NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

TRUSTED INSIDERS ARE COMMITTING FRAUD AND EMBEZZLEMENT WITHIN ORGANIZATIONS: IS THERE A CONNECTION TO ADDICTION, AS THE MOTIVATING FACTOR FOR THEIR ILLEGAL ACTIVITIES?

by

Paul R. Johnson

June 2014

Thesis Co-Advisors: David Brannan
Kathleen Kiernan

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
TRUSTED INSIDERS ARE COMMITTING FRAUD AND EMBEZZLEMENT WITHIN ORGANIZATIONS: IS THERE A CONNECTION TO ADDICTION, AS THE MOTIVATING FACTOR FOR THEIR ILLEGAL ACTIVITIES?

5. FUNDING NUMBERS

6. AUTHOR(S) Paul R. Johnson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Extensive studies and research have been conducted on insider threats, the possible causes, predictive models and best practices for prevention, early detection, and mitigation of the threats of insider attacks to a wide range of critical infrastructure, government agencies, and the private sector. Current research shows a great deal of attention directed at the cyber threats toward organizations.

In contrast, relatively little research has been conducted on the insider threat with regard to financial fraud and embezzlement to organizations. Left undetected, insiders can cause irreparable and devastating consequences to private and public sector organizations, which compromise the integrity of the overall financial system. Recent criminal cases have revealed a disturbing trend linking many of the trusted insiders convicted of conducting fraud or embezzlement within the victim organizations to an addiction to gambling or prescription drugs. Also alarming is the frequency of trusted insiders conducting fraud within government agencies to support their addiction. This paper studies research on insider threats, and suggests that addiction is a contributing factor to the motives of the insiders' criminal behaviors. Research also suggests that accurate reporting by law enforcement agencies is not occurring in police reports on motives or causes of the reasons insiders are committing their crimes.

14. SUBJECT TERMS
Insider Threats, Insider Attacks, Fraud, Embezzlement, Financial Crimes, Gambling Addiction, Pain Prescription Medication Addiction, U. S. Secret Service, Case Studies

15. NUMBER OF PAGES
155

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

TRUSTED INSIDERS ARE COMMITTING FRAUD AND EMBEZZLEMENT WITHIN ORGANIZATIONS: IS THERE A CONNECTION TO ADDICTION, AS THE MOTIVATING FACTOR FOR THEIR ILLEGAL ACTIVITIES?

Paul R. Johnson
Special Agent in Charge, United States Secret Service
Louisville Field Office, Louisville, KY
B.S., Bemidji State University, 1981

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
June 2014

Author: Paul R. Johnson

Approved by: Dr. David Brannan
Thesis Co-Advisor

Dr. Kathleen Kiernan
Thesis Co-Advisor

Mohammed M. Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Extensive studies and research have been conducted on insider threats, the possible causes, predictive models and best practices for prevention, early detection, and mitigation of the threats of insider attacks to a wide range of critical infrastructure, government agencies, and the private sector. Current research shows a great deal of attention directed at the cyber threats toward organizations.

In contrast, relatively little research has been conducted on the insider threat with regard to financial fraud and embezzlement to organizations. Left undetected, insiders can cause irreparable and devastating consequences to private and public sector organizations, which compromise the integrity of the overall financial system. Recent criminal cases have revealed a disturbing trend linking many of the trusted insiders convicted of conducting fraud or embezzlement within the victim organizations to an addiction to gambling or prescription drugs. Also alarming is the frequency of trusted insiders conducting fraud within government agencies to support their addiction. This paper studies research on insider threats, and suggests that addiction is a contributing factor to the motives of the insiders' criminal behaviors. Research also suggests that accurate reporting by law enforcement agencies is not occurring in police reports on motives or causes of the reasons insiders are committing their crimes.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACFE	Association of Certified Fraud Examiners
CDC	Centers for Disease Control and Prevention
CERT	Computer Emergency Response Team
CFO	chief financial officer
CHDS	Center for Homeland Defense and Security
DHS	Department of Homeland Security
DOD	Department of Defense
FBI	Federal Bureau of Investigation
FFRDC	funded research and development center
GA	Gamblers Anonymous
ICD	impulse control disorders
IP	intellectual property
IT	information technology
KSP	Kentucky State Police
LEA	law enforcement agency
MNO	Management and Organization Division
MO	modus operandi
NIBRS	National Incident-Based Reporting System
NRC	National Research Council
NSA	National Security Agency
NTAC	National Threat Assessment Center
PERSEREC	Defense Personnel Security Research Center
PII	personally identifiable information
SRS	Summary Reporting System
U.S.	United States
UCR	Uniformed Crime Report
USAO	U. S. Attorney's Office
USSS	U.S. Secret Service

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

> Trusted insiders are committing fraud and embezzlement within organizations: Is there a connection to addiction, as the motivating factor for their illegal activities?

Insider threats pose hazards to private industry, critical infrastructure, and government organizations. Threats include financial loss, security breaches, and a loss of confidence in the integrity and operations of all manner of institutions at which trusted insiders have access to controlled or restricted materials, including money. Research conducted on organizational insider threats and their possible causes have neglected a potentially useful aspect of investigation practices that could significantly mitigate the insider threat. Predictive modeling presented in this thesis proposes the creation of new means to mitigate threats of this nature. Current research directs a great deal of attention to cyber threats. Comparatively scant attention to an enduring, existing threat from insiders can be increased, and should have a high payoff in fraud and embezzlement prevention.

To begin, compilation of evidence from 40 recent criminal fraud and embezzlement cases involving trusted insiders, from four U.S. Secret Service field offices in Louisville, Cincinnati, Memphis, and Nashville revealed a disturbing, yet useful trend: most of the trusted insiders convicted of fraud or embezzlement were also addicted to gambling or to pain prescription medication. This high correlation between fraud and addictive behavior is the basis for the recommendations in this study. All cases reviewed for this research were closed and adjudicated—the total number of white-collar perpetrators included in the study is forty-five. Even though the information can be readily obtained through questioning and during the course of routine investigation, motives for illegalities by trusted insiders committing fraud and embezzlement often are omitted as unnecessary. Since they are not required to include that information in the record, law enforcement officials are not properly and uniformly recording the motives of these criminals. Motives matter because, armed with these data that drive behavior, private, non-profit, as well as public sector organizations, and law enforcement can be in a better position to predict, and therefore prevent, insider crimes with increased efficacy.

Consider this histogram in Figure 1, which is based on 10 years of case studies. Numbers indicate clearly that fraud and embezzlement cases from the four Midwest Secret Service field offices are strongly linked with addictive behavior. It seems reasonable that this finding will hold true in other field offices across the country.

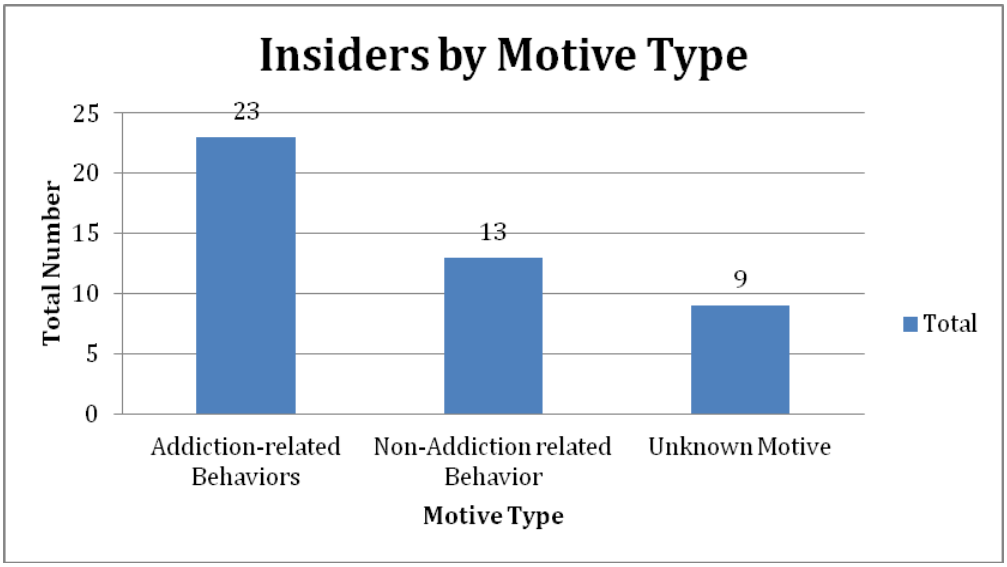

Figure 1. Secret Service Case Studies Showing Addiction Related Behavior in 23/45 Insiders Convicted of Fraud or Embezzlement

Given this obvious link between addictive-related behavior and white-collar crime, action is warranted. Approaching insider threat systematically requires a schema, and Dr. Donald Cressey provides a useful one.

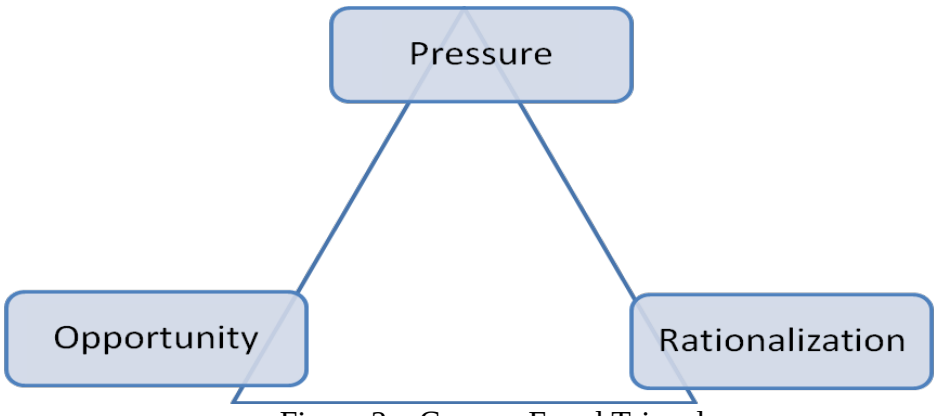

Figure 2. Cressey Fraud Triangle

The fraud triangle includes three contributing factors that encompass most criminal embezzlement actions: pressure to commit the offense, opportunity to commit the offense, and an excuse to rationalize the illegal behavior. This combination of factors, when acted upon, can compromise the integrity of a company, or of the entire financial system even when a single individual has earned trust and unfettered access to sensitive materials. Also alarming is the frequency of trusted insiders conducting fraud and embezzlement within government agencies to support their addiction(s). This paper studies research on insider threats, and suggests that addiction is a contributing factor to the motives of the insiders' criminal behavior.

Understanding sources of pressure, and recognizing when opportunity exists can help organizations and law enforcement officials intervene effectively to curb fraud and embezzlement before it occurs. Alertness can come in the form of recognition using existing cases, and the improved recording of motive in future cases, and paying especial attention to those cases in which addictive behavior is present.

Calculating the addiction rates for Americans is not an exact science; however, research indicates it is a significant cost to society. These statistics are collected in many ways by researchers; however, actual police statistics on reported crimes in which causality is a discernable item is clearly an area lacking a comprehensive method for accurate accounting. The lack of accurate statistics on the causality of crimes perpetrated because of an addiction is clearly an important measurement that researchers, criminologists, and homeland security officials should be able to capture. More compelling is the need for these same officials to be able to draw clear conclusions on accurate statistics surrounding causes and motives for not only fraud and embezzlement cases regarding trusted insiders, but additionally, all criminal acts reported to law enforcement. This lack of accurate reporting on causes and motives for criminal behavior indicates serious gaps in the overall crime reporting in this country, and a gap analysis including the comprehensive examination of motivating causes of crime, to include addiction is warranted.

Ultimately, what this study proposes is a multi-faceted approach to insider threats: accurate recording of motive in criminal cases, and promulgation of those reports to U.S.

law enforcement and homeland security stakeholders charged with the task of reducing insider threats. Specifically, knowledge afforded by this research indicates that the following entities should take specific actions:

U.S. SECRET SERVICE

Initially, future research should begin with the author's own agency, the U.S. Secret Service (USSS). As indicated in this thesis, the USSS investigates thousands of financial crimes cases each year, and more specifically, investigates hundreds of cases under the category of fraud, embezzlement and miss-appropriation, which is most closely aligned to trusted insiders committing fraud and embezzlement within organizations.

The USSS would be an excellent federal agency to conduct an in-depth case review of all its closed fraud, embezzlement, and misappropriation cases investigated in the last five years, to determine and document the trusted insiders' motive or causality of the criminal behavior. The USSS could take the lead in research as a federal agency under the Department of Homeland Security (DHS) that has a primary mandate to investigate complex financial crimes cases. The USSS could provide a comprehensive analysis of causation and motives for trusted insiders committing fraud and embezzlement against organizations. This documentation could provide valuable data to researchers on the ausation of financial crimes cases. This information would also provide an opportunity to determine what if any effect addiction plays in determining insider's motive for conducting their illegal activity.

KENTUCKY STATE POLICE

The Kentucky State Police (KSP) is the primary police records retention and reporting agency for the Commonwealth of Kentucky. KSP would be an excellent state agency to take on the role of requiring its 400 city and county law enforcement agencies to document and record the causality and motives of crimes committed in Kentucky. KSP could serve as a model for other state police agencies that also record and provide police criminal records to the FBI and the Department of Justice through the Uniform Crime Report.

FBI AND DEPARTMENT OF JUSTICE

The Federal Bureau of Investigation (FBI) and the Uniform Crime Report, as well as the National Incident-Based Reporting System, should require law enforcement agencies to report causality and motives of criminal offenses in police reports. This information plays a key role in understanding not only why criminals are committing crime but also provides law enforcement agencies' and researchers' insight into how much addiction plays a role in criminal behavior.

Finally, people are an organization's greatest asset and most critical vulnerability. The key to reducing fraud and embezzlement is recognizing that all organizations must consider the very real challenge of defending against the insider threat with at least the level of attention paid to external threats. Prevention, detection, and mitigation strategies are paramount for any organization to have in place before the insider attack occurs. Excellent programs are available to organizations for training and education on the insider threat. A number of programs already exist concerning best practices that organizations of all sizes should adhere to and incorporate as a part of their internal security policies and procedures regarding potential insider compromises.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I would like to thank my incredible wife, Lisa; my son, David; and daughter, Casey, for their love, patience, support, and many heartfelt prayers during this very challenging journey. You have sacrificed so much during the many weeks that I have had to spend away from home, the hundreds (maybe thousands) of late-night hours that I stayed at work to write and create the seemingly endless assignments and school projects, the missed family dinners, sporting events, and bedtime stories. The family dining table and surrounding space often turned into my "mobile thesis command post and late night inspiration laboratory."

Without the encouragement of numerous senior leaders, colleagues, and friends, I would not have been able to balance my intense work demands of running a very active and robust Louisville Secret Service Field Office, travel, and family life during the past 21 months. I need to thank my office support supervisors for fulfilling the needs of the mission during my absences. I especially thank: Craig, "Boss you can do this," Paul, Kirk, and Miss Judy.

This incredible academic and life journey would not have been possible without the dedicated staff, alumni and students at the Naval Postgraduate School Center for Homeland Defense and Security (CHDS). I am grateful to Ellen Gordon and Heather Issvoran for encouraging me to apply for the master of arts program and take the next step in my CHDS journey after completing the Executive Leaders Program. I am indeed grateful for the wisdom and leadership of Dr. Chris Bellavita, who instilled in me a renewed passion for learning and the art and practice of critical thinking. A special thanks goes to Drs. David Brannan, Anders Strindberg, Richard Bergin, Rodrigo Nieto-Gomez, and Eric Dahl for pushing my limits of intellectual stimulation and moving me beyond my comfort zone of appreciative inquiry. To my faithful companions and teammates, Serge Potapov, Danielle Lehman, and Max Geron, thanks for always having my back. To Dawn Mehlhalf, my dear cohort tablemate and good friend, you had a deep and lasting impact on my life and your brilliant intellect and capacity for grasping complex thought patterns will be forever missed. I am deeply indebted to my thesis committee, Dr. David

Brannan and Dr. Kathleen Kiernan, whose combined enthusiasm, strategic vision, commitment to excellence, and attention to detail kept me motivated and on track. A special thanks goes out to Randy Trzeciak at the CERT Insider Threat Center for providing guidance and allowing for research on my thesis topic. I will always be indebted to the entire CHDS family for challenging me to think critically and strategically every day. Your selfless commitment to the safety and security of the United States is how I will forever define the homeland security professional and patriot.

Finally, I would like to thank the men and women of the United States Secret Service, whom I have had the distinct honor and privilege of serving with for well over a quarter of a century. Your dedication to country, honor, and duty, and providing protection to the president of the United States and world leaders, as well as the nation's financial infrastructure, clearly makes you "Worthy of Trust and Confidence."

I. INTRODUCTION

A. BACKGROUND AND PROBLEM SPACE

In 2009, a former mid-level tax office manager for the District of Columbia was convicted of issuing $48 million in bogus property tax refunds for herself and her co-conspirators, who included family, friends, and a collusive bank manager. Described as the largest and longest-running embezzlement scheme in the city's history, investigation revealed that loopholes in software and lax internal controls had allowed her to carry on undetected for nearly two decades.[1] Until her arrest, this trusted insider was a 26-year tax employee operating inside of her organization. "She was known among her colleagues as a problem solver with a knack for finding solutions by using the department's antiquated and balky[sic] computers or finding a way around them."[2] According to the head of the tax office, "The system had in place a plethora of internal controls as well as a number of manual controls, but you are always vulnerable to an enterprising employee who knows how the controls work."[3]

Although she apologized for her conduct, the insider continued to display the confidence of a woman who managed to steal $48.1 million in fraudulent tax refunds before she was caught. "If you put me back in there today," she told a federal judge, "I could get each of you a check." The United States (U.S.) Attorney for the District of Columbia stated, "Many people think white-collar crime is a victimless crime, and it is not." "It may take years to recover from this." The former tax office manager has admitted that she exploited lax oversight in the tax office to issue more than 230 fraudulent property tax refund checks to friends and co-conspirators starting in 1989. Between 2000 and 2007, her most prolific period, she issued 152 fraudulent refund

[1] Ashley Southall, "17-Year Term for Official in Tax Scam," *New York Times*, July 1, 2009, sec. U.S., http://www.nytimes.com/2009/07/01/us/01embezzle.html.

[2] Christian W. Probst et al., "Aspects of Insider Threats," in *Insider Threats in Cyber Security*, ed. Christian W. Probst et al., Advances in Information Security 49, *Springer U.S.*, 1–15, 2010, http://link.springer.com/chapter/10.1007/978-1-4419-7133-3_1.

[3] Dan Keating, "Tax Suspect's Guidance on Software Left D.C. at Risk," *Washington Post*, June sec. Metro, 10, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/06/09/AR2008060902879_2.html.

checks worth $42 million. During this same time frame, investigators discovered that this trusted insider also gambled heavily, and made 45 trips to Las Vegas and Atlantic City.[4] Her lawyer said that she had a substance abuse and gambling addiction.[5]

This story, sensational in its severity and financial impact to the taxpayers of the District of Columbia, is unfortunately not unusual. Fraud and embezzlement committed by trusted insiders within organizations have been in existence as long as money has been moving through businesses.[6] What is compelling about the former DC tax office manager is that she operated at a high degree of competence for a prolonged period of time, with a substance abuse and gambling addiction as a primary motivating factor for her illegal activity.[7]

Fraud is defined as deceit, trickery, or breach of confidence or trust perpetrated for profit or to gain some unfair or dishonest advantage.[8] To embezzle is to appropriate fraudulently to one's own use, as money or property entrusted to one's care.[9] An "insider threat" is a term that can be defined as an individual, and more broadly, the danger posed by an individual who possesses legitimate access and occupies a position of trust within the infrastructure or institution being targeted.[10] An "insider attack" is when the

---

[4] Del Quentin Wilber, "Tax Scam Leader Gets More Than 17 Years," *Washington Post*, sec. Metro, July 1, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/06/30/AR2009063001652.html?sid=ST2008091700125.

[5] John Metcalfe, "Rita Crundwell vs. Harriette Walters: Who Embezzled Better?," *The Atlantic Cities*, April 18, 2012, http://www.theatlanticcities.com/neighborhoods/2012/04/rita-crundwell-vs-harriette-walters-who-embezzled-best/1797/.

[6] Gary S. Green, "White-Collar Crime and the Study of Embezzlement," *Annals of the American Academy of Political and Social Science* 525 (January 1, 1993): 95–106.

[7] Probst et al., "Aspects of Insider Threats."

[8] "Fraud," accessed January 20, 2014, http://www.merriam-webster.com/dictionary/fraud?show=0&t=1390187912.

