: Organizations Need More Skilled Cyber Professionals to Stay Secure*, 2011. <http://www.cert.org/archive/pdf/CyberSecuritySurvey2011.pdf>

**[Favere-Marchesi 2009]**

Favere-Marchesi, M. "Cognitive Effects of Decomposition on Fraud-Risk Assessments." *Proceedings of the 2009 Canadian Academic Accounting Association (CAAA) Annual Conference*. Montreal, Quebec, June 2009. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1325853](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1325853)

**[Fischer 2003]**

Fischer, L. F. "Characterizing Information Systems Insider Offenders," 289-296. *Proceedings of the 45<sup>th</sup> Annual International Military Testing Association Conference*. Pensacola, FL, November 3-6, 2003. <http://www.internationalmta.org/2003/2003Proceedings/03IMTAproceedings.pdf>

**[Hanley 2009]**

Hanley, Michael; Moore, Andrew P.; Cappelli, Dawn M.; & Trzeciak, Randall F. *Spotlight On: Malicious Insiders with Ties to the Internet Underground Community*. Software Engineering Institute and CyLab, Carnegie Mellon University, 2009. <http://www.cert.org/archive/pdf/CyLab%20Insider%20Threat%20Quarterly%20on%20Internet%20Underground%20-%20March%202009P.pdf>

**[Herbig 2002]**

Herbig, K. L. & Wiskoff, M. *Espionage Against the United States by American Citizens 1947-2001* (Technical Report 02-5). Defense Personnel Security Research Center, July 2002. <http://www.fas.org/sgp/library/spies.pdf>

**[Kaarbo 1999]**

Kaarbo, J. & Beasley, R. "A Practical Guide to the Comparative Case Study Method in Political Psychology." *Political Psychology* 20, 2 (June 1999): 369-391. <http://onlinelibrary.wiley.com/resolve/doi?DOI=10.1111/0162-895X.00149>

**[Keeney 2005]**

Keeney, M. M.; Kowalski, Eileen; Cappelli, Dawn; Moore, Andrew; Shimeall, Timothy; & Rogers, Stephanie. *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*. Software Engineering Institute and United States Secret Service, May 2005. <http://www.cert.org/archive/pdf/insidercross051105.pdf>

**[Kowalski 2008a]**

Kowalski, E.; Cappelli, D. M.; & Moore, A. P. *Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector*. Software Engineering Institute and United States Secret Service, January 2008. [http://www.cert.org/archive/pdf/insidertreat\\_it2008.pdf](http://www.cert.org/archive/pdf/insidertreat_it2008.pdf)



**[Kowalski 2008b]**

Kowalski, E.; Conway, Tara; Keverline, Susan; Williams, Megan; Cappelli, Dawn; Willke, Bradford; Moore, Andrew. *Insider Threat Study: Illicit Cyber Activity in the Government Sector*. Software Engineering Institute and United States Secret Service, January 2008. [http://www.cert.org/archive/pdf/insidethreat\\_gov2008.pdf](http://www.cert.org/archive/pdf/insidethreat_gov2008.pdf)

**[Maybury 2005]**

Maybury, M., et al. "Analysis and Detection of Malicious Insiders." *Proceedings of the 2005 International Conference on Intelligence Analysis*. McLean, VA, May 2-6, 2005. [http://www.mitre.org/work/tech\\_papers/tech\\_papers\\_05/05\\_0207/index.html](http://www.mitre.org/work/tech_papers/tech_papers_05/05_0207/index.html)

**[Moore 2009]**

Moore, A. P.; Cappelli, Dawn M.; Caron, Thomas C.; Shaw, Eric; & Trzeciak, Randall F. "Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model," 1-21. *Proceedings of the First International Workshop on Managing Insider Security Threats (MIST 2009)*. West Lafayette, IN, June 15-19, 2009. [http://www.cert.org/insider\\_threat/docs/Insider\\_Theft\\_of\\_IP\\_Model\\_MIST09.pdf](http://www.cert.org/insider_threat/docs/Insider_Theft_of_IP_Model_MIST09.pdf)

**[Moore 2008]**

Moore, A. P.; Cappelli, D. M.; & Trzeciak, R. F. *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures* (CMU/SEI-2008-TR-009). Software Engineering Institute, Carnegie Mellon University, 2008. <http://www.sei.cmu.edu/library/abstracts/reports/08tr009.cfm>

**[Mount 2006]**

Mount, M.; Ilies, R. & Johnson, E. "Relationship of Personality Traits and Counterproductive Work Behaviors: The Mediating Effects of Job Satisfaction." *Personnel Psychology* 59, 3 (2006): 591-622. <http://onlinelibrary.wiley.com/doi/10.1111/j.1744-6570.2006.00048.x/abstract>