[9] "Embezzle," accessed January 20, 2014, http://www.merriam-webster.com/dictionary/embezzle.

[10] Richard Brackney and Robert Andersen, "Understanding the Insider Threat: Proceedings of a March 2004 Workshop R. Understanding the Insider Threat: Proceedings of a March 2004 Workshop," in *Proceedings of a March 2004 Workshop* (Santa Monica, CA: RAND Corporation, 2004), http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2005/RAND_CF196.pdf.

individual who occupies a position of trust or authorization within an organization executes a prohibited or illegal action against it.[11]

1. Motives Matter When It Comes to Fraud and Embezzlement

After an organization discovers that it has been victimized by a trusted insider who has committed a financial crime against it, inevitably, the questions asked are always the same: Why did they do it? What motivated the individual to cause so much harm to the organization and in the end to themselves, their families, and in some cases, the communities they live in? Was it greed alone or does an individual commit financial fraud or embezzlement within an organization for other reasons? What drives them to breach the trust of their employer, was it a character flaw within the individual or simply a crime of opportunity? What propels a person to cross the line from trusted employee and friend to embezzler? The organizations themselves are faced with recovering from the forfeiture of trust, as well as the significant loss of financial resources. Executives and fellow co-workers in the victim organizations predictably question themselves and ask how did they miss reading the clues of dishonesty and deception with a trusted employee who once held their trust and confidence.

Unfortunately, one of the realities of studying insider threats to organizations in which fraud and embezzlement have occurred is the lack of detailed documented motives in police reports and investigations as to why the insider committed their illegal activities.[12] Further complicating the accuracy of knowing the motives behind insider criminal behavior is the availability of statistical data from the Uniformed Crime Report published every year by the Department of Justice.[13]

---

[11] Dawn Cappelli, Andrew P. Moore, and Timothy J. Shimeall, *Common Sense Guide to Prevention and Detection of Insider Threats* (Pittsburgh, PA: Carnegie Mellon University Cy Lab, July 2006).

[12] Jennifer N. Arthur, Robert J. Williams, and Yale D. Belanger, "The Relationship Between Legal Gambling and Crime in Alberta1," *Canadian Journal of Criminology & Criminal Justice* 56, no. 1 (January 2014): 49–84, doi:10.3138/cjccj.2012.E51.

[13] "Summary of the Uniform Crime Reporting Program," accessed March 7, 2014, http://nationalatlas.gov/articles/people/a_crimereport.html#two.

2. Facing the Trusted Insider

All organizations face the problem of an insider threat occurring within its boundaries. Private sector, public sector, and non-profit organizations are all susceptible to a trusted employee or individual operating legitimately within the safe working environment of the industry or sector affected who conduct themselves in illegitimate and illegal ways that can harm the organization.[14] Insider attacks also take on many different forms, from fraud and embezzlement to theft of intellectual property, espionage, and all variations of information technology (IT) misuse.[15] Cyber crime reports in the media and through other sources are a constant reminder that these events are publicly reported, and in fact, can have significant financial ramifications, as well as immeasurable damaging effects to an entity's reputation and stability of its workforce.[16] Left undetected, insiders can cause irreparable and devastating consequences to private and public sector organizations that compromise the integrity of the overall financial system, and therefore, potentially jeopardize the security of systems on which people depend to insure their security.[17]

---

[14] Dawn M. Cappelli, Andrew P. Moore, and Randall F. Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, 1st ed. (Boston, MA: Addison-Wesley Professional, Part of the SEI Series in Software Engineering Series, 2012).

[15] Frank L. Greitzer et al., "Combating the Insider Cyber Threat," *IEEE Security Privacy* 6, no. 1 (January/February 2008): 61–64, doi:10.1109/MSP.2008.8.

[16] Dawn M. Cappelli et al., "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.

[17] Adam Cummings et al., "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector," *Software Engineering Institute, Carnegie Mellon University and CyLab*, 2012, http://repository.cmu.edu/cgi/viewcontent.cgi?article=1688&context=sei; R. Ladouceur et al., "Social Cost of Pathological Gambling," *Journal of Gambling Studies* 10, no. 4 (1994): 399–409.

3. Can Addiction Be a Motivating Factor for Committing Fraud and Embezzlement?

Research suggests that a gambling addiction,[18] an addiction to pain prescription medication,[19] and an enhanced lifestyle may be an indicator of an insider threat to an organization.[20] From a homeland security perspective, government organizations and related private sector agencies are also at risk to insider threats from individuals conducting fraud or embezzlement with addiction behaviors.[21] This claim is supported by behavioral research case studies, which have indicated that a relationship exists between insiders conducting fraud and embezzlement, and addiction to gambling or pain prescription medication.[22]

Recent criminal cases have revealed a disturbing pattern linking many of the trusted insiders with an addiction to gambling or prescription drugs as the motivating factor for perpetrating embezzlement or fraud against victim organizations.[23] Also alarming is the frequency of trusted insiders conducting fraud and embezzlement within

---

[18] Alex Blaszczynski, Neil McConaghy, and Anna Frankova, "Crime, Antisocial Personality and Pathological Gambling," *Journal of Gambling Behavior* 5, no. 2 (June 1, 1989): 137–52, doi:10.1007/BF01019760.

[19] Stephen J. Ziegler and Nicholas P. Lovrich, "Pain Relief, Prescription Drugs, and Prosecution: A Four-State Survey of Chief Prosecutors," *The Journal of Law, Medicine & Ethics* 31, no. 1 (2003): 75–100, doi:10.1111/j.1748-720X.2003.tb00060.x.

[20] Green, "White-Collar Crime and the Study of Embezzlement."

[21] Richard J. Frances, Sheldon I. Miller, and Avram H. Mack, *Clinical Textbook of Addictive Disorders* (New York: Guilford Press, 2005), 234–236; National Research Council, *Pathological Gambling: A Critical Review, Committee on the Social and Economic Impact of Pathological Gambling, Committee on Law and Justice, Commission on Behavioral and Social Sciences and Education* (Washington, DC: National Academy Press, 1999), 3–26.

[22] Jay Albanese, "White Collar Crimes and Casino Gambling: Looking for Empirical Links to Forgery, Embezzlement, and Fraud," *Crime, Law & Social Change* 49, no. 5 (June 2008): 333–47, doi:10.1007/s10611-008-9113-9; Virgil W. Peterson, "Why Honest People Steal," *Journal of Criminal Law and Criminology* 38, no. 2, art. 2 (1947): 94–103.

[23] Southall, "17-Year Term for Official in Tax Scam"; Bryan Smith, "Rita Crundwell and the Dixon Embezzlement," *Chicago Magazine*, December 2012, http://www.chicagomag.com/Chicago-Magazine/December-2012/Rita-Crundwell-and-the-Dixon-Embezzlement/; Associated Press, "Tulsa Fires Athletic Director over Gambling Probe," December 4, 2012, http://bigstory.ap.org/article/tulsa-fires-athletic-director-over-gambling-probe; USDOJ, "Convention Center's Former Executive Director Sentenced to 24 Months in Prison for Embezzlement," *U.S. Attorney's Office—Western District of Kentucky*, June 7, 2012, http://www.justice.gov/usao/kyw/news/2012/20120607-01.html.

government agencies to finance and support their addiction.[24] Many of these trusted government employees who have committed illegal activities have had access to sensitive information concerning their particular municipalities, and in some cases, have had access to some of this nation's most guarded secrets and intelligence programs, which when revealed compromises the reputation and integrity of their oaths of office, and potentially, national security.[25]

The Association of Certified Fraud Examiners announced in its "2012 Annual Report to the Nations" that workplace fraud costs a typical organization five percent of its annual revenue. "Applied to the estimated 2011 Gross World Product, this figure translates to a potential projected global fraud loss of more than $3.5 trillion." The median loss caused by the occupational fraud cases in the study was $140,000. More than one-fifth of these cases caused losses of at least $1 million.[26] It is estimated that the costs of white-collar crime in the United States may reach as much as $1 trillion annually.[27]

"The 2012 Marquet Report on Embezzlement" shows that the number of major embezzlements in the United States has increased significantly in a recent two-year period. The average size of the reported losses in the reviewed cases also increased at a rate of $1.4 million in 2012 compared with an average of $750,000 in 2011. According to

---

[24] Metcalfe, "Rita Crundwell vs. Harriette Walters: Who Embezzled Better?"; Robert Patrick, "Former Brentwood Official Admits Embezzling Money, Gambling It Away," *Stltoday.com*, June 29, 2011, http://www.stltoday.com/news/local/crime-and-courts/former-brentwood-official-admits-embezzling-money-gambling-it-away/article_210f8282-a269-11e0-84b8-0019bb30f31a.html; Terry Collins, "Calif. Politician Pleads Guilty to Misusing Funds," *Associated Press*, accessed September 30, 2013, http://bigstory.ap.org/article/ex-n-calif-politician-pleads-guilty-felonies; Elliot Spagat, "Ex-San Diego Mayor's Gambling Wagers Top $1B," *Associated Press*, accessed September 30, 2013, http://bigstory.ap.org/article/ex-san-diego-mayor-faces-money-laundering-charge.

[25] Nolan Clay, "Ex-FBI Agent in Oklahoma Gets Six Months in Prison for Embezzling," *NewsOK.com*, accessed March 14, 2014, http://newsok.com/ex-fbi-agent-in-oklahoma-gets-six-months-in-prison-for-embezzling/article/3738422; Larry Lebowitz, "Ex-FBI Agent Sentenced to Five Years in Prison," *Sun Sentinel*, November 24, 1998, http://articles.sun-sentinel.com/1998-11-24/news/9811240441_1_sentence-sullivan-s-role-gambling-debts; Associated Press in Washington, "U.S. Nuclear Commander Tim Giardina Fired Amid Gambling Investigation," *The Guardian*, October 9, 2013, http://www.theguardian.com/world/2013/oct/09/us-nuclear-commander-tim-giardina-fired-amid-gambling-investigation.

[26] "2012 Report to the Nations—Key Findings and Highlights," accessed January 17, 2014, http://www.acfe.com/rttn-highlights.aspx.

[27] Laurie L. Ragatz, William Fremouw, and Edward Baker, "The Psychological Profile of White-collar Offenders Demographics, Criminal Thinking, Psychopathic Traits, and Psychopathology," *Criminal Justice and Behavior* 39, no. 7 (July 1, 2012): 978–97, doi:10.1177/0093854812437846.

the study, "Gambling and substance abuse was a clear motivating factor in driving some major embezzlement cases."[28]

It is important to be able to better detect insiders within organizations who have a predisposition to an addiction to gambling or pain prescription medication.[29] Research and recent criminal cases suggests a connection between insider threats and addiction as a motivating factor and cause of illegal activities perpetrated by trusted insiders, as well as providing a compelling impetus for further case study into this phenomenon.

Within the broad parameters of the insider threat, extensive studies and research have been conducted that have focused primarily on cyber-attacks, IT, espionage, and intellectual property theft. A growing knowledge base is available, which defines possible causes, predictive models, and best practices for mitigation.[30] However, within the comprehensive research that has been published on the insider threat, less attention has been placed on the narrower focus of insider fraud and embezzlement cases in which the trusted insiders were motivated by the need to finance and support an addiction as the primary reason for conducting their illegal activity within the victim organization.

This study addresses the connection between insider fraud and embezzlement cases to individuals with addictive personality behaviors, specifically, gambling and pain medication addiction. It examines the connection to addiction with regard to insider fraud and embezzlement as a financial motivator for committing crime within organizations. It also asserts that many contributing factors cause insider threats to organizations; however, it is suggested that addiction plays a determining factor in many criminal cases

---

[28] Marquet International, Ltd., "The 2012 Marquet Report on Embezzlement: A White Collar Fraud Study of Major Embezzlement Cases Active in the U.S. in 2012," May 14, 2013, http://www.marquetinternational.com/pdf/the_2012_marquet_report_on_embezzlement.pdf.

[29] David M. Ledgerwood et al., "Clinical Features and Treatment Prognosis of Pathological Gamblers with and Without Recent Gambling-Related Illegal Behavior," *Journal of the American Academy of Psychiatry and the Law Online* 35, no. 3 (September 1, 2007): 294–301; Nady el-Guebaly et al., "Compulsive Features in Behavioral Addictions: The Case of Pathological Gambling," *Addiction* 107, no. 10 (October 2012): 1726–1734, doi:10.1111/j.1360-0443.2011.03546.x.

[30] Andrew Moore et al., "A Preliminary Model of Insider Theft of Intellectual Property," *Software Engineering Institute*, June 1, 2011, http://repository.cmu.edu/sei/726; George Silowash et al., "Common Sense Guide to Mitigating Insider Threats, 4th Edition," *Software Engineering Institute*, December 1, 2012, http://repository.cmu.edu/sei/677; Cappelli, Moore, and Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*..

of fraud and embezzlement conducted by trusted insiders and focuses on addiction as a motivating factor, primarily due to time and space restrictions for this paper. It is argued that this phenomenon is underreported in law enforcement investigations, and the Uniformed Crime Report, and may be occurring more frequently than is conveyed.

B. RESEARCH QUESTION

Trusted insiders are committing fraud and embezzlement within organizations: Is there a connection to addiction as the motivating factor for their illegal activities?

C. SIGNIFICANCE OF RESEARCH

A review of the literature clearly indicates that organizations are vulnerable to insider threats.[31] The trusted insider with ill intent who has access to information, systems, and facilities is capable of doing significant damage to an organization.[32] The literature also indicates that trusted insiders who have an addiction or a predisposition to addictive behaviors are susceptible to conducting illegal actions to finance and support the addiction.[33] However, literature regarding threats to organizations caused by trusted insiders conducting fraud and embezzlement because of an addiction is scarce. Further, when it comes to reporting whether the insider was addicted to gambling or pain prescription medication, data is lacking regarding the amount of criminal activity being reported by law enforcement agencies concerning the motives for fraud and embezzlement cases conducted by insiders.[34] This study contributes to the existing research on insider threats to organizations and helps bridge gaps with regard to the

[31] Cappelli, Moore, and Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*; Green, "White-Collar Crime and the Study of Embezzlement"; Joseph T. Wells, *Corporate Fraud Handbook: Prevention and Detection* (Hoboken, NJ: John Wiley & Sons, 2011).

[32] Greitzer et al., "Combating the Insider Cyber Threat"; Marissa R. Randazzo et al., *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector* (Pittsburg, PA: Software Engineering Institute, June 2005).

[33] *National Gambling Impact Study Commission, Final Report* (Washington, DC: Impact Study Commission, June 1999); Donald R. Cressey, *Other People's Money; A Study in the Social Psychology of Embezzlement* (Montclair, NJ: Patterson Smith, 1973); Henry R. Lesieur, "Gambling, Pathological Gambling and Crime," in *Handbook on Pathological Gambling*, ed. Thomas Galski (Springfield, IL: Charles C. Thomas, 1987), 89–110.

[34] Arthur, Williams, and Belanger, "The Relationship Between Legal Gambling and Crime in Alberta1."

limited reporting of addiction as a motive for the causation of fraud and embezzlement cases by insiders' being reported to and by law enforcement.

D. METHODOLOGY

This research focuses on individuals—"trusted insiders"—within organizations who have committed fraud or embezzlement against an organization. The research determines what, if any, connection the insiders' motivation for committing the offense was due to an addiction. A hybrid research methodology employing case studies exercising both qualitative and quantitative features is used.

E. ORGANIZATION OF THIS RESEARCH

First, 40 recently closed and adjudicated fraud and embezzlement criminal cases involving 45 convicted insiders investigated by the U.S. Secret Service (USSS) in the Louisville, Cincinnati, Memphis, and Nashville Field Offices are reviewed.[35] The objective of this research was to determine if addiction or addictive actions played a role or contributed to the motivating factors by the insiders' for committing their illegal activities. USSS fraud and embezzlement cases were chosen because of the close association that a trusted insider plays in committing these types of crimes within organizations.

Next, the results of research conducted by the Software Engineering Institute at Carnegie Mellon University Computer Emergency Response Team (CERT) Program are examined. CERT completed data research on 680 insider threat cases currently in their database to determine if addiction or addictive behaviors were a contributing factor to the

[35] Ten recently closed criminal cases each from the above four Secret Service Field Offices are reviewed, with 45 convicted insiders from the 40 closed criminal cases reviewed. Only information provided by the closed criminal case files was reviewed by the writer who had unrestricted access to the information contained in the closed case reports as the Special Agent in Charge of the U.S. Secret Service Louisville Field Office. No personally identifiable information (PII) information of the convicted insiders was used in this review, unless it was from published open source media reports.

convicted insider's' motives for conducting their illegal activity.[36] The research is then evaluated, conclusions drawn, and recommendations provided for further research and review of insiders committing fraud and embezzlement in organizations due to addiction-related characteristics.

[36] Currently, the CERT Program has over 700 documented cases of malicious insiders convicted in a U.S. court of law for criminal violations regarding illegal insider activity involving some form of critical IT services. The current cases in the insider threat database involve insider incidents from 1996 to the present. The following are the sources of information CERT used to code insider threat cases: public sources of information include media reports, court documents, and publications. Non-public sources of information include law enforcement investigations, organization investigations, interviews with victim organizations and convicted insiders. No PII information of individuals in the Insider Threat database is disclosed or published by CERT.

II. LITERATURE REVIEW

A. INTRODUCTION

Since June 2013, the world became fixated on a former National Security Agency (NSA) "trusted insider," by the name of Edward Snowden, who began releasing damaging secrets of NSA spying activities on American citizens, world leaders, and others, in a global tale of intrigue that would be the largest intelligence leak in the agency's history. The U.S. government was once again caught off guard by one of its own, who using IT, revealed some of the nation's most highly protected secrets. Snowden's motives for doing so appear to be purely ideological in nature.[37] However, ideology is not the only reason, or even the most important reason, an individual may become an insider threat.

In a criminal case that involved a highly esteemed, "trusted insider" who also garnered worldwide media attention in 2013, the former mayor of San Diego, admitted that she took $2.1 million from her late husband's charitable foundation in a decade-long gambling spree when she wagered more than $1 billion. "The former Mayor was a selfless public official who contributed much to the well-being of San Diego," said the U.S. Attorney for the Southern District of California. "However, no figure, regardless of how much good they've done or how much they've given to charity can escape criminal liability with impunity."[38] The trusted insider's' motive for conducting her illegal activity was due to a gambling addiction.[39] San Diego is the seventh largest city in the United States and is home to numerous U.S. military bases.[40]

Insider attacks have occurred across all public, private and non-profit sectors, which cause significant damage to the affected organizations. These acts have ranged

---

[37] Glenn Greenwald, "Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations|World News," *The Guardian*, June 9, 2013, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[38] Spagat, "Ex-San Diego Mayor's Gambling Wagers Top $1B."

[39] Ibid.

[40] "San Diego, California—City Information, Fast Facts, Schools, Colleges, and More," accessed May 27, 2014, http://www.citytowninfo.com/places/california/san-diego.

from less technical attacks, such as fraud and embezzlement or theft of proprietary information, to technically sophisticated cybercrimes that sabotage the entire organization.[41] "Damages are not only financial, but can also include severe impact to the organization's reputation, resulting from widespread public reporting of the event."[42]

During the past three decades, the U.S. government and the private sector have made a significant investment in the study of behavioral risk indicators associated with espionage, sabotage, and threats to IT systems associated with an employee.[43] Thirty years ago, it was reported in *Americans Who Spied Against Their Country Since World War II* that the most significant risk to national security was associated with the employee who was on the inside, and not the result of actions conducted by "secret agents from foreign governments."[44]

Today, organizations are growing in understanding that the insider threat is real and all sectors are potential targets of a trusted insider operating legitimately within the borders of the enterprise. A growing field of research analyzes the insider threat with extensive studies focused on espionage, sabotage, theft of intellectual property and threats to IT systems.[45] A developing knowledge base is available from numerous academic researchers and practitioners, which defines possible causes, probable motives, predictive models, and best practices for mitigating the threats of insider attacks to a wide

---

[41] Michelle Keeney et al., *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors* (Pittsburgh, PA: U.S. Secret Service and CERT Coordination Center, Carnegie Mellon Software Engineering Institute, 2005).

[42] Cappelli et al., *Common Sense Guide to Prevention and Detection of Insider Threats*.

[43] Michael G. Gelles, David L. Brant, and Brian Geffert, "Building A Secure Workforce: Guard Against Insider Threat," *Deloitte Federal Government Services*, 2008, https://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_ps_insiderthreat_100108.pdf.

[44] Suzanne Wood and Martin F. Wiskoff, *Americans Who Spied Against Their Country Since World War II* (Monterey, CA: Defense Personnel Security Research Center, 1992).

[45] Eric Cole and Sandra Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft: Protecting the Enterprise from Sabotage, Spying, and Theft* (Maryland Heights, MO: Syngress, 2005); Moore et al., "A Preliminary Model of Insider Theft of Intellectual Property"; Steven Band et al., "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis|SEI Digital Library," *Software Engineering Institute, Carnegie Mellon University*, 2006, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8163#.

range of the nation's critical infrastructure, government agencies, and the private sector.[46]

In contrast to the emerging body of study on IT threats, less research has been conducted on the insider threat posed by financial fraud and embezzlement to organizations caused by addiction as a motivating factor or primary cause for the insider attack. Recent criminal cases have revealed a disturbing pattern linking many of the insiders perpetrating fraud or embezzlement, with an addiction to gambling or prescription drugs.[47] Also alarming is the frequency of trusted insiders conducting fraud or embezzlement within government agencies to support their addiction.[48] Left undetected, insiders with an addiction can cause permanent and destructive consequences to private, public, and non-profit sector organizations, potentially bankrupting, demoralizing, and possibly, compromising the soundness and strength of the overall financial system of the United States or even impacting national security.[49]

It is important for homeland security officials to take note and study insider threat cases at all levels of government, as well as the private sector. This literature review is a critical examination of the relevant literature on the issue of the insider threat along with addiction as a motivating factor. It begins with defining insider threat, reviews what the scope of the insider threat is, examines studies completed on insider threats, and analyzes

---

[46] Randazzo et al., *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*; Cummings et al., "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector"; Cappelli, Moore, and Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).*

[47] Southall, "17-Year Term for Official in Tax Scam"; John Schriffen, "Ex-Comptroller Faces Jail in $53M Scam," *ABC News*, November 15, 2012, http://abcnews.go.com/Business/comptroller-rita-crundwell-pleads-guilty-stealing-53m-illinois/story?id=17723699; Cynthia R. Fagen, "Twisted Sister in Nun Jail," *New York Post*, November 13, 2011, http://www.nypost.com/p/news/local/twisted_sister_in_nun_jail_gZfMQUNa031kduaErl9htM; USDOJ, "Convention Center's Former Executive Director Sentenced to 24 Months in Prison for Embezzlement."

[48] Metcalfe, "Rita Crundwell vs. Harriette Walters: Who Embezzled Better?"; Patrick, "Former Brentwood Official Admits Embezzling Money, Gambling It Away"; Joseph De Avila, "Financial Scandal Strains Community in Winsted, Conn.," October 16, 2013, http://online.wsj.com/news/articles/SB10001424052702304561004579137440704100238?KEYWORDS=+embezzlement+and+gambling+.

[49] Associated Press, "Retired Colonel Sentenced for Embezzling Millions," *KTVK Azfamily.com*, March 28, 2012, http://www.azfamily.com/news/Retired-colonel-sentenced-for-embezzling-millions-144694985.html; Associated Press in Washington, "U.S. Nuclear Commander Tim Giardina Fired Amid Gambling Investigation"; Lebowitz, "Ex-FBI Agent Sentenced to Five Years in Prison."

related research on addiction, specifically, in the areas of gambling and pain prescription medication in which insiders conducted fraud and embezzlement to support their addictive behaviors.

The literature concludes with possible preventative measures, identification, and insider threat mitigation strategies. The review suggests that further scientific case studies on insiders who have committed fraud or embezzlement because of addiction as a primary motivator is warranted. The literature indicates that motives and causation of crime is not captured in police reports and through the Uniformed Crime Report regarding individuals committing crime due to an addiction. The literature suggests that a connection between insider threats and insiders with addiction or addictive behavior traits exists, and may provide a compelling impetus for further case study of this phenomenon, which is what this paper intends to demonstrate.

B. INSIDER THREATS DEFINED

The literature shows that the definition of "insider" and "insider threat" has evolved over the years and varies depending on the context in which it is used. According to one researcher, even the definitions of insider can be contradictory.[50] For example, a RAND report defines an insider as "an already trusted person with access to sensitive information and information systems."[51] Elsewhere in the report it defines an insider as "someone with access and privilege, or knowledge of information and systems," and omits the need for that person to be trusted.[52]

Matt Bishop and Carrie Gates believe that an insider is an individual who has "access, knowledge and trust" within an organization.[53] John Patzakis defines the insider

---

[50] Matt Bishop and Carrie Gates, "Defining the Insider Threat" (presented at the Fourth Annual Cyber Security and Information Intelligence Research Workshop, Davis, CA: ACM Press, 2008), 1, doi:10.1145/1413140.1413158.

[51] Brackney and Andersen, "Understanding the Insider Threat: Proceedings of a March 2004 Workshop R. Understanding the Insider Threat: Proceedings of a March 2004 Workshop."

[52] Ibid., 10.

[53] Matt Bishop et al., "A Risk Management Approach to the 'Insider Threat,'" in *Insider Threats in Cyber Security*, ed. Christian W. Probst et al., Advances in Information Security 49 (Springer U.S., 2010), 116–117, http://link.springer.com/chapter/10.1007/978-1-4419-7133-3_6.

as, “anyone operating inside the security perimeter,” but ignores trust and knowledge of the systems.[54] Dawn Cappelli et al. defines the 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.”[55]

Thomas Noonan and Edmund Archuleta, in their report from “The National Infrastructure Advisory Council,” defines the insider threat to critical infrastructures as, “one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity’s security, systems, services, products, or facilities with the intent to cause harm.”[56] Frank L. Greitzer et al. refers to the insider threat as “harmful acts that trusted individuals might carry out; for example, something that causes harm to the organization, or an unauthorized act that benefits the individual. The insider threat is manifested when human behaviors depart from established policies, regardless of whether it results from malice or disregard for security policies.”[57]

Jeffrey Hunker and Christian Probst provide the definition of an insider from a 2008 cross-disciplinary workshop on Countering Insider Threats, “as a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization’s structure.” Although minor contradictions occur in the

---

[54] John Patzakis, “IRBestPractices.pdf,” *Guidance Software*, September 2003, http://faculty.usfsp.edu/gkearns/Articles_Fraud/IRBestPractices.pdf.

[55] Cappelli et al., *Common Sense Guide to Prevention and Detection of Insider Threats*.

[56] Thomas Noonan and Edmund G. Archuleta, “The National Infrastructure Advisory Council’s Final Report and Recommendations on–The Insider Threat to Critical Infrastructures,” *Department of Homeland Security*, April 8, 2008, 11. http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.

[57] Frank L. Greitzer et al., “Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats,” in *2012 45th Hawaii International Conference on System Science (HICSS)*, 2012, 2392–2401, doi:10.1109/HICSS.2012.309.

definition of an insider, the core element is always based on an individual who has access into, or within, an organization.[58]

C. SCOPE AND IMPACT OF INSIDER THREATS

Statistics vary regarding the prevalence of cases perpetrated by insiders compared to those perpetrated by those external to the targeted organizations.[59] Marissa Randazzo et al. opines, "Nevertheless, insiders pose a substantial threat by virtue of their knowledge of and access to their employers' systems and/or databases, and their ability to bypass existing physical and electronic security measures through legitimate means."[60]

In a "2007 Computer Security Institute Survey" about computer crime and security, 59% of respondents indicated that they had experienced insider exploitation of IT resources. Roughly one in four believed that more than 40% of their total financial losses from cyber-attacks were due to insider activities.[61]

A "2008 National Computer Security Survey" suggests that the insider threat is real and the consequences significant: 40% of all incidents reported were attributed to insiders. Additionally, 74% of all cyber theft was attributed to insiders, including 93% of embezzlement incidents and 84% of intellectual property thefts.[62] "The 2013 State of Cyber Crime Survey" reveals that 33% of respondents identified "insider crimes as more likely to cause more damage to an organization than an external attack."[63]

---

[58] Jeffrey Hunker and Christian W. Probst, "Insiders and Insider Threats—An Overview of Definitions and Mitigation Techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 2, no. 1 (2011): 6–7.

[59] Robert Richardson, "CSI FBI Survey 2003—Fbiraportti.pdf," *yle*, 2003, http://www.yle.fi/mot/kj040524/fbiraportti.pdf.

[60] Dawn Cappelli et al., "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," *U.S. Secret Service and CERT Coordination Center/Software Engineering Institute*, 2004, http://www.cert.org/archive/pdf/bankfin040820.pdf.

[61] Robert Richardson, "The 12th Annual Computer Crime and Security Survey," Computer *Security Institute*, 2007, http://gocsi.com/sites/default/files/uploads/2007_CSI_Survey_full-color_no%20marks.indd_.pdf.

[62] Louis M. Davis et al., "The National Computer Security Survey (NCSS): Final Methodology–RAND_TR544.pdf," *The RAND Corporation*, 2008, http://www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR544.pdf.

[63] CSO Magazine et al., "2013 State of Cybercrime Survey," *PwC*, 2013, http://www.pwc.com/us/en/press-releases/2013/cybercrime-threats-continue.jhtml.

The damages caused by malicious insiders each year are substantial, and continue to increase. The toll of insider events causes not only financial strain, but also negative publicity, loss of public confidence, and untold other negative consequences for an organization.[64] A recently disclosed theft of personal information on 26.5 million U.S. veterans and active-duty personnel from the home of a Department of Veterans Affairs analyst lead one writer to proclaim, "This is a catastrophe that should have been anticipated and could have been avoided." The security risks posed by insiders are becoming more visible and damaging but are far from new. "Many executives in the federal government and corporate America remain ill equipped and unprepared to address the security threats posed by their trusted insiders."[65]

According to a 2013 RSA presentation that cited open-source data-breach reports and data-loss surveys gathered over a recent 10-year period, "The average cost per incident is $412,000, and the average loss per industry is $15 million over ten years. In several instances, damages reached more than $1 billion."[66]

These financial losses strongly suggest that organizations need to address insider attacks, especially when research indicates that trusted insiders against organizations perpetrate 70% of fraud rather than external criminals, yet, 90% of security controls and monitoring are focused on external threats. "With the appropriate motivation and time, human beings who are trusted insiders will find their way around most technical controls."[67]

---

[64] Cappelli, Moore, and Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).*

[65] Sean Steele, "VA Breach Shows Growing Insider Threats," *Network World* 23, no. 24 (June 19, 2006): 43–43.

[66] Kathleen Richards, "RSA 2013: FBI Offers Lessons Learned on Insider Threat Detection," *Search Security*, March 5, 2013, http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection.

[67] Carl Colwill, "Human Factors in Information Security: The Insider Threat – Who Can You Trust These Days?," *Information Security Technical Report* 14, no. 4 (November 2009): 186–96, doi:10.1016/j.istr.2010.04.004.

D. FRAUD AND EMBEZZLEMENT: IS IT REALLY THAT BAD?

According to a report recently published by Marquet International, major embezzlement incidents in the United States (defined by cases in which at least $100,000 was misappropriated) increased 11% in 2012 when compared to the number of cases analyzed in 2011. The 528 cases analyzed in "The 2012 Marquet Report on Embezzlement" are the most ever recorded in the report's five-year history. In the cases analyzed, the average amount of money lost by businesses was about $1.4 million. The businesses in all the cases analyzed lost a total of approximately $737 million.[68]

The "2012 Report to the Nations" produced annually by the Association of Certified Fraud Examiners (ACFE) reported that fraud being conducted by trusted insiders lasted an average of 18 months before being detected. The perpetrators conducting the fraud who possessed higher levels of authority within the organization tended to cause much larger losses. The average amount of loss among frauds committed by owners/executives was $573,000, the median loss caused by managers was $180,000, and the median loss caused by other employees was $60,000.[69]

Occupational fraud conducted by trusted insiders is a significant threat to small businesses. The smallest organizations in the study suffered the largest median losses because, "these organizations typically employ fewer anti-fraud controls than their larger counterparts, which increases their vulnerability to fraud."[70]

Research conducted by the ACFE concluded that the industries most commonly victimized are banking and financial services, government and public administration, and the manufacturing sectors. The research reflected that individuals working in one of six departments committed the majority, or 77% of all frauds: accounting, operations, sales, executive/upper management, customer service, and purchasing. This distribution was very similar to what was found in the 2010 ACFE study.[71]

---

[68] Marquet International, Ltd., "The 2012 Marquet Report on Embezzlement: A White Collar Fraud Study of Major Embezzlement Cases Active in the U.S. in 2012."

[69] "2012 Report to the Nations—Key Findings and Highlights."

[70] Ibid.

[71] Ibid.

"The 2012 Marquet Report on Embezzlement" indicated that the organizations most susceptible to fraud and embezzlement schemes by trusted insiders are those that do not have a division of labor when it comes to their finances or a multitude of people monitoring money coming in and out of the organization. The most common victims of insider fraud and embezzlement were non-profit, religious organizations, and small businesses, which revealed that these types of enterprises have relatively weak controls in place to counter the insider attack.[72] This literature indicates that these are informal, self-reported estimates, but indicate that the problem is genuine and noteworthy.

Shari Pfleeger and Salvatore Stolfo believe that credible data describing the scope and impact of unwelcome insider actions are more difficult to determine, for two reasons:

> First, many organizations are unwilling to reveal the nature and magnitude of insider incidents they have experienced for fear of reputational harm. Second, most published cyber surveys are convenience surveys; it is impossible to know what population the results represent. This paucity of data is challenging for insider threat researchers who require good data with which to build models, make predictions, and support good decision-making by end users.[73]

Quantifying the damage of an insider attack can be difficult because it can extend far beyond the stolen or corrupted items' actual cost. For example, it is extremely difficult to estimate the amount of damage to finances and confidence around negative publicity for a publicly traded company, a non-profit, or a government organization affected by a high profile or high-level employee conducting an insider attack.[74]

In a recent survey of small businesses, a University of Cincinnati criminal justice researcher found that only 16% of those that have experienced theft by employees actually reported that theft to the police, in spite of 64% of the small businesses surveyed reported experiencing employee theft. The researcher stated, "It's important to look at this topic because such theft represents a loss to the tax base and would also seem to put

---

[72] Marquet International, Ltd., "The 2012 Marquet Report on Embezzlement: A White Collar Fraud Study of Major Embezzlement Cases Active in the U.S. in 2012."

[73] Shari Lawrence Pfleeger and Salvatore Stolfo, "Addressing the Insider Threat," *IEEE Security & Privacy* 7 (2009), http://academiccommons.columbia.edu/catalog/ac:125619, 10.

[74] Cappelli et al., *Common Sense Guide to Prevention and Detection of Insider Threats*.

such businesses at risk, and so, put our overall economy at risk. After all, small businesses with 100 or fewer employees comprise 97% of all businesses in the United States."[75]

According to the U.S. Chamber of Commerce, one third of small business bankruptcies are the result of employee theft, which includes fraud and embezzlement. This development comes at a time when long-term trends show that small businesses have been responsible for more than 65% of new jobs over the last 17 years, according to the U.S. Small Business Administration.[76]

The "2011 CyberSecurity Watch Survey" shows, "the public may not be aware of the number of insider events or the level of the damage caused because 70% of insider incidents are handled internally without legal action." This element of the survey was in line with the "2010 CyberSecurity Watch Survey" completed on insider threats.[77] "Moreover, due to the secretive nature of white-collar crime, it is also severely underreported in both frequency of occurrence and prosecution. Because prosecutors screen cases for further investigation and prosecution, the number of cases accepted for prosecution grossly underrepresents the frequency of occurrence."[78]

E. RESEARCH ON INSIDER THREATS AND INSIDER ATTACKS

Literature reviewed indicates that considerable research has been done to examine and define the general nature of inappropriate insider activity primarily in the IT space, with the goal that eventually organizations can reduce the threat and have a more complete understanding of the nature of insider threats. Beginning in 1999, RAND conducted a series of workshops to generate a research agenda for addressing this

---

[75] M. B. Reilly, "Surprising Survey: Most Small Businesses Remain Silent Rather Than Report Employee Theft," February 18, 2014, http://phys.org/news/2014-02-survey-small-businesses-silent-employee.html.

[76] Ibid.

[77] "2011 CyberSecurity Watch Survey: Organizations Need More Skilled Cyber Professionals to Stay Secure," *Marketwire*, accessed February 10, 2014, http://www.marketwired.com/press-release/2011-CyberSecurity-Watch-Survey-Organizations-Need-More-Skilled-Cyber-Professionals-1387863.htm.

[78] Ziegler and Lovrich, "Pain Relief, Prescription Drugs, and Prosecution: A Four-State Survey of Chief Prosecutors.

problem.[79] The objective of the RAND workshops was to address researchers and to encourage a more penetrating exploration of the causes of and possible solutions to mitigating the insider threat within the information technology domains.[80] The workshops focused on defining the nature of insider threats and developing a foundation of knowledge on insider attacker characteristics, vulnerabilities they tend to exploit, and attack methods they employ.[81]

The Defense Personnel Security Research Center (PERSEREC) and CERT at Carnegie Mellon University's Software Engineering Institute initiated an ongoing partnership in 2001 to research cyber- or computer-related insider threats jointly in the military services and defense agencies. This partnership formed and enabled work to begin in response to recommendations in the 2000 Department of Defense (DOD) "DOD Insider Threat Mitigation Report." The focus of the partnership was to identify characteristics of the environment surrounding insider threats and insider cyber events evaluated for criminal prosecution by DOD investigative services. Since that time, both organizations have conducted separate research in this area, and published detailed results analyzing both the psychological and technical aspects of malicious technical activity by trusted insiders.[82]

---

[79] Robert H. Anderson, "Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems: Results of a Three-Day Workshop. RAND CF-151-OSD," *RAND Corporation*, 1999, http://citeseer.uark.edu:8080/citeseerx/showciting;jsessionid=66C66F7E33D77E8C7241750AD878F092?cid=252875.

[80] Robert H. Anderson et al., "Research on Mitigating the Insider Threat to Information Systems—#2 Proceedings of a Workshop Held August, 2000" (RAND Corporation, 2000), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA386077.

[81] Brackney and Andersen, "Understanding the Insider Threat: Proceedings of a March 2004 Workshop R. Understanding the Insider Threat: Proceedings of a March 2004 Workshop."

[82] *Final Report of the Insider Threat Integrated Process Team, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)* (Washington, DC: Department of Defense, April 24, 2000), 7–8; Eric D. Shaw, "'Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders,' Report 2—Case Studies, Technical Report 05–05," *Defense Personnel Security Research Center, Monterey, CA*, 2005, http://www.dhra.mil/perserec/reports.html; Eric D. Shaw and Lynn F. Fischer, "Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations," *Defense Personnel Security Research Center, Monterey, CA*, September 2005, http://www.dhra.mil/perserec/reports/tr05-13.pdf; Cummings et al., "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector."

The literature reveals thorough case studies of convicted insiders, attack characteristics, and analysis on the background surrounding the insider attack on individual insider cases. Adam Cummings et al. noted that this early work was important because PERSEREC compiled information related to espionage and insider events against U.S. concerns. PERSEREC produced two valuable data sets that have been used extensively by insider threat researchers.[83]

In its noted work, "Espionage Against the United States by American Citizens, 1947–2001 and The National Security Espionage Database," PERSEREC produced detailed information on 150 cases of one-time trusted insiders who committed espionage against the United States. Several categories of information were gathered in their database including biographic, employment and related security clearance characteristics, details of each act of espionage perpetrated, motivations, and consequences of the acts. Money was cited as the dominant motivator for the trusted insider as the reason for their acts of spying.[84] One researcher stated, "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."[85]

"Project Slammer" was a study conducted by the DOD and the Federal Bureau of Investigation (FBI), which examined the motives and patterns of behavior of convicted

---

[83] *Final Report of the Insider Threat Integrated Process Team, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)* (Washington, DC: Department of Defense, April 24, 2000), 7–8; Eric D. Shaw, "'Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders,' Report 2—Case Studies, Technical Report 05–05," *Defense Personnel Security Research Center, Monterey, CA*, 2005, http://www.dhra.mil/perserec/reports.html; Eric D. Shaw and Lynn F. Fischer, "Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations," *Defense Personnel Security Research Center, Monterey, CA*, September 2005, http://www.dhra.mil/perserec/reports/tr05-13.pdf; Cummings et al., "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector."

[84] Katherine L. Herbig and Martin F. Wiskoff, "Espionage Against the United States by American Citizens 1947–2001, PERSEREC Technical Report 02–5," *Defense Personnel Security Research Center, Monterey, CA*, July 2002, http://www.fas.org/sgp/library/spies.pdf.

[85] Cummings et al., "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector," 3.

spies. This study brought to light a series of complicated and multifaceted motivational factors that drove spies to do what they did. This group of spies was asked about their life circumstances at the time they began spying, the motivation behind their acts, and the thought processes that led them to spy.[86] The results identified an interaction of factors, none of which alone was sufficient to result in an act of espionage, but taken together over time, the traits and experiences common to many of the perpetrators appear to have formed a common pathway by way of personal stressors and predispositions to cause the acts of espionage.[87] Money featured highly in the motivations to act illegally.