**[Nykodym 2005]**

Nykodym, Nick; Taylor, Robert; & Vilela, Julia. Criminal Profiling and Insider Cyber Crime. *Digital Investigation* 2, 4: 261-267 (2005). <http://www.sciencedirect.com/science/article/pii/S1742287605000915>

**[O'Gara 2004]**

O'Gara, J. D. *Corporate Fraud: Case Studies in Detection and Prevention*. Wiley, 2004. <http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471493503.html>

**[Predd 2008]**

Predd, J.; Pflieger, S.; Hunker, J.; & Bulford, C. "Insiders Behaving Badly." *IEEE Security and Privacy* 6, 4 (July 2008): 66-70. <http://www.computer.org/csdl/mags/sp/2008/04/msp2008040066-abs.html>

**[Randazzo 2004]**

Randazzo, M. R., et al. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector* (CMU/SEI-2004-TR-021). Software Engineering Institute, Carnegie Mellon University, 2004. <http://www.sei.cmu.edu/library/abstracts/reports/04tr021.cfm>

**[Rich 2005]**

Rich, E., et al. (July 2005). "Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model." *Proceedings of the 23rd International Conference of the System Dynamics Society*. Boston, MA, July 17-21, 2005.

[http://www.cert.org/insider\\_threat/docs/insider\\_threatISDC2005.pdf](http://www.cert.org/insider_threat/docs/insider_threatISDC2005.pdf)

**[Sackett 2002a]**

Sackett, P. R. "The Structure of Counterproductive Work Behaviors: Dimensionality and Relationships with Facets of Job Performance." *International Journal of Selection and Assessment* 10, 1-2 (March/June 2002): 5-11. <http://onlinelibrary.wiley.com/doi/10.1111/1468-2389.00189/abstract>

**[Sackett 2002b]**

Sackett, P. R. & DeVore, C. J. Ch. 8, "Counterproductive Behaviors at Work," 145-164. *Handbook of Industrial, Work and Organizational Psychology, Volume 1: Personnel Psychology*. Edited by N. Anderson; D. S. Ones; H. K. Sinangil; & C. Viswesvaran. SAGE Publications Ltd., 2002. <http://www.uk.sagepub.com/books/Book209714>

**[Salgado 2002]**

Salgado, J. F. "The Big Five Personality Dimensions and Counterproductive Behaviors." *International Journal of Selection and Assessment* 10, 1-2 (March 2002): 117-125.

<http://onlinelibrary.wiley.com/doi/10.1111/1468-2389.00198/abstract>

**[Shaw 2006]**

Shaw, E. D. "The Role of Behavioral Research and Profiling in Malicious Cyber Insider Investigations." *Digital Investigation* 3, 1 (March 2006): 20-31. <http://www.sciencedirect.com/science/article/pii/S1742287606000090>

**[Shaw 2005]**

Shaw, E. & Fischer, L. G. *Ten Tales of Betrayal: The Threat to Corporate Infrastructure by Information Technology Insiders* (Technical Report A392144). Defense Personnel Security Research Center, 2005. <http://www.dhra.mil/perserec/reports/tr05-13.pdf>

**[Shaw 1998]**

Shaw, E.; Ruby, K. G.; & Post, J. M. "The Insider Threat to Information Systems: The Psychology of the Dangerous Insider." *Security Awareness Bulletin*, 2-98 (1998): 27-46.

<http://home.engineering.iastate.edu/~guan/course/CprE-536/paperreadinglist606/profiling/sab.pdf>

**[Stamper 2002]**

Stamper, C. L. & Masterson, S. S. "Insider or Outsider? How Employee Perceptions of Insider Status Affect their Work Behavior." *Journal of Organizational Behavior*, 23 (2002): 875-894.