Eric Shaw and Lynn Fischer conducted important research on 10 cases of trusted insiders operating in the critical infrastructure sectors. The cases in question were IT insider events in which an insider or former insider, having had legitimate access to a critical information system, abused or violated that trust for personal advantage or to exact revenge on a person or organization. In each case, the actions of a disgruntled or self-interested offender seriously damaged or compromised the operability of a critical information system. They investigated background behaviors of the malicious insiders, attempted to determine possible motivating factors for the insiders' actions, documented relevant case facts of each incident, and endeavored to draw appropriate conclusions on insider behavior that occurred before, during, and after each event.[88] Kramer suggests that further research is needed on predictive indicators and algorithms because when opportunity and motivation come together, an insider attack is possible.[89] However,

---

[86] CIA, Freedom of Information Act Electronic Reading Room, "Project Slammer Interim Report (U)," Director of Central Intelligence, 1992, http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000218679.pdf.

[87] Krista Forcier, "Project Slammer: Why Spies Are Spying," *National Security Training Institute*, November 12, 2013, https://www.nstii.com/content/project-slammer-why-spies-are-spying.

[88] Shaw and Fischer, "Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations."

[89] Lisa A. Kramer, Richards J. Heuer, Jr., and Kent S. Crawford, "Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage," Defense Personnel Security Research Center, *Federation of American Scientists*, May 2005, http://www.fas.org/sgp/othergov/dod/insider.pdf.

despite considerable research into the psychology and motivation of insiders, it remains difficult to predict who will commit insider fraud.[90]

In 2002, CERT and the USSS initiated the *Insider Threat Study*, *a* joint study of the psychological and technical issues surrounding actual insider threat cases. The study combined the U.S. National Threat Assessment Center's expertise in behavioral psychology with CERT's technical security expertise, to provide in-depth analysis of approximately 150 insider incidents involving IT that occurred in critical infrastructure sectors between 1996 and 2002. Analysis included the thorough review of case documentation and interviews of personnel involved in each incident.[91]

Four reports were published as part of the *Insider Threat Study*, one of which analyzed malicious insider incidents in the banking and finance sector by examining actual cases identified through public reporting or as a computer fraud case investigated by the USSS. Each case was analyzed from a behavioral and a technical perspective to identify behaviors and communications in which the insiders engaged prior to and during their harmful activities.[92] Michele Keeney et al. analyzed insider attacks across all critical infrastructure sectors in which the insider's intent was to harm the organization, an individual, or the organization's data, information system, or network.[93] Subsequently, two additional reports followed with similar extensive research and attack analysis on insiders in the IT sector,[94] and threats to the government sector.[95] The reports include statistical findings and implications regarding technical details of the incidents, detection

---

[90] Cappelli et al., "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," 2004.

[91] Band et al., "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis|SEI Digital Library."

[92] Randazzo et al., *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*.

[93] Keeney et al., "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors."

[94] Eileen F. Kowalski, Dawn M. Cappelli, and Andrew P. Moore, "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/insiderthreat_it2008.pdf.

[95] Eileen F. Kowalski et al., "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/insiderthreat_gov2008.pdf.

and identification of the insiders, nature of harm, as well as insider planning, communication, behavior, and characteristics.[96]

Additionally, completed studies on police corruption and fraud, and studies on sabotage and the exploitation of information systems have been completed.[97] Cole analyzes incidents of insider theft, sabotage, and spying from private sector and public sector entities, which draw attention to pitfalls organizations are missing by not putting protective measures in place. Case studies are reviewed and technology remedies are applied to counter the insider threat.[98]

F. SHOULD WE GO BACK TO BASICS ON PREDICTING INSIDER THREATS WHEN IT COMES TO INSIDER FRAUD AND EMBEZZLEMENT?

While the motivating factor among perpetrators of fraud and embezzlement cases was hard to ascertain in a majority of the cases examined in "2012 Report to the Nations," produced annually by the ACFE, those discovered included supporting gambling addictions and problems with substance abuse, or in some cases, providing for a loved one. The report shows the average duration for a major embezzlement scheme is nearly five years with some lasting as long as 20 years before they are uncovered.[99]

The ACFE Report indicated that most occupational fraudsters who were trusted insiders within organizations are first-time offenders with clean employment histories. Approximately 87% of occupational fraudsters have never been charged with or convicted of a fraud-related offense, and 84% have never been punished or terminated by an employer for fraud-related conduct.[100] Research has consistently shown that most

---

[96] Cappelli et al., "Common Sense Guide to Prevention and Detection of Insider Threat, 3rd Edition—Version 3.1."

[97] Carol Meyers, Sarah Powers, and Daniel Faissol, "Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches," *Lawrence Livermore National Laboratory*, April 2009, https://e-reports-ext.llnl.gov/pdf/379498.pdf.

[98] Cole and Ring, *Insider Threat*.

[99] Joel Griffin, "Major Embezzlement Cases on the Rise," *SecurityInfoWatch.com*, May 20, 2013, http://www.securityinfowatch.com/article/10946366/marquet-international-report-finds-major-embezzlement-cases-increased-in-2012.

[100] "2012 Report to the Nations—Key Findings and Highlights."

trusted insiders who commit fraud and embezzlement within organizations do not have a previous criminal record.[101]

G. THE FRAUD TRIANGLE

Trying to explain why insider threats occur, specifically fraud and embezzlement, is complicated. If research shows that most people who commit fraud against their employers are not career criminals, are trusted employees who have no criminal history, and who when caught, do not consider themselves to be lawbreakers, what is being missed? Common factors contribute to the vulnerability of these otherwise normal, law-abiding persons, to commit fraud.

Research indicated that the fraud triangle explains one of the more highly regarded theories as to why insider fraud occurs. Developed in the early 1950s by criminologist Donald Cressey,[102] the fraud triangle is one of the most well-known fraud-specific models published.[103] Cressey interviewed imprisoned bank embezzlers and observed that many of these formerly law-abiding citizens, people he called "trust betrayers," had a "non-sharable financial problem."[104] This observation led him to develop the fraud triangle, depicted in Figure 1.

---

[101] Green, "White-Collar Crime and the Study of Embezzlement," 95–106; Cressey, *Other People's Money; A Study in the Social Psychology of Embezzlement*; Cappelli et al., "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," 2004; Band et al., "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis|SEI Digital Library"; Wells, *Corporate Fraud Handbook: Prevention and Detection*.

[102] Wells, *Corporate Fraud Handbook: Prevention and Detection*; Green, "White-Collar Crime and the Study of Embezzlement"; W. Albrecht et al., *Fraud Examination* (Stamford, CT: Cengage Learning, 2008); Randazzo et al., *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*.

[103] Cressey, *Other People's Money; A Study in the Social Psychology of Embezzlement*, ch. 1.

[104] Non-sharable problems all involve some sort of embarrassment, shame, or disgrace. More importantly, they all threaten the fraudster's status as a person trusted by others.

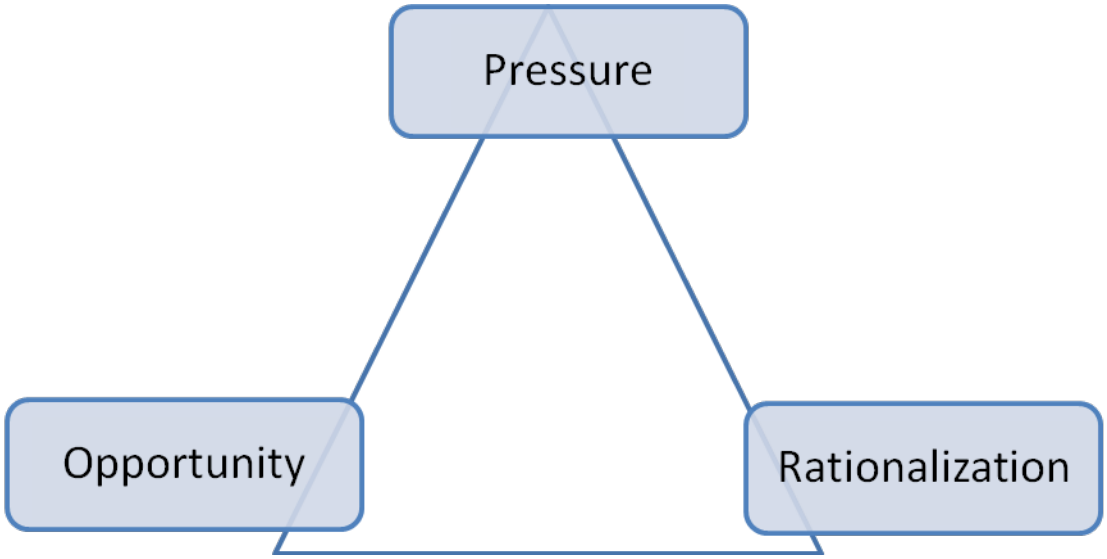

Figure 1. The Fraud Triangle

Cressey's theory holds that for fraud to occur, three dimensions must all be present: pressure, opportunity, and rationalization.[105]

> ***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 needed to resolve their problem in secret, making it "non-sharable."[106]
>
> ***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 employees' ability to commit fraud and then effectively detect it when it occurs.[107]
>
> ***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 miss-treatment, 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 it is possible repay it. At the other end of the spectrum,

[105] Cressey, *Other People's Money; A Study in the Social Psychology of Embezzlement*, ch. 1.

[106] Ibid.

[107] Ibid.

rationalization incorporates misunderstanding of the severity of the fraudulent acts or apathy about their consequences.[108]

Cressey emphasizes that in the vast majority of cases he studied, at some time prior to the crime, the individuals believed certain situations existed in which trust violation was acceptable. When subjects applied these situations to their personal circumstances, trust was violated. "Further, the neutralization aspect of Cressey's process is consistent with the theory of differential association in that there was a gradual erosion of the subjects' morality, culminating in the justification for embezzlement, assuming that the excuses were not post factum impressions.[109]" While Cressey's offenders did not associate with persons who directly influenced their decisions to embezzle, some evidence exists that through contacts with others, they came to believe that some business offenses were merely technical violations rather than morally wrong.[110] Justifications for committing the crime such as, "I was only borrowing the money" or "I deserve a little more in my paycheck for all the work I do around here," come to light. It is also noted that the research did not conclude that Cressey's theory was an absolute reason for individuals committing fraud or embezzlement within organizations; however, it was valid in many circumstances surrounding an individual's motivations.[111]

H. THE ADDICTION ANGLE TO INSIDER THREATS

Greitzer et al., in their research on identifying at risk employees, considers "concerning behavior" as an indicator for at risk employees; however, they fail to identify addictive characteristics as part of the behavioral indicators.[112] This finding is consistent

[108] Cressey, *Other People's Money; A Study in the Social Psychology of Embezzlement,* ch. 1.

[109] Green, "White-Collar Crime and the Study of Embezzlement."

[110] Ibid.

[111] Ibid; Ragatz, Fremouw, and Baker, "The Psychological Profile of White-collar Offenders Demographics, Criminal Thinking, Psychopathic Traits, and Psychopathology," 978–97; Dorothy Zietz, *Women Who Embezzle or Defraud: A Study of Convicted Felons* (New York: Praeger Publishers, 1981).

[112] Greitzer et al., "Identifying At-Risk Employees."

in the literature reviewed.[113] Researchers on recent insider threat studies might be missing a key connection between addictions to gambling or prescription pain medication and the perpetration of illicit financial crime activity by trusted insiders within organizations.

1. Gambling

According to the National Research Council (NRC) study on Pathological Gambling, "the existence of a number of costly financial problems are related to pathological gambling, including a variety of crimes such as embezzlement, loss of employment, and bankruptcy."[114] The NRC study stated, "Although the research in this area is sparse, it suggests that the magnitude and extent of personal consequences on the pathological gambler and on his family may be severe."[115] Other research indicates that, where casino jurisdictions exist, an increase nationally in the statistics for increased embezzlement arrests appears to occur.[116] The National Gambling Impact Study classifies pathological gambling as an impulse disorder that may include such activities "as committing illegal acts such as forgery, fraud, theft or embezzlement to finance gambling."[117] In a recent paper, entitled "Pathological Gambling and "Other Behavioral" Disorders," the author reports on increased drug behavioral disorders and impulse control disorders (ICD), which include pathological gambling and compulsive buying disorder.

---

[113] "Insider Fraud Is Common and Often Flies Under Corporate Radar," *Security: Solutions for Enterprise Security Leaders* 48, no. 11 (November 2011): 12–15; Darrell D. Dorrell and Gregory A. Gadawski, "Investigating Embezzlement: Three Don'ts," *Value Examiner*, August 7, 2012, 26–28; Nancy Blodgett, "Stealing Your Practice Blind," *ABA Journal* 73, no. 8 (August 1, 1987): 78–82; Ragatz, Fremouw, and Baker, "The Psychological Profile of White-collar Offenders Demographics, Criminal Thinking, Psychopathic Traits, and Psychopathology."

[114] National Research Council, *National Research Council. Pathological Gambling: A Critical Review, Committee on the Social and Economic Impact of Pathological Gambling, Committee on Law and Justice, Commission on Behavioral and Social Sciences and Education.*

[115] Ibid.

[116] Albanese, "White Collar Crimes and Casino Gambling: Looking for Empirical Links to Forgery, Embezzlement, and Fraud," 333–47; Ricardo C. Gazel, Dan S. Rickman, and William N. Thompson, "Casino Gambling and Crime: A Panel Study of Wisconsin Counties," *Managerial & Decision Economics* 22, no. 1–3 (January 2001): 65–75; Richard J. Rosenthal and Henry R. Lesieur, "Pathological Gambling and Criminal Behavior," in *Explorations in Criminal Psychopathology: Clinical Syndromes with Forensic Implications*, ed. Louis B. Schlesinger (Springfield, IL: Charles C. Thomas Publisher, 1996), 149–169.

[117] University of North Texas University, "National Gambling Impact Study Commission Final Report," 1999, http://govinfo.library.unt.edu/ngisc/reports/fullrpt.html.

The study stresses that a possible connection can be made between these disorders and that health practitioners and counselors should be knowledgeable of the implied correlation.[118]

Early research conducted on embezzlement cases revealed that the most frequent factor in motives identified with the perpetrators (trusted insiders) of embezzlement cases was gambling.[119] "The personal and social effects of pathological gambling often include psychological distress, significant financial losses, family problems, legal and employment difficulties, and suicide."[120] Gerhard Meyer and Michael Stradler indicate in their research, "The majority of clinical studies on pathological gamblers in outpatient treatment centers and self-help groups indicate that a high percentage of subjects committed criminal offenses in order to finance their gambling."[121] According to Max Abbott et al., between one and two-thirds of problem gamblers engaged in treatment or mutual help groups like Gamblers Anonymous (GA) report having committed gambling-related offences.[122] Several studies have reported high rates of gambling-related criminal activity amongst severe problem gamblers.[123]

---

[118] Richard J. Frances, Irvin Miller Miller, and Avram H. Mack, *Clinical Textbook of Addictive Disorders, Third Edition*, 3, illustrated (New York: Guilford Press, 2011), http://books.google.com/books/about/Clinical_Textbook_of_Addictive_Disorders.html?id=JJk52UeE6hYC.

[119] Peterson, "Why Honest People Steal," 94–103; Cressey, *Other People's Money; A Study in the Social Psychology of Embezzlement*; Henry R. Lesieur, *The Chase: Career of the Compulsive Gambler*, vol. xxi (Oxford, England: Anchor, 1984); Henry R. Lesieur and Robert L. Custer, "Pathological Gambling: Roots, Phases, and Treatment," *American Academy of Political and Social Science* 474, no. 1, (July 1, 1984): 146–56; Gerhard Meyer and Michael A. Stadler, "Criminal Behavior Associated with Pathological Gambling," *Journal of Gambling Studies* 15, no. 1 (March 1, 1999): 29–43, doi:10.1023/A:1023015028901; Alex Blaszczynski, "Criminal Offences in Pathological Gamblers," *Psychiatry, Psychology and Law* 1, no. 2 (1994): 129–38, doi:10.1080/13218719409524836.

[120] Larry L. Ashley and Karmen K. Boehlke, "Pathological Gambling: A General Overview," *Journal of Psychoactive Drugs* 44, no. 1 (March 2012): 27–37, doi:http://dx.doi.org.libproxy.nps.edu/10.1080/02791072.2012.662078.

[121] Meyer and Stadler, "Criminal Behavior Associated with Pathological Gambling," 29.

[122] Max W. Abbott, Brian G. McKenna, and Lynne C. Giles, "Gambling and Problem Gambling Among Recently Sentenced Male Prisoners in Four New Zealand Prisons," *Journal of Gambling Studies* 21, no. 4 (Winter 2005): 537–58, doi:10.1007/s10899-005-5562-6.

[123] Alex Blaszczynski and Derrick Silove, "Pathological Gambling: Forensic Issues," *Australian and New Zealand Journal of Psychiatry* 30, no. 3 (June 1, 1996): 358–69, doi:10.3109/00048679609065000; Blaszczynski, McConaghy, and Frankova, "Crime, Antisocial Personality and Pathological Gambling," 137–52, doi:10.1007/BF01019760; Iain (R I F) Brown, "Pathological Gambling and Associated Patterns of Crime: Comparisons with Alcohol and Other Drug Addictions," *Journal of Gambling Behavior* 3, no. 2 (June 1, 1987): 98–114, doi:10.1007/BF01043449.

Academic research and the prevalence of numerous criminal cases have shown the existence of a relationship between criminal behavior and pathological gambling.[124] Research indicates that pathological gambling is frequently associated with financial, vocational, interpersonal, and psychiatric problems. Some gamblers also experience substantial legal problems related to gambling.[125] These types of related illegal behaviors typically include fraudulent financial dealings, such as embezzlement, theft, writing bad checks, and surreptitious use of another person's credit or using another's personal identity to obtain credit cards or obtain loans in that person's name.[126] Such crimes are frequently committed in desperation, either to cover up financial damage from gambling related losses or to fund further gambling sprees. Illegal activities may intensify the severity of gambling-related problems, and ultimately, result in arrest, conviction and incarceration, or in desperation, suicide.[127] John Kindt, in his study on the success of tobacco lawsuits, argues that the gambling industry should be financially held responsible for pathological gamblers because, "Pathological gamblers tend to engage in forgery, theft, embezzlement, drug dealing, and property crimes to pay off gambling debts."[128]

Henry Lesieur's early research on pathological gamblers describes the development of excessive gambling in individuals wherein the gambler's intensifying financial pressures and increasing desire to maintain the ability to gamble causes the gambler ultimately to become involved in criminal activity. This work accurately describes behaviors of trusted insiders engaged in fraud or embezzlement with the need to provide a mechanism of funding 'their gambling activities at any cost. Lesieur

---

[124] Rosenthal and Lesieur, "Pathological Gambling and Criminal Behavior," in *Explorations in Criminal Psychopathology: Clinical Syndromes with Forensic Implications*; Stephenie Overman, "Addiction: Odds Are Gamblers Cost Companies," *HRMagazine* 35, no. 4 (April 1990): 50; Blaszczynski, "Criminal Offences in Pathological Gamblers."

[125] Lesieur, "Gambling, Pathological Gambling and Crime," in *Handbook on Pathological Gambling*, 89–110.

[126] *National Gambling Impact Study Commission, Final Report.*

[127] Ledgerwood et al., "Clinical Features and Treatment Prognosis of Pathological Gamblers with and Without Recent Gambling-Related Illegal Behavior," 294–301; Lesieur, *The Chase*; Alex Blaszczynski and Eimear Farrell, "A Case Series of 44 Completed Gambling-related Suicides," *Journal of Gambling Studies* 14, no. 2 (1999): 93–109.

[128] John Warren Kindt, "The Costs of Addicted Gamblers: Should the States Initiate Mega-Lawsuits Similar to the Tobacco Cases?," *Managerial and Decision Economics* 22, no. 1/3 (January 1, 2001): 22.

describes a roadmap of the pathological gambler who makes a series of wrong turns conducting illegal actions that then cascade into making bad decisions that will ultimately destroy the gambler in the end.[129]

Studies vary on the exact pervasiveness in the trend with respect to the growth in the population of pathological gamblers.[130] Statistics indicate that the prevalence of the disorder is on the rise. In 1976, research estimated that the base rate of the U.S. adult population who constituted pathological gamblers was 0.77%.[131] In its 1997 meta-analysis of literature on problem and pathological gambling prevalence, the Harvard Medical School Division on Addictions estimated at the time that the number of adult problem and pathological gamblers in the United States was 7.5 million. The study also estimated adolescent problem and pathological gamblers numbered 7.9 million.[132] Current studies, however, estimate that approximately 1.6–5% of the adult gambling population in America experiences significant problems because of their gambling activities.[133] This percentage is presumed to be even higher among special populations including those comprising young adults, people with mental health disorders, and incarcerated individuals.[134]

Across numerous countries, it is recognized that problem gambling is a significant public health concern with between 1–2% of the population estimated to be affected. Despite having a lower prevalence than substance abuse disorders, such as alcoholism,

---

[129] Lesieur, *The Chase*; Rosenthal and Lesieur, "Pathological Gambling and Criminal Behavior," in *Explorations in Criminal Psychopathology: Clinical Syndromes with Forensic Implications*, 149–69.

[130] Ledgerwood et al., "Clinical Features and Treatment Prognosis of Pathological Gamblers with and Without RecentGambling-Related Illegal Behavior"; Howard J. Shaffer, Matthew N. Hall, and Joni Vander Bilt, "Estimating the Prevalence of Disordered Gambling Behavior in the United States and Canada: A Research Synthesis," *American Journal of Public Health* 89, no. 9 (September 1999): 1369–75; "How Many Pathological Gamblers Are There?" accessed February 1, 2014, http://www.americangaming.org/industry-resources/faq/how-many-pathological-gamblers-are-there.

[131] Ashley and Boehlke, "Pathological Gambling," 28.

[132] *National Gambling Impact Study Commission, Final Report*, 4–1.

[133] Ledgerwood et al., "Clinical Features and Treatment Prognosis of Pathological Gamblers with and Without Recent Gambling-Related Illegal Behavior"; Ashley and Boehlke, "Pathological Gambling."

[134] Nigel Turner et al., "The Relationship of Problem Gambling to Criminal Behavior in a Sample of Canadian Male Federal Offenders," *Journal of Gambling Studies* 25, no. 2 (June 2009): 153–69, doi:10.1007/s10899-009-9124-1.

problem gambling often presents as an acute disorder.[135] Problems can emerge within a relatively short period of time and the effects are often thought to extend to as many as, "10 to 15 people who have contact with the gambler, including spouse, children, parents, and fellow gamblers, people stolen from, employers and employees."[136]

As one researcher has noted:

> As was the case with alcoholism for many years, compulsive gambling often is unrecognized and misunderstood. Perhaps this is because compulsive gambling is a drugless addiction. A pathological gambler will end up in one of three places: in recovery, institutionalized in a hospital or jail, or dead. The keys to treatment are education, prevention, and intervention.[137]

2. Pain Prescription Medication

Addictive gambling is pathological. However, pathology extends beyond the psychological to the physical. Recent criminal cases involving pain prescription medication are indicative of the growing concern regarding trusted insiders within organizations committing fraud and embezzlement to support their addiction. In 2012, the former office manager for a dental office was sentenced to 30 months in federal prison for embezzling over $174,000. According to the U.S. Attorney for the Western District of Washington, "The defendant committed a long-running scheme of financial crimes to feed her oxycodone addiction and betray the trust of her employer." Commenting further on the case, the U.S. Attorney also noted, "People need to recognize that prescription drug abuse is growing in communities, leaving heavy damage in its wake."[138]

---

[135] Paul Delfabbro, "Problem and Pathological Gambling: A Conceptual Review," *Journal of Gambling Business & Economics* 7, no. 3 (September 2013): 35–53.

[136] Lesieur and Custer, "Pathological Gambling: Roots, Phases, and Treatment," 148.

[137] Denise Phillips, "Gambling: The Hidden Addiction," *Behavioral Health Management* 25, no. 5 (October 2005): 32–37.

[138] U. S. Attorney's Office (USAO), "U.S. Attorney's Office—U.S. Department of Justice," September 7, 2012, http://www.justice.gov/usao/waw/press/2012/September/bowman.html.

According to the Centers for Disease Control and Prevention, prescription drug abuse is the nation's fastest growing drug problem and has been classified as an epidemic.[139] According to a release from the Department of Justice, it is reported that:

> National statistics show an increasing level of unlawful drug diversion and abuse of pharmaceutical controlled substances, as well as overdoses of such drugs resulting in rising medical costs. Studies reflect that hospital admissions attributable to prescription drug abuse and overdose have increased 500% over the last 10 years, and are currently costing the United States more than $1 billion dollars in health care costs each year.[140]

Government employees are not immune to committing crimes to support a pain medication addiction as noted in another 2012 insider fraud case; the former executive director and a co-conspirator of a city-county convention center was convicted of embezzlement. "They devised a scheme to steal money that was intended for the greater good of the community,"[141] stated the U.S. Attorney for the Western District of Kentucky. "In doing so, they violated the public's trust and harmed an important community asset." The trusted insider embezzled $250,000 to support his addiction to pain medication.[142]

"The economic cost of nonmedical use of prescription opioids in the United States totals more than $50 billion annually; lost productivity and crime account for the vast majority (94%) of these costs."[143] In a 2006 Congressional Hearing, Laxmaiah Manchikanti, MD, the chief executive officer of the American Society of Interventional Pain Physicians testified, "Prescription drug abuse today is second only to marijuana abuse…. initiates to drug abuse started with prescription drugs (especially pain

---

[139] The White House, "Office of National Drug Control Policy," 2012, http://www.whitehouse.gov/ondcp.

[140] U. S. Attorney's Office (USAO), "Health Care Professional Pleads Guilty to Product Tampering Demerol Diverted at Bellevue, WA Surgery Clinic," May 28, 2009, http://www.justice.gov/usao/waw/press/2009/may/gibson.html.

[141] USDOJ, "Convention Center's Former Executive Director Sentenced to 24 Months in Prison for Embezzlement."

[142] Ibid.

[143] Ryan N. Hansen et al., "Economic Costs of Nonmedical Use of Prescription Opioids," *The Clinical Journal of Pain* 27, no. 3 (2011): 194, doi:10.1097/AJP.0b013e3181ff04ca.

medications) more often than with marijuana."[144] In a recent article in the *Journal of Safety Research* about prescription addiction issues in the workplace, it was noted, "Prescription opioids are killing Americans at more than five times the rate that heroin is, according to the most recent numbers from the Centers for Disease Control and Prevention."[145] Commenting about the growing abuse of opioids, and the recent death of actor Phillip Seymour, investigative reporter Joel Achenbach noted, "These drugs are sold under such familiar brand names as OxyContin, Vicodin and Percocet and can be found in medicine cabinets in every city in American society."[146]

Research examining news reports and government media releases indicate that numerous recent criminal investigations have revealed a number of insider fraud and embezzlement cases related to prescription drug addiction,[147] and gambling addiction.[148] A significant overlap also appears to exist between pathological gambling and chemical dependency.[149] Research further indicates an underlying organizational vulnerability perpetrated by individuals who have been compromised by addictive behavior.[150]

It is also important to note that the research indicated that a significant portion of these recent criminal cases have involved mid- to high-level "trusted insider" government

---

[144] Laxmaiah Manchikanti, "Prescription Drug Abuse: What Is Being Done to Address This New Drug epidemic? Testimony before the Subcommittee on Criminal Justice, Drug Policy and Human Resources.," *Pain Physician* 9, no. 4 (2006): 287.

[145] Leonard J. Paulozzi, "Prescription Drug Overdoses: A Review," *Journal of Safety Research* 43, no. 4 (September 2012): 283–89, doi:10.1016/j.jsr.2012.08.009.

[146] Joel Achenbach, "Philip Seymour Hoffman's Death Points to Broader Opioid Drug Epidemic," *Washington Post*, sec. National, February 8, 2014, http://www.washingtonpost.com/national/health-science/philip-seymour-hoffman-heroin-death-points-to-broader-opioid-drug-epidemic/2014/02/07/42dbbc5a-8e61-11e3-b46a-5a3d0d2130da_story.html.

[147] USDOJ, "Convention Center's Former Executive Director Sentenced to 24 Months in Prison for Embezzlement"; Jason Geary, "Dentist Gets Probation in Prescription Drug Case|TheLedger.com," July 20, 2013, http://www.theledger.com/article/20130720/NEWS/130729923?p=1&tc=pg.

[148] Patrick, "Former Brentwood Official Admits Embezzling Money, Gambling It Away"; Maryclaire Dale, "Pa. Church's Ex-CFO Gets 2–7 Years in $900k Theft," accessed September 30, 2013, http://bigstory.ap.org/article/pa-churchs-ex-cfo-gets-2-7-years-900k-theft.

[149] Rosenthal and Lesieur, "Pathological Gambling and Criminal Behavior," in *Explorations in Criminal Psychopathology: Clinical Syndromes with Forensic Implications*, 32.

[150] Overman, "Addiction"; Metcalfe, "Rita Crundwell vs. Harriette Walters: Who Embezzled Better?"; Alex P. Blaszczynski and Neil McConaghy, "Criminal Offenses in Gamblers Anonymous and Hospital Treated Pathological Gamblers," *Journal of Gambling Studies* 10, no. 2 (June 1, 1994): 99–127, doi:10.1007/BF02109935.

officials from local, state, and federal agencies.[151] For these reasons, it is critical for the homeland security professional, at an executive level, to be aware that an insider can devastate the operation of any organization, whether it is a private sector corporation or a government agency.[152] Employees with an addictive personality behavior can greatly increase risk to the organization for which they work.[153] To make this point, history has also revealed that at least four Americans convicted as spies and who conducted espionage against the U.S. government, did so to help alleviate debts incurred because of compulsive gambling.[154]

I. SHOULD MOTIVES MATTER IN REGARD TO REPORTING CRIME?

Accurate crime statistics are hard to place on gambling-related criminal offenses, especially in fraud and embezzlement cases. Many police departments and law enforcement agencies do not have specific reporting requirements as to motives or causation of the crime.[155]

---

[151] Southall, "17-Year Term for Official in Tax Scam"; Spagat, "Ex-San Diego Mayor's Gambling Wagers Top $1B"; Michael Schwirtz and Ravi Somaiya, "Vice Admiral Is Suspended in Gambling Investigation," *New York Times*, September 28, 2013, http://www.nytimes.com/2013/09/29/us/vice-admiral-is-suspended-in-gambling-investigation.html?_r=0.

[152] Walter Pavlo, "Fmr Dixon, IL Comptroller, Rita Crundwell, Sentenced to 19 1/2 Years in Prison," *Forbes*, February 14, 2013, http://www.forbes.com/sites/walterpavlo/2013/02/14/fmr-dixon-il-comptroller-rita-crundwell-sentenced-to-19-12-years-in-prison/; Josh Funk, "Neb. AG: Senator Misused Campaign Cash at Casinos," accessed September 30, 2013, http://bigstory.ap.org/article/neb-ag-senator-misused-campaign-cash-casinos.

[153] Marty Griffin, "Dozens of TSA Employees Fired, Suspended for Illegal Gambling Ring at Pittsburgh Int'l Airport," *CBS Pittsburgh*, September 19, 2013, http://pittsburgh.cbslocal.com/2013/09/19/dozens-of-tsa-employees-fired-suspended-for-illegal-gambling-ring-at-pittsburgh-intl-airport/; Carolyn Thompson, "James Bagarozzo, Buffalo Parking Meter Mechanic, Jailed In $210K Scam," *Huffington Post*, August 17, 2013, http://www.huffingtonpost.com/2013/08/17/theft-of-840k-coins-sends_0_n_3772807.html; CBS News, "Pa. School 'Lunch Ladies' Allegedly Stole $94K to Gamble," February 27, 2013, http://www.cbsnews.com/8301-504083_162-57571435-504083/school-lunch-ladies-accused-of-stealing-$94k-to-gamble/.

[154] Kramer, Heuer, and Crawford, "Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage."

[155] Ziegler and Lovrich, "Pain Relief, Prescription Drugs, and Prosecution"; G. G. Smith, H. Wynne, and T. Hartnagel, *Examining Police Records to Assess Gambling Impacts: A Study of Gambling-related Crime in the City of Edmonton* (Edmonton, Alberta, Canada: The Alberta Gaming Research Institute, 2003); Blaszczynski and Silove, "Pathological Gambling."

Smith et al. express the view that:

> Scholars researching this topic" of accurate crime related statistics directly as a result of pathological gambling are, "facing an inherent paradox; the fact that official police statistics and court records do not show gambling-related crime to be a serious problem, yet knowing that police and court databases are incomplete to the extent that gambling is seldom identified as a motive or precipitating factor for crime.[156]

Arthur, Williams and Belanger, who investigated how increased legal gambling availability has affected crime in Alberta, emphasize in their study that overall jurisdictional crime rates were useful in analyzing trends in crime and specific crime rates by category.

> However, the main limitation of this type of data is that the causes of crime are not recorded within these statistics. One potential way to address this problem is to examine the original police report, where the responding officer has the option to record, in detail, any causes and mitigating factors of the incident to which she/he is responding.[157]

This situation appears to be a consistent issue for many police jurisdictions with regard to causality in crime. Local, state, and federal law enforcement agencies in the United States are required to report annually to the FBI Uniformed Crime Report, statistics concerning acts of crime by gender, age, and jurisdiction; however, motive and causality are not required statistical data in most criminal cases, especially in fraud and embezzlement crimes, as it is a Schedule 2 offense (the only required reporting of those offenses is age and gender).[158]

As was previously indicated in Henry Lesieur's research on gambling addiction and the pathological gamblers' need to fund their addiction once they have run out of an income source, the risk intensifies in individuals to commit criminal offenses to sustain their habit. If these individuals are trusted insiders operating within an organization, fraud

---

[156] Smith, Wynne, and Hartnagel, *Examining Police Records to Assess Gambling Impacts: A Study of Gambling-related Crime in the City of Edmonton*, 4.

[157] Arthur, Williams, and Belanger, "The Relationship Between Legal Gambling and Crime in Alberta1," 49–84.

[158] "Offenses in Uniform Crime Reporting—Crime in the United States 2004," accessed March 7, 2014, https://www2.fbi.gov/ucr/cius_04/appendices/appendix_02.html.

and embezzlement is often the avenue of choice to fund their illegal behavior.[159] The research indicates that a problematic situation arises for accurate reporting statistics, when motives and causality of a criminal offense are not recorded in official police reports or investigative notes on financial crimes caused by addiction to gambling. The issue of causality and motive for the offender committing a crime is a concern, as Blaszcynski and Silove have noted:

> Accurate rates of the prevalence and extent of gambling-related criminal behaviors are difficult to obtain. Arrest and conviction rates are inadequate because gambling is not necessarily identified on conviction records as underlying the offense, and not all gambling related offenses are detected or offenders apprehended. Therefore, the true prevalence rate is likely to be underestimated.[160]

This state of affairs is an example of law enforcement personnel investigating an individual, who may also be a potential trusted insider within an organization, for fraud or embezzlement and not indicating in their reporting, the underlying motive or causation for the individual committing the criminal offense.

The United States Secret Service (USSS) as a federal law enforcement agency has, as one of its core investigative missions, the investigation of financial crimes cases.[161] It does not have a mechanism in place to record and report causation or motives of criminal financial crimes offenses in a format that can readily be used to provide a statistical analysis of causation or motives for the occurrence of a financial crime, whether for gambling or any other addiction-related motive.[162]

The Kentucky State Police (KSP) is the agency charged with retaining criminal police records and traffic offense reports for city and county law enforcement agencies throughout the Commonwealth of Kentucky. The KSP Records Division advises that it is

---

[159] Lesieur, *The Chase*.

[160] Blaszczynski and Silove, "Pathological Gambling," 360.

[161] "United States Secret Service," accessed January 21, 2014, http://www.secretservice.gov/.

[162] As the Special Agent in Charge of the U.S. Secret Service, Louisville Field Office, with over 25 years of experience in criminal investigations, the author can report that no requirement exists for Special Agents to include in their case reports, causality or motive, for a perpetrator of a criminal offense in a financial crimes investigation, as to their reason for committing a criminal offense.

not currently able to capture causation (motives) for most criminal offenses, with the exception of fatal traffic accidents.[163]

J. INSIDERS HAVE THE ADVANTAGE: PREVENTION, DETECTION, AND MITIGATION IS VITAL

The literature agrees that trusted insiders have substantial advantages over others who might want to damage an organization. Dawn Cappelli et al. summarized it well in their "3rd Edition of Common Sense Guide to Prevention and Detection of Insider Threats:"

> Insiders can bypass physical and technical security measures designed to prevent unauthorized access. Mechanisms such as firewalls, intrusion detection systems, and electronic building access systems are implemented primarily to defend against external threats. However, not only are insiders aware of the policies, procedures, and technology used in their organizations, but also they are often aware of their vulnerabilities, such as loosely enforced policies and procedures or exploitable technical flaws in networks or systems.[164]

Andy Jones advocates that stopping and apprehending a malicious insider involves more than implementing strong technical measures; ultimately, the problem is a people issue. "Advocating strong physical, procedural and personnel measures in an organization will reduce the likelihood of a malicious attack occurring and increase the likelihood of an attack being detected."[165] Consensus exists in the literature that to detect insider threats as early as possible, or to prevent them altogether, management, IT, human resources, security officers, and others in the organization must understand the psychological, organizational, and technical aspects of the problem, as well as how they coordinate their actions over time.[166]

---

[163] Kentucky State Police, "Commonwealth of Kentucky 2012 Crime Report," 2013, http://www.kentuckystatepolice.org/pdf/cik_2012.pdf.

[164] Cappelli et al., "Common Sense Guide to Prevention and Detection of Insider Threat, 3rd Edition—Version 3.1."

[165] Andy Jones, "Catching the Malicious Insider," *Information Security Technical Report* 13, no. 4 (November 2008): 220–24, doi:10.1016/j.istr.2008.10.008.

[166] Eric Savitz and Kevin Cunningham, "Insider Attacks Are Impacting Your Bottom Line," *Forbes.com*, December 23, 2011, 11–11; Silowash et al., "Common Sense Guide to Mitigating Insider Threats, 4th Edition"; Greitzer et al., "Combating the Insider Cyber Threat."

A common theme throughout the literature concludes that, regardless of the size of the organization, prevention, early detection, and mitigation, with buy-in from all levels of the corporate or organization management structures, are critical components. Building a layered and well-defined approach to insider fraud is clearly the goal. Having a plan in place to defend against, prevent, and deal with an insider attack, should one occur, is vital for any organization's' ability to recover quickly from an insider event of any magnitude.[167]

Academic literature suggests that authorized employees are usually familiar with some or all the internal process of their organization. For example, insiders are almost always aware of the policies, procedures, security countermeasures, and the associated vulnerabilities, which relate to them, or they have the ability to gain that knowledge without suspicion.[168] Illicit insider activity in the IT sector in particular serves as a prime example of the importance of educating and training all employees at every level of the organization in security awareness issues, acceptable use policies, and the key role each employee can play in prevention and early detection of insider activities. It is critical that employees from clerical staff to high-level managers in any organization who observe unusual activity or become aware of an insider's plans must have a mechanism in place to report their knowledge or suspicions. Education that helps employees to recognize threats and encourages them to report unusual behaviors is a critical step in the early detection of insider activity. Creating a culture of security in which employees understand that they are an important line of defense against harmful and abusive attacks on systems and data is a key component of any strategy to mitigate the threat of illicit insider activity.[169]

---

[167] Silowash et al., "Common Sense Guide to Mitigating Insider Threats, 4th Edition"; Greitzer et al., "Combating the Insider Cyber Threat"; Wells, *Corporate Fraud Handbook: Prevention and Detection*.

[168] Cappelli, Moore, and Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, 2012; Randazzo et al., *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*; Greitzer et al., "Combating the Insider Cyber Threat"

[169] Kowalski, Cappelli, and Moore, "Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector"; Cappelli, Moore, and Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, 2012; Gelles, Brant, and Geffert, "Building A Secure Workforce: Guard Against Insider Threat."

K. LEADING INDICATORS SUGGEST MORE NEEDS TO BE DISCOVERED ABOUT INSIDER THREAT'S CONNECTED TO ADDICTION AS A MOTIVE FOR COMMITTING FRAUD AND EMBEZZLEMENT

Insider threats and insider fraud have been studied, researched, and documented. Clear definitions of insider threats, parameters around possible causes, predictive models, and best practices for prevention, early detection, and mitigation have been established.[170] However, the research is lacking more in depth analysis and case studies on actual insider events in which a relationship to addiction exists as the motivating factor for the trusted insiders committing their crime.