<http://onlinelibrary.wiley.com/doi/10.1002/job.175/abstract>

**[Sterman 2000]**

Sterman, J. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Irwin McGraw-Hill, 2000. <http://www.amazon.com/Business-Dynamics-Systems-Thinking-Modeling/dp/007238915X>

**[Strauss 1998]**

Strauss, A. L. & Corbin, J. M. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Sage Publications, 1998.  
<http://www.sagepub.com/books/Book226809>

**[USSS 2010]**

United States Secret Service. *Criminal Investigations*.  
<http://www.secretservice.gov/criminal.shtml> (2010)

**[Verizon 2011]**

Verizon. *2011 Data Breach Investigations Report*. Report of the Verizon Risk Team with Cooperation from the U. S. Secret Service and the Dutch High Tech Crime Unit, (2011).  
[http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2011\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf)

**[Weiland 2010]**

Weiland, Robert M.; Moore, Andrew P.; Cappelli, Dawn M.; Trzeciak, Randall F.; & Spooner, Derrick. *Spotlight On: Insider Threat from Trusted Business Partners*. Software Engineering Institute and CyLab, Carnegie Mellon University, 2010.  
<http://www.cert.org/archive/pdf/TrustedBusinessPartners0210.pdf>

**[Wilks 2004]**

Wilks, T. Jeffrey & Zimbelman, Mark F. "Decomposition of Fraud Risk Assessments and Auditors' Sensitivity to Fraud Cues." *Contemporary Accounting Research* 21, 3 (Fall 2004): 719–45.  
<http://onlinelibrary.wiley.com/doi/10.1506/HGXP-4DBH-59D1-3FHJ/abstract?systemMessage=Wiley+Online+Library+will+be+disrupted+21+May+from+10-12+BST+for+monthly+maintenance>

**[Wilks 2002]**

Wilks, T. Jeffrey & Zimbelman, Mark F. "The Effects of a Fraud-Triangle Decomposition of Fraud Risk Assessments on Auditors' Sensitivity to Incentive and Opportunity Cues," 57 – 59. *Proceedings of the 15th University of Illinois Symposium on Auditing Research*. Urbana-Champaign, IL, October 2002. University of Illinois at Urbana-Champaign, 2002.  
[http://www.business.illinois.edu/accountancy/events/symposium/audit/proceedings/proceedings\\_2002.pdf](http://www.business.illinois.edu/accountancy/events/symposium/audit/proceedings/proceedings_2002.pdf)

**[Yin 2009]**

Yin, R. K. *Case Study Research: Design and Methods*. Sage Publications, Inc., 2008 (ISBN-10: 1412960991). <http://www.sagepub.com/books/Book232182>

| <b>REPORT DOCUMENTATION PAGE</b>   |  |   | <i>Form Approved</i><br><i>OMB No. 0704-0188</i> |  |
|--|--|---|--|--|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.   |  |   |  |  |
| 1. AGENCY USE ONLY<br>(Leave Blank)  | 2. REPORT DATE<br>July 2012                              | 3. REPORT TYPE AND DATES COVERED<br>Final                       |  |  |
| 4. TITLE AND SUBTITLE<br>Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector  |  | 5. FUNDING NUMBERS<br>FA8721-05-C-0003                          |  |  |
| 6. AUTHOR(S)<br>Adam Cummings; Todd Lewellen; David McIntire; Andrew P. Moore; & Randall Trzeciak  |  |   |  |  |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>Software Engineering Institute<br>Carnegie Mellon University<br>Pittsburgh, PA 15213   |  | 8. PERFORMING ORGANIZATION REPORT NUMBER<br>CMU/SEI-2012-SR-004 |  |  |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)<br>HQ ESC/XPK<br>5 Eglin Street<br>Hanscom AFB, MA 01731-2116  |  | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER                  |  |  |
| 11. SUPPLEMENTARY NOTES  |  |   |  |  |
| 12A DISTRIBUTION/AVAILABILITY STATEMENT<br>Unclassified/Unlimited, DTIC, NTIS  |  | 12B DISTRIBUTION CODE   |  |  |
| 13. ABSTRACT (MAXIMUM 200 WORDS)<br>This report describes a new insider threat study funded by the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) in collaboration with the U.S. Secret Service (USSS) and the CERT Insider Threat Center, part of Carnegie Mellon University's Software Engineering Institute. Researchers extracted technical and behavioral patterns from 67 insider and 13 external fraud cases; all 80 cases occurred between 2005 and the present. Using this information, we developed insights and risk indicators of malicious insider activity within the banking and finance sector. This information is intended to help private industry, government, and law enforcement more effectively prevent, deter, detect, investigate, and manage insider threats in this sector. |  |   |  |  |
| 14. SUBJECT TERMS<br>Insider threat, financial services  |  | 15. NUMBER OF PAGES<br>76                                       |  |  |
| 16. PRICE CODE   |  |   |  |  |
| 17. SECURITY CLASSIFICATION OF REPORT<br>Unclassified  | 18. SECURITY CLASSIFICATION OF THIS PAGE<br>Unclassified | 19. SECURITY CLASSIFICATION OF ABSTRACT<br>Unclassified         | 20. LIMITATION OF ABSTRACT<br>UL                 |  |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18  
298-102