Each year, federal law enforcement agencies investigate hundreds of criminal cases involving insider crime.[171] Researchers have studied a relatively small percentage of the actual insider fraud and embezzlement cases.[172] Important lessons are to be learned regarding why insider threats and insider fraud and embezzlement are so pervasive. Research indicates that a gap exists on scientific case studies regarding addictive personality behavior and addiction to gambling and prescription drug abuse as a possible indicator of predictive insider threats. Recent criminal cases point to a trend toward insiders committing fraud and embezzlement due to pressure brought on by an addiction. Research also indicates that motives for why individuals commit fraud and embezzlement are not readily accessible from the Uniformed Crime Reports or from actual law enforcement documentation reporting these crimes.

Press reports and open source records also indicate that public and government officials are not immune from committing fraud and embezzlement within their organizations, with addiction as a mitigating factor for their illegal behavior. Compelling evidence exists linking trusted insiders committing financial crimes offenses within

---

[170] Cappelli, Moore, and Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, 2012.

[171] Management and Organization Division, *United States Secret Service Annual Statistical Report—Fiscal Year 2013* (Washington, DC: Department of Homeland Security, 2013).

[172] Cappelli, Moore, and Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, 2012.

organizations, to behavioral addictive patterns, such as an addiction to gambling, or pain prescription medication. Further research examining this connection is warranted.

III. U.S. SECRET SERVICE CASE STUDIES

This chapter focuses on an examination of the USSS role in investigating fraud and embezzlement cases and also looks at the results from four of its field offices that reviewed 10 closed criminal cases in each office involving fraud and embezzlement to determine if addiction was a causal factor for the insiders' illegal activity.

The USSS, under 18 U.S. Code 1056, is authorized to investigate financial crimes. As one of the agency's primary core investigative functions, it has historically been actively involved with investigations of fraud and embezzlement criminal cases conducted by trusted insiders within private sector, non-profit, and public sector organizations.[173]

A. DEFINING THE SECRET SERVICE ROLE IN CRIMINAL INVESTIGATIONS

In 2015, the USSS will celebrate its 150th year as one of the oldest federal law enforcement agencies in the nation. While best known for its mission of protecting the President and other senior officials, the USSS was created in 1865 under the Department of Treasury at the end of the Civil War for the investigation of counterfeit currency, a mission it is still mandated to conduct.

Today, the agency's primary investigative mission is to safeguard the payment and financial systems of the United States. This protection has been historically accomplished through the enforcement of counterfeiting statutes to preserve the integrity of U.S. currency, coin, and financial obligations.

Since 1984, the USSS' investigative responsibilities have expanded to include crimes that involve financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, electronic funds transfers, and money laundering as it relates to the agency's core violations. To combat

[173] "United States Secret Service."

these crimes, the USSS has adopted a proactive approach that utilizes advanced technologies.[174]

In March 2003, as part of the enactment of the Homeland Security Act of 2002, the USSS was transferred from the Department of the Treasury to the Department of Homeland Security (DHS) as a distinct entity.[175] The USSS actively investigates the following types of crimes:

Threats against the president and other protected persons (Protective Intelligence)
Counterfeiting of currency (foreign and domestic)
Counterfeiting of U.S. commercial securities
False identification
U.S. Treasury check forgery
U.S. bond forgery
Electronic financial transaction fraud (commercial and consumer)
Access device fraud (credit and debit card fraud)
Computer fraud (scams, intrusion and hacking)
Embezzlement and misappropriation (public and private)
Food stamp fraud
Telecommunication fraud
Child pornography[176]

B. RELEVANT CRIMINAL CASE FACTS FROM THE SECRET SERVICE

The USSS' Management and Organization Division (MNO) provides comprehensive analytical products and compiles a wide variety of statistics, including reported fraud and embezzlement cases worked by USSS Field Offices. The following numbers were produced by the MNO.

---

[174] "United States Secret Service."

[175] Shawn Reese, *The U.S. Secret Service: An Examination and Analysis of Its Evolving Missions*, Report for Congress, CRS Report RL34603 (Washington, DC: Congressional Research Service, January 8, 2013), http://www.fas.org/sgp/crs/homesec/RL34603.pdf.

[176] "United States Secret Service."

In fiscal year 2013, the USSS closed 6,283 criminal financial crimes investigations, including cybercrimes, and arrested 5,148 individuals. In FY2013, the USSS efforts in combating financial crimes prevented an estimated 5.3 billion dollars in losses, of which 1.1 billion involved cybercrimes. These numbers do not include arrest statistics for USSS protective intelligence related investigations.

In FY2013, the USSS closed 498 cases of financial crimes investigations under the category of fraud, embezzlement and misappropriation investigations and arrested 587 individuals for these crimes.[177] These investigations are not restricted to only insiders, but are generally concentrated on insiders within organizations that have committed a financial crime. It should be noted that this category is not exclusive of all insider threat identified cases worked within the USSS, but is generally indicative of individuals committing financial crimes within organizations across public, private, and non-profit sectors.

1. Louisville Field Office

As the Special Agent in Charge of the USSS, Louisville Field Office, the author began to notice that an increased number of current fraud and embezzlement cases involving trusted insiders under investigation in Kentucky and Southern Indiana involved defendants addicted to gambling or pain prescription medication as primary motivators for committing their crimes.[178] After further examination, he discovered in the summer of 2013, that six out of 11 then-open criminal cases involving fraud or embezzlement conducted by trusted insiders were motivated by either a gambling addiction or an addiction to pain prescription medication. This discovery led the author to ask the research question for this thesis: Insiders are committing fraud and embezzlement within organizations: Is there a connection to addiction?

---

[177] Management and Organization Division, *United States Secret Service Annual Statistical Report—Fiscal Year 2013*.

[178] In reviewing an open criminal case in 2013, on a $1.7 million embezzlement investigation, the author discovered from the case agent that a trusted insider, responsible for the finances of a non-profit organization, had used the entire amount of funds he embezzled for the sole purpose of feeding a gambling addiction with which both he and his wife were involved. The investigation had revealed through wire transfers over the period of several months that $1.7 million had been transferred to several casinos and withdrawn by the insider and his spouse.

As a research objective for this project, he reviewed 10 closed and adjudicated criminal cases under the USSS financial crimes category of fraud, embezzlement and misappropriation investigations, in the Louisville Field Office. As stated above, and as a general rule, this category of financial crimes investigation involves individuals who have defrauded or embezzled funds within their control, as employees of public, private, or non-profit sector organizations. The objective of the research was to establish motivating factors for the criminal actions and reasons the defendant provided or could be determined during the course of the criminal investigation by the investigator or case agent for the illegal act.[179]

The results of this review are as follows.

Louisville Case 1

Organization Type: Private Sector
Insider Description Female, 61 y/o
Fraud Loss Dollar Amount: $1,382,495
Motives: Gambling addiction, but also used money for personal items
Dates of Embezzlement/Fraud: Embezzlement started in 2007, was discovered in late 2010, prosecuted in 2011
Incident description: Insider was the president of private company. Upon review of bank statements, the owner of the company was contacted by a bank representative about possible fraudulent actions of the now former president of the company. With closer inspection, it was revealed that the insider, over the course of roughly 3 years, made a number (18) of wire transfers and deposited checks (180) created by the insider for personal gain. The investigation began after suspicious activity occurred when it was known to the bank that the company was going out of business and neither the amount of money withdrawn nor number of checks written made sense. The insider covered her tracks by creating fraudulent reports to hide the illegal activity. The insider was convicted of wire fraud and embezzlement, pled guilty, and was sentenced to 41 months incarceration, two years supervised release, and restitution.

[179] The examination of the closed criminal cases was done because of the Special Agent in Charge of the Louisville Field Office participation in the Naval Postgraduate School Cohort 1206 Master's program. The examination only looked at the possible motive of the insiders' crime.

Louisville Case 2

Organization Type: Public Sector
Insider Description: Male, 43 y/o, Female, 52 y/o
Fraud Loss Dollar Amount: $233,120
Motives: Insider had an addiction to pain prescription addiction, specifically Lortab pills in this case
Dates of Embezzlement/Fraud: Insider began embezzlement in 2010, was discovered in 2011, and prosecuted federally in 2012.
Incident description: Insider was a public sector agency's Executive Director and over the duration of the insider's employment, the insider embezzled funds by creating fraudulent invoices, issuing fraudulent checks and splitting the proceeds with a collusive vendor for services never rendered for the agency. The embezzlement was uncovered when a bank teller became suspicious when the insider was making a bank deposit and called the police. When confronted, the insider admitted he was addicted to pain pills and the fraudulent scheme funded his addiction. The insider was convicted in federal court for one count of embezzlement and sentenced to two years in prison, two years supervised release, and ordered to pay restitution in the amount of $248,120.

Louisville Case 3

Organization Type: Public Sector
Insider Description: Male, 53 y/o
Fraud Loss Dollar Amount: $282,000
Motives: Insider had depleted trust fund and embezzled to maintain lifestyle above his means
Dates of Embezzlement/Fraud: Insider began embezzlement in 2002, was discovered in 2009, and prosecuted federally in 2010
Incident Description: Insider was an agency's fire chief and over the duration of the insider's employment, the insider embezzled funds by using the company credit card for personal expenses, issuing himself additional fraudulent paychecks and paying for personal expenses from a chartable account he exclusively maintained. The embezzlement was uncovered when the insider was fired and the Board of Trustees discovered the chartable account. When confronted, the insider stated the embezzlement was a result of his inability to manage the business end of his position. The insider was convicted in federal court for counts of mail fraud, wire fraud and money laundering, sentenced to three years and five months in prison, three years supervised release, and ordered to pay $190,000 in restitution.

Louisville Case 4

Organization Type: Private Sector
Insider Descriptors: Male, 26 y/o
Fraud Loss Dollar Amount: $17,313.11
Motives: Unknown (Possible drug addiction)
Dates of Embezzlement/Fraud: 11/23/09–02/25/11
Incident Description: Insider was an employee at a privately owned storage facility who had a responsibility of accepting rental payments from storage tenants; both in cash and in check form. The employee would embezzle cash payments while entering the amount paid on a computer system to allow the employee to show daily reconciliation sheets to the owner, which displayed correct payments for that day keeping the tenants in good standing. After providing a correct reconciliation sheet to the owner, the employee would return to the computer system and remove cash he had taken from the reconciliation sheets to allow the employee to produce a second sheet, not showing the cash he embezzled, that he would provide to the business accountant with the checks and/or extra cash he did not take. In this manner, it would balance the amount taken in as rental payments with the reconciliation sheets, thus showing no discrepancy between monies taken in on that day and the amount shown on the reconciliation sheets. Insider pleaded guilty to theft over $10,000 and was given a two-year suspended sentence, and ordered to pay full restitution of $17,313.11 to the victim.

Louisville Case 5

Organization Type: Private Sector
Insider Descriptors: Two Males, 27 and 33 y/o
Fraud Loss Dollar Amount: $311, 000
Motives: Insider's suffered from a pain prescription addiction
Dates of Embezzlement/Fraud: Criminal activity began in 2007, was discovered in 2011, and prosecuted in 2012
Incident Description: Both insiders worked in IT department of private company, and had access to the company credit card to purchase IT supplies. Upon audit of the companies "order history," the Senior Vice President of the company discovered possible fraudulent activity by two employees. With closer inspection, it was discovered that the insiders were buying high priced electronic equipment with the company credit card. The insiders would then sell or trade these items for prescription pain medication. Both insiders were convicted of wire/mail fraud and sentenced to 21 months incarceration in federal prison, three years supervised release, and restitution in the amount fraudulently obtained.

Louisville Case 6

Organization Type: Private Sector
Insider Descriptors: Female, 44 y/o
Fraud Loss Dollar Amount: $648,525.47
Motives: Insider had a gambling addiction
Dates of Embezzlement/Fraud: Insider began embezzlement in 2004, was discovered in 2008, and was prosecuted in 2010.
Incident Description: This case originated in 2008 with a call from representatives of a loan credit company. Corporate office personnel discovered multiple issues indicative of fraudulent activity, including loans with checks being issued to someone other than the borrower, after a review was conducted at one of the company branch locations. Further investigation revealed that the insider was the Branch Manager who in turn created approximately 190 fraudulent loans using the personal identifiers of former customers and other individuals in the community. The insider would then have friends and family members cash the issued checks and bring her the proceeds from the loans. The insider stated in a suspect interview that she committed the fraud to support a gambling habit. The insider pled guilty to a violation of 18 USC 1343, wire fraud, and was sentenced to three years and five months in federal prison, $648,525.47 in restitution, and three years of supervised release.

Louisville Case 7

Organization Type: Private Sector
Insider Descriptors: Female, 45 y/o
Fraud Loss Dollar Amount: $2,139,788.86
Motives: Insider used embezzled funds to purchase home, vehicles, provide support for a home business, and for charitable purposes.
Dates of Embezzlement/Fraud: Insider began embezzlement in 1997, was discovered in 2007, and was prosecuted federally in 2008.
Incident Description: Insider was a company's control accountant and was considered by management to be a "trusted employee, like a member of the family." In 1997, insider began embezzling funds from the company's petty cash account by writing checks to herself and to other employees that she considered loans. She used the money she received to put a down payment on a house, to purchase a recreational vehicle, automobile, boat and all-terrain vehicles, and to purchase equipment for her home-based business. Management discovered the embezzlement after an audit revealed discrepancies in account balances. Insider was convicted in 2008 in federal court and sentenced to serve 37 months incarceration, two years' supervised release, ordered to pay $2,383,723.44 in restitution, and $2,000 in court costs.

Louisville Case 8

Organization Type: Private Sector
Insider Description: Male, 51 y/o
Fraud Loss Dollar Amount: $1,100,000.00
Motives: Insider had an addiction to gambling and pain prescription medication pills
Dates of Embezzlement/Fraud: Insider conducted embezzlement over a 3-month period in 2008. Fraud was discovered in 2010, and prosecuted federally in 2013.
Incident description: Insider was an owner of a small business. When his gambling and pain medication addiction became out of control, he created and passed counterfeit checks made on the company business and moved funds from account to account over a three-month period of time, drawing the money out to feed his gambling addiction. The owner/insider placed the businesses into bankruptcy and closed the doors. He was later prosecuted federally for wire and mail fraud.

Louisville Case 9

Organization Type: Private Sector
Insider Description: Female, 54 y/o
Fraud Loss Dollar Amount: $2,400,000.00
Motives: Insider had a pain prescription medication addiction
Dates of Embezzlement/Fraud: Insider began embezzlement in 2000, discovered in 2008, and prosecuted in 2010.
Incident Description: Insider was the bookkeeper at a small law-firm where she had worked for over 18 years. Insider and her husband both became addicted to pain prescription medication and began embezzling funds in 2000 to support both of their addictions. Insider was prosecuted federally, pled guilty to wire fraud and was sentenced in 2010 to 51 months, three-year supervision, and ordered to pay restitution in the amount of $2,400,000.00.

Louisville Case 10

Organization Type: Private Sector
Insider Description: Male, 28 y/o
Fraud Loss Dollar Amount: $4800
Motives: Insider was addicted to pain prescription medication
Dates of Embezzlement/Fraud: Insider began illegal activity in 2008, discovered in 2009, and sentenced federally in 2010.
Incident Description: Insider became addicted to pain prescription medication after having medical surgeries in 2007 and 2008. Insider was a company IT administrator and began using organizational client data to obtain pain prescription medication utilizing clients' PII. Insider began ordering pain prescription medication in company client's names. Insider had access to a large

database of client information numbering in the hundreds of thousands of possible victims. Insider pled guilty to wire fraud and was sentenced to one year and one day in federal prison.

As research for this thesis, the author asked the USSS Cincinnati, Memphis, and Nashville Field Offices for their criminal case files from the 10 most recently closed criminal cases on insider fraud or embezzlement, under the USSS financial crimes category of fraud, embezzlement and misappropriation investigations to determine what the motivating factor(s) were for the insiders' illegal activity. The goal of the research was to determine if addiction had a role to play in the motives for the insiders' illegal activity. The following is a list of the questions asked to be completed by each office.

USSS field office research questions on closed/adjudicated criminal cases involving trusted insiders within organizations prosecuted for fraud and or embezzlement (most recent 10 closed criminal cases) research question: is addiction associated with the motive of the illegal activity?

- Secret Service Case Number (For internal tracking purposes only)
- Victim Organization Type (Public Sector/Private Sector/Non-Profit)
- Insider Descriptors: Gender, Age
- Fraud Loss Dollar Amount
- Motives for embezzlement/fraud: **Please note if the Insider had any type of addiction as a motivating factor in the embezzlement or fraud** (Ex. Insider had a Gambling Addiction, Insider had a Pain Medication Addiction, Insider had an Enhanced Lifestyle Addiction
- Provide very brief Incident Description (Example: Insider was a chief financial officer (CFO) of family business, became addicted to pain prescription medication, used access to organization data base, committed identity theft and opened/had issued unauthorized credit cards, employer discovered illegal insider activity while insider was away on vacation. Insider embezzled $100,000, convicted in federal court on three counts of aggravated identity theft, received 24 month sentence, fined $100, ordered to pay restitution in the amount of $100,000)

The following are the responses received from each field office.

2. Cincinnati Field Office

Cincinnati Case 1

Organization Type: Public Sector
Insider Descriptors: Male, 37 y/o.
Fraud Loss Dollar Amount: $15,000
Motives: Insider had an online gambling addiction.
Dates of Embezzlement/Fraud: Insider began embezzlement in 2006, was discovered in 2012, and was prosecuted locally in 2013.
Incident Description: Insider was an agency's union treasurer and secretary. Embezzlement began in 2006; the time of the insider's nomination, until a new union secretary and treasurer was nominated. Over the duration of the insider's position, the insider embezzled funds directly from the union bank accounts. To hide the embezzlement, the insider would destroy bank statements, records, and check stubs. At the time of the yearly audit, the insider would claim to have personally performed the audit, and provide false reports showing no discrepancy. The embezzlement was discovered after the union decided to review the financial records following the completion of the insider's position. When confronted, it was discovered that the insider used the funds to support his online gambling addiction. The insider was convicted in local court of one count of theft, and two counts of forgery. Insider was sentenced to 60 days in jail, five years of probation, a fine of $300, and ordered to pay restitution in the amount of $15,000.

Cincinnati Case 2

Organization Type: Private Sector
Insider Descriptors: Female, 40 y/o
Fraud Loss Dollar Amount: $159,208.82
Motives: Insider had a gambling addiction.
Dates of Embezzlement/Fraud: Insider began embezzlement in 2008, was discovered in 2009, and was prosecuted in 2013.
Incident Description: Insider was a Managing Director and responsible for the company's bookkeeping**.** Over the course of a year, insider embezzled $159,208.82 with a potential loss of $474,730.17 through several methods, including direct embezzlement, payroll embezzlement, personal use of the company's credit card, payroll making, and the use of a health saving's account to mask embezzlement. The embezzlement was discovered during a company audit. A majority of the money was used to support the insider's gambling addiction. The insider was convicted in federal court on one count of wire fraud and was

sentenced to 18 months incarceration with supervised release, and ordered to pay $258,000 in restitution to the victim.

Cincinnati Case 3

Organization Type: Private, Non-profit
Insider Descriptors: Male, 53 y/o.
Fraud Loss Dollar Amount: $10,100.00
Motives: Insider has a severe gambling addiction.
Dates of Embezzlement/Fraud: Insider embezzled $10,100.00 in January of 2013.
Incident Description: Insider worked as a CFO for a private, non-profit organization. After the insider took leave citing stress, the organization performed an audit on all deposits for the month of January 2013 and the accessible funds within the company vault. It was discovered that $10,100.00 was missing from the vault safe. When confronted, the insider claimed that he had a problem and was going to return the money. Later, it was discovered that the insider had a severe gambling addiction. The insider was convicted in local court on one count of forgery, and was granted admittance into a Diversion Program.

Cincinnati Case 4

Organization Type: Private sector
Insider Descriptors: Male 32 y/o, female 31, y/o.
Fraud Loss Dollar Amount:
Motives: Insiders had a heroin addiction
Dates of Embezzlement/Fraud: 2002–2012
Incident Description: Offenders conspired with a group of various individuals that passed fraudulent and stolen checks at various chain stores with the help of insiders. Insiders would process the checks as traveler's checks at the victim store to bypass the identification requirements. They would then take the items to another store to return them, where they would receive cash. Of the fraudulent checks used, some belonged to companies in which the people worked, or stolen/used from employee/friends. They would use the money received to purchase heroin. A store regional investigator discovered the fraud/embezzlement. The case was federally prosecuted, with the male insider receiving 16 years, and the female insider receiving four years for conspiracy and wire fraud.

Cincinnati Case 5

Organization Type: Private
Insider Descriptors: 50 y/o female
Fraud Loss Dollar Amount: $408,848.23
Motives: Insider has a gambling addiction
Dates of Embezzlement/Fraud: The embezzlement began in 2006, discovered in 2012, and prosecuted in 2013.

Incident Description: Insider was a bookkeeper for a private company and ran the accounting department within the company. The insider would write company checks payable to her husband's company without his knowledge, and immediately withdraw the funds from the account and gamble the money away at the slot machines. The company owner, due to his forged signature on the checks, discovered the embezzlement. Insider was very cooperative during the investigation, and served a federal target letter with a charge of bank fraud. The insider negotiated a plea agreement.

Cincinnati Case 6

Organization Type: Private Sector
Insider Descriptors: 43 y/o female
Fraud Loss Dollar Amount: $328,290.86
Motives: Insider has a gambling addiction
Dates of Embezzlement/Fraud: Insider began the embezzlement in 2010, and was discovered in 2013.
Incident Description: Insider was the Vice President of Operations for one year prior to the start of the embezzlement in 2010. The insider directly transferred funds from the company account into a bank account controlled by the insider. The insider was suspended when the company grew suspicious, and an employee took over the insider's duties. The employee discovered several customer refunds placed into an unidentified account under the insider's name. The insider was terminated. The case met federal prosecution.

Cincinnati Case 7

Organization Type: Private
Insider Descriptors: Insider is a 46 y/o female
Fraud Loss Dollar Amount: $154,094.71
Motives: Insider has a severe shopping addiction
Dates of Embezzlement/Fraud: Embezzlement began in 2010, and was discovered and prosecuted in 2013.
Incident Description: Insider worked for the company for 15 years, and hit financial trouble. Insider began using the company credit card to pay bills, but the spending quickly escalated. Over the course of three years, the insider embezzled $154,094.71. The majority of the money went towards the insider's shopping sprees, with the use of the company credit card, or using the company credit card to pay off the insider's personal credit card. The credit card company reported the fraud, as the transactions were indicative of wire fraud, money laundering, and credit card fraud, and embezzlement on behalf of an employee. The case has been federally prosecuted on one count of wire fraud.

Cincinnati Case 8

Organization Type: Private
Insider Descriptors: Insider is a 51 y/o female
Fraud Loss Dollar Amount: $408,484.00
Motives: Insider had a severe gambling problem
Dates of Embezzlement/Fraud: Insider began the embezzlement in 2006, was discovered in 2012, and prosecuted in 2013
Incident Description: Insider was a bookkeeper at a small business that was a distribution center. Trusted insider used business checks, forged the signature of the owner of the company, and deposited checks into fraudulent personal accounts to support her gambling addiction. Insider admitted that she was a compulsive gambler who had a previous conviction for embezzlement in 1998. Part of the insider's previous sentence was a mandatory enrollment into GA.

Cincinnati Case 9

Organization Type: Private
Insider Descriptors: Insider is a 45 y/o male
Fraud Loss Dollar Amount: $96,579.00
Motives: Insider had financial problems
Dates of Embezzlement/Fraud: 2011–2012
Incident Description: Insider used the company credit card and began making unauthorized purchases of gift cards. Insider began embezzlement to pay for financial problems. Unknown if insider had any known addictions.

Cincinnati Case 10

Organization Type: Private
Insider Descriptors: Insider is a 54 y/o female
Fraud Loss Dollar Amount: $1,340,636.00
Motives: Insider appeared to desire an enhanced lifestyle
Dates of Embezzlement/Fraud: 2007–2013
Incident Description: Insider was a bookkeeper for a private company and embezzled company funds by falsifying company ledger accounts after she had written herself numerous checks and deposited them into accounts she controlled. Insider was found guilty on 10 counts of theft over $10,000, and two counts of forgery in state court. Unknown if the insider had any addictions.

3. Memphis Field Office

Memphis Case 1

State docket
Private company
Male, 47 yoa at arrest
Loss: $1.2 million
Motives: Unknown motives, refused to be interviewed. No known addictions
Dates: Embezzlement began in 2000, discovered in 2011, prosecuted in 2012
Incident: Insider was the CEO of company who wrote legitimate checks on company accounts to fictitious vendors, and through a scheme involving unwitting employees, he received the illicit funds. Insider was arrested at the airport en route to Hawaii. In State court, he pled guilty to one count of theft of property over $60,000, sentenced to 10 years in state prison, and restitution of $811,075.50.

Memphis Case 2

Federal Docket
Private company
Male, 48 yoa at arrest
Loss: $431,983.79
Motive: financial stress, possible enhanced lifestyle addition
Dates: embezzlement began in 2003, discovered in 2011, prosecuted in 2012.
Incident: Insider was the Vice President of Finance at a private sector corporation, forged company checks, and subsequently, deleted the checks from the companies system. The fraud was discovered during an audit. He pleaded guilty in federal court to one count of bank fraud. He was sentenced to 33 months incarceration, three years' probation, restitution in the amount of $431,983.79, and a special assessment of $100.000.

Memphis Case 3

Federal docket
Private company
Female, 47 yoa at arrest
Loss: $1.5 million
Motives: financial pressures, possible enhanced lifestyle addiction (four houses and an antique business were funded through the fraud)
Dates: embezzlement began in 2006, discovered in 2010, and prosecuted in 2011.
Incident: Insider was a bookkeeper for a construction firm who made unauthorized electronic transfer of funds and wrote company checks (without signature authority) to pay for four houses, two cars, a motorcycle and an antique business. The fraud was discovered in an audit. The firm was forced into

bankruptcy. She pleaded guilty in federal court to one count of bank fraud, was sentenced to 51 months in custody, and restitution in the amount of $1,578,277.75.

Memphis Case 4

State docket
Private company
Female 37 yoa at arrest
Loss: $19,690.79
Motives: unknown, refused interview
Dates: embezzlement began in 2008, ended in 2010, discovered in 2011, and prosecuted in 2012
Incident: Insider was the accounting manager at a private corporation, developed a scheme in which she would locate stale uncashed checks in the system and reissue them to herself using an unauthorized signature stamp for validation. The loss was discovered during an audit. In state court, she pleaded guilty to 36 counts of forgery, and one count of theft under $60,000. She was placed on diversion for three years and paid $19,690.79 in restitution.

Memphis Case 5

Federal docket
Private company
Male 72 yoa at arrest
Loss: $1.75 million
Motives: enhanced life style, business pressures
Dates: Embezzlement/check writing began in 1987, discovered in 2011, and prosecuted in 2012
Incident: Insider was an attorney who used funds under his control from real estate escrow accounts, trust fund accounts, and probate estate accounts to fund other business and an enhanced lifestyle. He pleaded guilty in federal court and was sentenced to 48 months incarceration, two years supervised release, and restitution of $1.75 million.

Memphis Case 6

Federal docket
Private person
Female 39 yoa at arrest
Loss: $234,000
Motive: enhanced lifestyle, no known addictions
Dates: embezzlement began in 2006, discovered in an audit 2012, and prosecuted in 2012

Incident: Personal assistant of a business executive who used credit cards and bank accounts in unauthorized transactions to fund an enhanced lifestyle. She pleaded guilty in federal court to one count of mail fraud. She was sentenced to 27 months in custody, three years supervised release, and $234000 in restitution.

Memphis Case 7

State docket
Public college
Female 56 yoa at arrest
Loss: $134,964
Motive: gambling addiction
Dates: embezzlement began in 2008, discovered in 2010, and prosecuted in 2013
Incident: Insider was a college bookstore manager, used elaborate system to void valid checks to the bookstore and redirect the funds to herself. She claimed to have gone through a divorce and needed funds to live, then became depressed, and used gambling as a coping mechanism. She pleaded guilty in state court and was sentenced to serve one year in state custody, and nine years probation with $50,000 restitution.

Memphis Case 8

Federal docket
Private bank
Female 33 yoa at arrest
Loss: $31,750
Motive: Business pressures, stolen funds were used to bolster husband's trucking business
Dates: Began in 2009, discovered in 2010, and prosecuted in 2011
Incident: Insider was a bank teller, stole cash from her drawer and manipulated electronic records to cover the loss. Discovered at audit. She pleaded guilty to one count of misapplication of bank funds and was sentenced to 90-day incarceration; three years supervised release, and restitution of $31,750.

Memphis Case 9

Federal docket
Private company
Female 53 yoa at arrest
Loss: $274,390.33
Motive: gambling addiction
Dates: Began 2008, discovered in 2011, and prosecuted in 2012
Incident: Insider was the bookkeeper who forged company check to herself to provide funds for gambling. Discovered at audit. She pleaded guilty in federal

court to two counts of fraud and was sentenced to 18 months incarceration, three years supervised release, and restitution of $274,390.33

Memphis Case 10

Federal docket
Private company
Female 36 yoa at arrest
Loss: $260,727.35
Motive: enhanced lifestyle
Dates: began in 2009, discovered in 2010, prosecuted in 2011
Incident: Insider was an accounts clerk at a private company who deferred incoming payments to a medical firm to her own accounts. She spent the money on clothes and travel. It was discovered after the bank questioned her deposits. She pleaded guilty in federal court to one count of forged checks. She was sentenced to 18 months incarceration, two years supervised release, and restitution of $260,727.35.

4. Nashville Field Office

Nashville Case 1 (No known addiction association)

Closed 2002
Federal Docket
Victim Organization Type: Individual
Insider Descriptors: Male, Age (at time of initial fraud): 23
Actual Fraud Loss Dollar Amount: $50,900.00
Potential Fraud Loss Dollar Amount: $62,730,900.00
Motives for Fraud: None indicated
Dates of Embezzlement: 11/12/98–12/05/98
Incident Description: An informant provided information implicating the insider for fraud related activities in May 1998. While investigating another case, an agent discovered evidence of five money transfers from the victim to the insider between 11/12/98 and 12/05/98 as part of a Nigerian advance fee fraud scheme. Insider was arrested in 2001. Insider pled guilty to misuse of a social security number, wire fraud, and bank fraud in federal court on 2001. Insider was sentenced to 18 months in federal prison in 2001.

Nashville Case 2 (No known addiction association)

Closed 2002
Federal Docket
Victim Organization Type: Individual

Insider Descriptors: Insider One: Male, Age (at time of initial fraud): 28; **Insider Two:** Male, Age (at time of initial fraud): 27
Fraud Loss Dollar Amount: $50,000.00
Potential Fraud Loss Dollar Amount: $1,000,000.00
Motives for Fraud: None indicated
Dates of Embezzlement: 1998
Incident Description: Two individuals scammed victim in 1998 for $18,000 as part of a Nigerian advance fee fraud scheme. The victim reported the fraud. Evidence of identity theft and credit card fraud was also discovered from surveillance cameras in several electronics stores in the ensuing investigation. Insider one was arrested in 1999; the insider gave the location of insider two during a post-arrest interview. Insider two was then arrested in 1999. Agents found numerous fraudulent identification documents in insider two's apartment that implicated another individual (who was eventually charged, sentenced, and deported for the documents). Insider two pled guilty to the misuse of a social security number in 1999 in federal court; he was released after agreeing to testify in another case. Insider one pled guilty to credit card fraud in 1999 in federal court and was sentenced to 12 months one day in 2000.

Nashville Case 3 (No known addiction association)

Closed 2003
Criminal Case Court Docket Number: N/A
Victim Organization Type: Individual
Insider Descriptors: Insider One: Male, Unknown Age; **Insider Two:** Male, **Age (at time of initial fraud):** 30; **Insider Three:** Male, Age (at time of initial fraud): 30
Actual Fraud Loss Dollar Amount: $498,969.75
Potential Fraud Loss Dollar Amount: $1,000,000.00
Motives for Fraud: None indicated
Dates of Embezzlement: 1998
Incident Description: A bank fraud investigator contacted the USSS in 1998. A victim sent three cashier's checks from Nashville to Canada totaling $41,462.50 in a telemarketing advance fee fraud scheme. A total of 14 checks were written in 1998 and sent to Canada by the victim. Investigators contacted the Canadian police and consolidated this case with a Canadian case due to common suspects (three total suspects). Two insiders were arrested in 1999 in Montreal; the third insider was never apprehended. Canadian prosecution of the suspects was declined on 2002. The USAO declined prosecution in 2002.

Nashville Case 4 (No known addiction association)

Closed 2008
State Docket
Victim Organization Type: Private Sector

Insider Descriptors: Female, Age (at time of initial fraud): 32
Actual Fraud Loss Dollar Amount: $92,849.22
Potential Fraud Loss Dollar Amount: $94,149.49
Motives for Fraud: Insider used some of the money for house payments.
Dates of Embezzlement: 2004–2005
Incident Description: A local detective contacted the USSS in 2005 when the victim had initially reported the incident. A secretary of a trucking business made numerous unauthorized wire transactions from a business account to a personal bank account from 2004–2005. Insider was ordered to pay $287,480.32 in damages and fees on 03/14/07.

Nashville Case 5 (No known addiction association)

Closed 2010
Federal Docket
Victim Organization Type: Individual
Insider Descriptors: Female, Age (at time of initial fraud): 30
Actual Fraud Loss Dollar Amount: $61,940.81
Potential Fraud Loss Dollar Amount: $76,806.61
Motives for Fraud: Insider used the funds obtained from the student loans to attend two state universities from 1993–1996.
Dates of Embezzlement: 1993–1996.
Incident Description: Insider used her spouse's former wife's identity to obtain numerous student loans in the victim's name and attend two universities from 1993–1996. Insider also falsely filled out a naturalization application using the victim's identity in 2007. The victim received notices as early as 1999 about the loans and filed several false claim reports but disregarded them. The victim reported the fraud in 2006, and the USSS began its investigation. An agent interviewed the insider in 2007. Insider was arrested in 2009. Insider pled guilty in federal court to false statements relating to naturalization, citizenship, or alien registration in 2010 and was sentenced to three years' probation. Insider was also ordered to pay restitution totaling $50,365.31.

Nashville Case 6 (No known addiction association)

Closed 2011
State Docket
Victim Organization Type: Private Sector
Insider Descriptors: Male, Age (at time of initial fraud): 49
Actual Fraud Loss Dollar Amount: $2,000.00
Potential Fraud Loss Dollar Amount: $2,000.00
Motives for Fraud: None indicated
Dates of Embezzlement: 2011

Incident Description: A Nashville detective contacted the USSS in 2011 regarding an employee theft. The insider used a credit card to obtain a cash advance of $2,000 without authorization. Insider was arrested on 2011.

Nashville Case 7 (No known addiction association)

Closed 2012
Criminal Case Court Docket Number: N/A
Victim Organization Type: Private Sector
Insider Descriptors: N/A
Actual Fraud Loss Dollar Amount: $518,813.99
Potential Fraud Loss Dollar Amount: $518,813.99
Motives for Fraud: None indicated
Dates of Embezzlement: October 2010
Incident Description: The victim, a representative of Computer Marketing Corporation, reported fraud related to counterfeit purchase orders on 2010. The purchase orders were for computer equipment to be shipped to an address out of state. Two controlled deliveries were attempted unsuccessfully. The individual shipping the products could not be identified. It was determined that the fraud originated overseas.

Nashville Case 8 (Possible addiction association)

Closed 2012
State Docket
Victim Organization Type: Private Sector
Insider Descriptors: Female, Age (at time of initial fraud): 27
Actual Fraud Loss Dollar Amount: $63,540.10
Potential Fraud Loss Dollar Amount: $63,540.10
Motives for Fraud: The insider used the money for a variety of effects including groceries, sex toys, music, casino charges, cart payments, cart insurance, electric bills, and her husband's child support payments. Insider may have a gambling and sex addiction.
Dates of Embezzlement: 2008–2010
Incident Description: The victim reported in 2011 that an employee used company credit cards and commercial checks without permission; the victim reported a loss of over $63,000. The insider from 2008 to 2010 used 74 fraudulent checks and four company credit cards. Insider was arrested on 2011 for theft of property and credit card fraud charges. Insider pled guilty to theft of property in state court in 2012. Insider was sentenced to eight years supervised probation, fined $732.05 in court costs, and was instructed to pay $65,100 in restitution.

Nashville Case 9 (Possible addiction association)

Closed 2012
State Docket
Victim Organization Type: Private Sector
Insider Descriptors: Female, Age (at time of initial fraud): 28
Actual Fraud Loss Dollar Amount: $118,395.69
Potential Fraud Loss Dollar Amount: $118,395.69
Motives for Fraud: Insider used the credit card for various personal expenditures including utility payments, a Disney World vacation, and a law school loan. Insider claimed that her spending "turned into a compulsion" and that she had a "binge spending disorder." * (p. 7 of criminal indictment)
Dates of Embezzlement: 2007–2009
Incident Description: The victim reported in 2010 the unauthorized use of two credit cards by an employee. Insider was employed as an assistant from 2006 to 2010. After determining that the insider was the only one with access to the cards, insider was arrested for credit card theft on 2011. Insider pled guilty in state court in 2012 for fraudulent use of a credit card and was given a nine-year sentence. The sentence was suspended on 2012 and insider was given 12 years of supervised probation and ordered to pay $90,000 of restitution in monthly payments of $800.

Nashville Case 10 (No known addiction association)

Closed 2013
Federal Docket
Victim Organization Type: Private Sector
Insider Descriptors: Female, Age (at time of initial fraud): 38
Actual Fraud Loss Dollar Amount: $34,945.00
Potential Fraud Loss Dollar Amount: $34,945.00
Motives for Fraud: Insider used all embezzled funds to pay for a new car and rent.
*A possible enhanced lifestyle addiction is possible adue to many large returned checks, but it is not noted in the case file.
Dates of Embezzlement: 2009–2010.
Incident Description: The victim reported in 2010 that the insider, in the company's name, had used numerous forged checks. The insider worked at the company from 2009–2010. Insider was arrested in 2011. Insider pled guilty in federal court to bank fraud and was sentenced to weekend imprisonment for eight months; insider also was ordered to make restitution in the amount of $34,945.00.

C. CASE ASSESSMENTS

It should be noted that the author did not have direct access to the closed criminal case files from the Cincinnati, Memphis or Nashville Field Offices. He relied solely on the written responses regarding all of the insider threat cases reported by each office as the basis for this assessment. The cases requested to be reviewed by each field office were under the USSS category of fraud, embezzlement and misappropriation investigations.

1. Louisville Field Office

As the Special Agent in Charge, the author had complete access to the closed case files in the Louisville Field Office and the ability to interview the case agents who had completed the investigations. Thus, he was able to conduct an accurate assessment of the cases. The cases ranged from small victim organizations of less than six employees, to large organizations of over 10,000 employees. Many of the cases devastated the organization and caused irreparable financial or reputational harm. In some cases, the insider fraud harmed the entire community due to the widespread publication of the event.

At first review of the closed cases, the author discovered from the investigative information contained within the case reports that four out of the 10 closed cases indicated that an addiction to pain prescription medication was the motivating factor for the insider's reason to commit the crime. He then specifically asked each case agent to respond to a question on each of the closed cases to determine if that agent recalled if the insider/defendant(s) had any known addiction-related behaviors that were uncovered during the course of the criminal investigation and might not have been recorded in the case file.

In Case 1, it was discovered that although not listed in the case reports, the investigating case agents recalled that the defendant was addicted to gambling, and had admitted during the course of the investigation that, "they were feeding a gambling addiction." When asked why the gambling addiction information was not included in the case report, the case agent did not think it was relevant to the facts of the case. In Case 4,

the case agent highly suspected the insider was using pain prescription medication because a witnesses interviewed for the case stated that the insider was "addicted to pain pills." However, the case agent did not indicate this addition in his case report since the insider did not admit to using pain prescription medication and it was not corroborated.[180]

Out of the 10 Louisville closed cases reviewed for this thesis, the defendants in five of the cases were insiders addicted to prescription drug medication; three insiders admitted to being addicted to gambling, and in one case, the insider admitted an addiction to both gambling and pain prescription medication as his motivating factor for the embezzlement. The other two cases indicated the insiders' desire for an enhanced lifestyle. In one of these, Case 3, the investigating case agents reported that the case involved a trusted insider who had a collection of 12 high-priced collector vehicles, and the insider reportedly, "spent the majority of his embezzlement funds on maintaining his prized car collection." The investigating agents opined that the insider was "obsessed with his cars."

One of the goals of USSS investigations into financial crimes is to identify assets or proceeds that a defendant has stolen or purchased with their ill-gotten gains. Once bank accounts or items of value can be identified as proceeds of a crime, the government has a process in place to be able to seize and forfeit illegally obtained assets to make restitution to the victim organizations.[181] Of note, in the eight cases involving gambling or pain prescription medication as a motivating factor for the illegal behavior, investigating agents discovered that no assets were available to seize or recover. All the illegal proceeds from the crimes committed had gone to support the insiders' addiction to gambling or pain prescription medication. The loss in one case was over $2.4 million, two cases were over $1 million, and in four cases, losses were several hundred thousand dollars.

[180] It should be noted that an addiction to gambling or pain prescription medication is not required to be noted in case reports for Secret Service reporting requirements.

[181] The USSS, as a federal agency, is empowered by federal statutes to seize assets believed to have been obtained through illegal means, and based on the outcome of civil or criminal action, return those seized assets to the victims of the crime.

2. Cincinnati Field Office

Closed criminal case reviews for this thesis conducted by the Cincinnati Field Office had the largest reported insider motivations for fraud and embezzlement listed as gambling addictions. In six out of 10 instances, the motives for the illegal activity were reported to be gambling addictions. In four of the gambling addiction cases, the insiders were female, and in two instances, the insiders were male. In Case 8, the insider admitted to being previously convicted of insider theft with a former employer due to her gambling addiction prior to the embezzlement conducted at the insider's current place of employment. It should also be noted that the insider admitted that as a part of her judgment, she was ordered to enroll in Gamblers Anonymous (GA) as a condition of her sentencing in the previous offense.

In Case 4, two insiders conducted fraud, one female and one male. The motivation given for their illegal behavior was an addiction to heroin. In Case 7, the female embezzler conducted her illegal insider activities due to a severe shopping addiction. In Case 9, the insider's motives for conducting his illegal activity were due to financial pressures.

3. Memphis Field Office

The Memphis Field Office closed criminal cases had the largest number of trusted insiders convicted of illegal fraud and embezzlement activities listed as female perpetrators, eight out of 10 cases. Males accounted for two of the cases. In Cases 7 and 9, both insiders were convicted of fraud and claimed to have been addicted to gambling as the motivation for their criminal behavior in each case. In Case 7, the female insider reported, "she was going through a divorce, was depressed, and used gambling as a coping mechanism."

In two cases, no known motivations for the illegal insider activity were discovered. In five cases, the motives reported for conducting the illegal insider fraud or embezzlement were to maintain an enhanced lifestyle. In Case 8, the insider admitted to embezzling funds due to financial pressures to provide support for her husband's trucking business.

4. Nashville Field Office

The Nashville closed criminal cases reported that in two out of the 10 cases, addiction appeared to be a motivating factor in the insider's illegal activity. In Case 8, the female insider appeared to have an addiction to gambling, as well as a sex addiction. In Case 9, the female insider claimed to have admitted that her spending "turned into a compulsion" and that she had a "binge spending disorder."

In five cases, motives for the illegal activity could not determined from the case files. In Cases 4 and 5, both with female perpetrators, the cause appeared to be outside financial pressures. In Case 10, the insider appeared to desire an enhanced lifestyle as the motivating factor for her embezzlement. See Table 1.

Motive	Male	Female
Gambling Addiction	3	8
Pain Prescription Med Addiction	4	2
Gambling and Pain Med Addiction	1	0
Heroin Addiction	1	1
Possible Pain Med Addiction	1	0
Gambling and Sex Addiction	0	1
Binge Shopping Disorder	0	1
Enhanced Lifestyle	3	6
Financial Pressures	1	3
Unknown Motive	8	1
Total	22	23

Table 1. Results of Motives

5. Case Assessment General Findings

The USSS case reviews conducted by the Louisville, Cincinnati, Memphis and Nashville Field Offices under the USSS category of fraud, embezzlement and misappropriation investigations revealed the following general statistics.

Forty closed criminal cases were reviewed with a total of 45 insiders involved in fraud or embezzlement; the perpetrators were 24 females and 21 males. Out of 40 entities victimized, four were from the public sector, one was non-profit, and 35 private sector bodies that suffered loss due to an insider threat being conducted against it. Eleven cases

had a gambling addiction as a motivating factor, three of which had male perpetrators and eight were female. Six events had pain prescription medication addiction as a motivating factor, and in one case, an addiction to both gambling and pain prescription medication was listed as the motive. In one case, both a male and female insider claimed a heroin addiction as the motivating factor. Another incident had both a gambling addiction and a sex addiction as the motivating factor, and yet another case had a binge spending or shopping disorder as the insiders' motivation for her illegal activity. Nine cases listed an enhanced lifestyle as a motivating factor, four incidents listed outside financial pressures as the motivating factor, and in nine instances, a motive for the insider criminal action could not be determined and was listed as unknown.

Figure 2 shows the 40 case motives for committing fraud and embezzlement separated by gender. It is interesting to note that the majority of female perpetrators had motives related to gambling addiction, and aside from unknown motives, the male perpetrators' majority motive was pain prescription medication addiction.

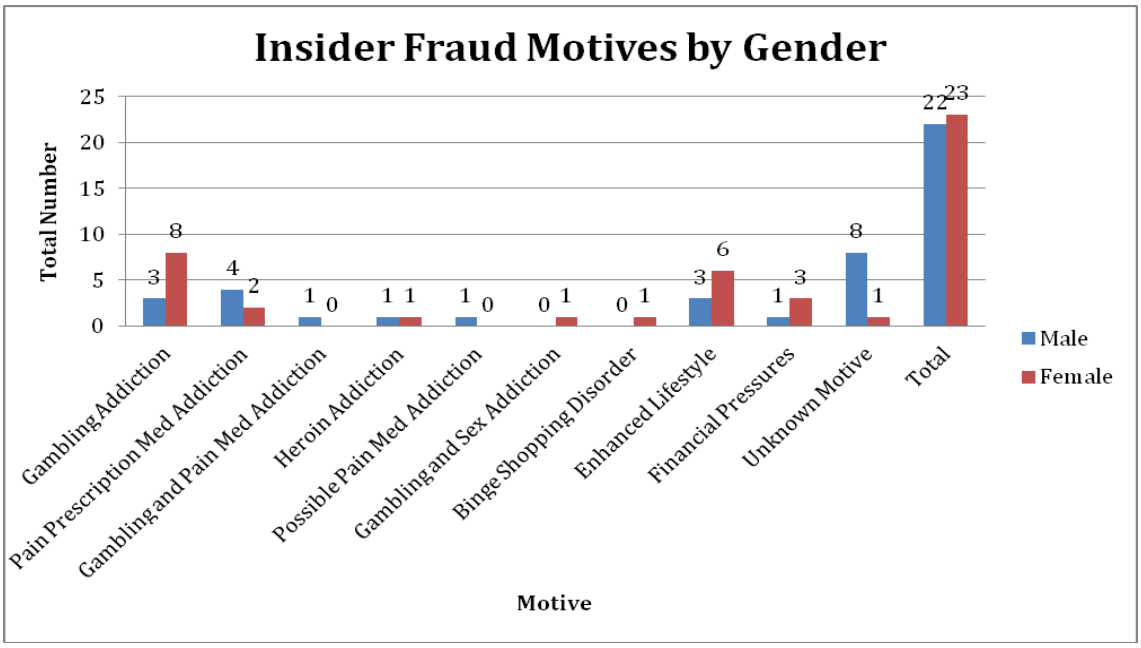

Figure 2. Insider Fraud Motives by Gender

In these 40 cases reviewed for a determination of motive(s) by the 45 insiders committing fraud or embezzlement activities, Figure 3 provides an indication of the breakdown of motives. Twenty-three individuals were identified with an addictive behavior, 13 motives were tied to financial pressures or a desire for an enhanced lifestyle as motivating factors, and in nine cases, the motives were unknown.[182]

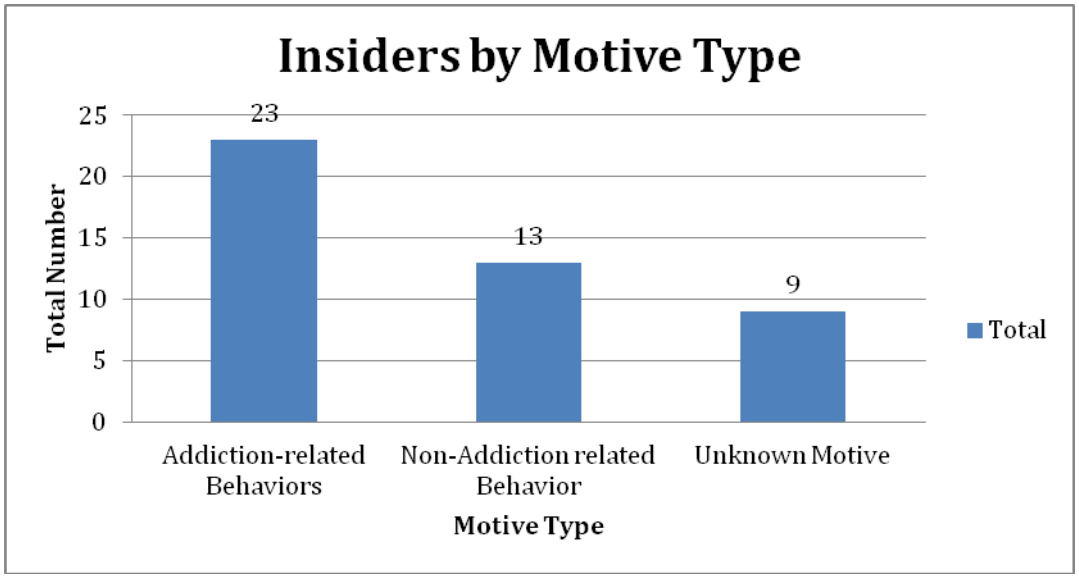

Figure 3. Insiders by Motive Type

D. CERT INSIDER THREAT CASE STUDIES

The CERT Insider Threat Center conducts empirical research and analysis to develop and transition socio-technical solutions to combat insider cyber threats. It has been researching this problem since 2001 in partnership with the DOD, the DHS, the USSS, other federal agencies, the intelligence community, private industry, academia,

[182] The USSS does not require case agents to document a specific motive or motives for a suspect or defendant in a criminal case, as to their reason for conducting their illegal activities. Case agents are focused on determining the criminal elements of a case and being able to determine probable cause of illegal criminal activity to provide documentation of the elements of a crime to present the facts of criminal wrongdoing to a prosecuting attorney for judicial action to occur.

and the vendor community. CERT is located at Carnegie Mellon University's Software Engineering Institute, a federally funded research and development center (FFRDC).[183]

Currently, the CERT program has over 700 documented cases of malicious insiders convicted in a U.S. court of law for criminal violations regarding illegal insider activity involving some form of critical IT services; see Figure 3. The current cases in the insider threat database involve insider incidents from 1996 to the present.[184]

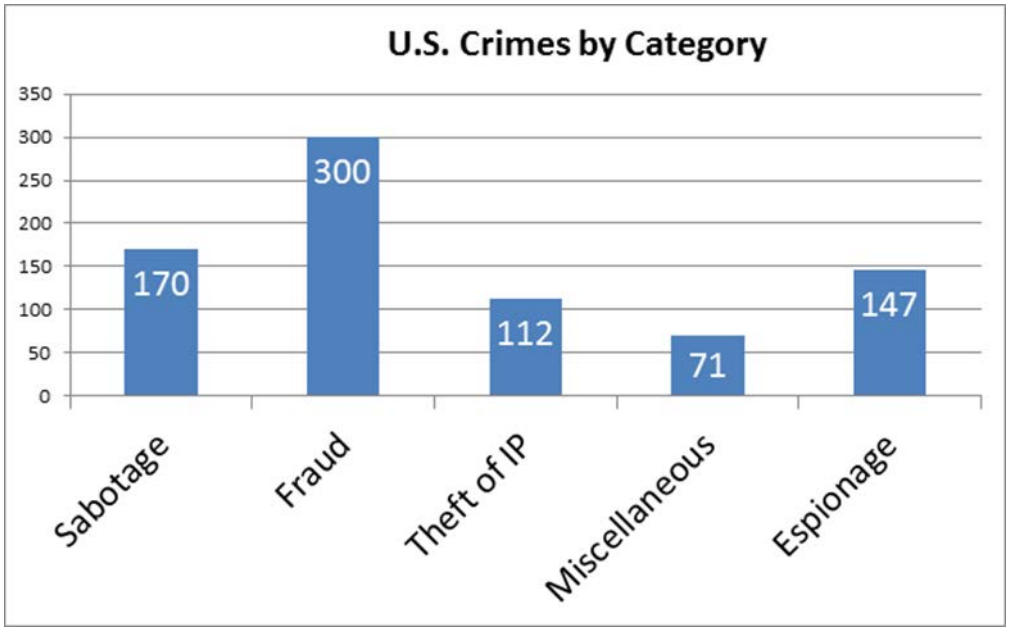

Figure 4. CERT Insider Threat Cases by Category[185]

CERT breaks down its research of insider threats into five types of crimes.

IT sabotage: An insider's use of IT to direct specific harm at an organization or an individual.

Fraud: An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or

[183] Michael Hanley et al., *An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases* (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, February 2011).

[184] Cappelli, Moore, and Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).*

[185] All graphs in this section were provided by CERT for this thesis research.

theft of information that leads to an identity crime (e.g., identity theft, credit card fraud).

Theft of intellectual property (IP): An insider's use of IT to steal intellectual property from the organization. This category includes industrial and national security espionage involving insiders.

Miscellaneous: Cases in which the insider's activity was not for IT sabotage, fraud, or IP theft.

Espionage: An insider's use of IT for the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used for the injury of the United States or to the advantage of any foreign nation. (It should be noted that no espionage cases were used for this study.)[186]

CERT defines an insider threat as:

> A malicious insider threat to an organization 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.[187]

The following are the sources of information CERT used to code insider threat cases.

Public sources of information

- Media reports
- Court documents
- Publications

Non-public sources of information

- Law enforcement investigations
- Organization investigations
- Interviews with victim organizations
- Interviews with convicted insiders[188]

---

[186] Cappelli, Moore, and Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, xviii–xxi.

[187] Cappelli et al., "Common Sense Guide to Prevention and Detection of Insider Threat, 3rd Edition—Version 3.1."

[188] Randall Trzeciak, "The CERT Insider Threat Database|Insider Threat," *CERT Insider Threat Center,* August 15, 2011, http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=76.

Listed as follows are types of information about each incident collected including, but not limited to the following

Details of the insider's behavior and interactions with coworkers

Vulnerabilities in organization systems that the inside was able to exploit in the attack

Unmet expectations related to job conditions

Technical and nontechnical methods used by the insider

Evidence of planning and deception

How the incident was detected or reported

Types of information or assets that were stolen or targeted

Information about coconspirators and recruitment[189]

1. Thesis Research Conducted by CERT

The research examined by the CERT program for this thesis reviewed 680 documented insider threat cases currently evaluated and in their database. The purpose of this study was to determine if any of the documented motivating factors for the insider's illegal activity had any references to addiction as a motive.[190]

Out of the 680 insider threat cases reviewed by CERT for the research on this thesis, the principal data set revealed that 29 out of the 680 cases involved some kind of addiction related motive as a contributing factor for the illegal insider activity. It should be noted that addiction was listed in the CERT database only if it was documented during the investigation or through any of the above listed public and non-public sources of information. The data revealed that the addiction noted in the findings involved gambling, drug use, or alcohol.[191] See Table 2.

[189] Hanley et al., *An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases*.

[190] Information provided by CERT for research on this thesis.

[191] Ibid.

Action	Count
Alcohol and Drug Use	3
Drug Use (non-alcohol)	15
Alcohol Use	5
Gambling	6

Table 2. CERT Insider Threat Cases by Breakdown of Addictive Indicators[192]

In the 29 identified cases with known addiction behaviors, 21 indicated fraud as the illegal activity committed by the insider, as noted in Figure 5, with almost half of those cases coming from the banking and finance sector. Figure 6 shows the 29 cases identified with addiction-related behaviors, broken down by type of case.

Count of Incident_ID	Column Labels			
Row Labels	Fraud	Miscellaneous	Sabotage	Grand Total
Agriculture and Food	1			1
Banking and Finance	10	1	1	12
Commercial Facilities	2			2
Communications	1			1
Education	1			1
Government-Federal	1		2	3
Government-State/Local	2			2
Healthcare and Public Health	1		1	2
Information Technology	1		3	4
Water	1			1
Grand Total	**21**	**1**	**7**	**29**

Figure 5. CERT Insider Threat Cases with Addiction As a Motivating Factor[193]

[192] All graphs in this section were provided by CERT for this thesis research.

[193] All graphs in this section were provided by CERT for this thesis research.

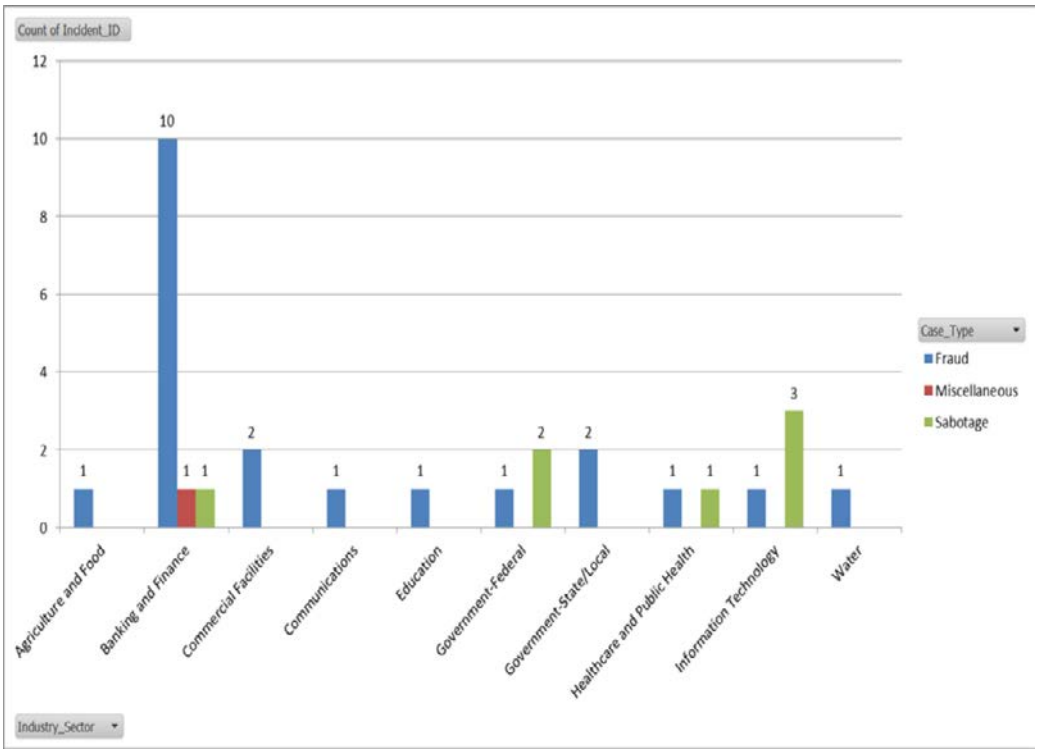

Figure 6. CERT Insider Threat Cases with Addiction As a Motivating Factor Broken Down by Sectors[194]

In 24 out of the 29 insider threat cases, gambling and drug use was indicated as the addictive behavior trait. As was previously stated, fraud connected criminal activity, accounted for 21 out of the 29 insider threat cases of addiction related illegal insider behavior in the CERT database, which is reflective of the thesis literature review in Chapter II. In most incidents in which fraud is committed because of the insider attack, the need to finance the addiction is often indicated as the motivating factor driving the insider to conduct their illegal activity.[195]

[194] Ibid.

[195] Lesieur, *The Chase: Career of the Compulsive Gambler*, vol. xxi; Cressey, *Other People's Money; A Study in the Social Psychology of Embezzlement*; Green, "White-Collar Crime and the Study of Embezzlement," 95–106.

2. Detailed Breakdown

CERT detailed breakdown of the cases with addiction as a motivator follows.[196]

Total Number of Addiction/Alcohol/Gambling Drugs Cases

- 29 Cases Industry Sector and 27 Cases Banking and Finance: 44.44%
- Information Technology: 14.81%
- Government/Federal: 11.11%
- Government/State/Local: 7.41%
- Agriculture and Food: 3.7%
- Water: 3.7%
- Communications: 3.7%
- Education: 3.7%
- Commercial Facilities: 3.7%
- Healthcare and Public Health: 3.7%

Gender of Insider: 29 Cases

- Male: 65.52%
- Female: 34.48%

Insider's Employment Type: 29 Cases

- Full Time: 82.61%
- Contractor: 17.39%

Insider's Employment Status: 29 Cases

- Current: 71.43%
- Former: 28.57%

Trusted Business Partner: 29 Cases

- No: 82.14%
- Yes : 17.86%

Type of Trusted Business Partner Relationship: 5 Cases

- Organizational: 40.0%
- Contract Employee: 40.0%

[196] CERT detailed breakdown of cases with addiction provided in raw data format.

- Individual Consultant: 20.0%

Prior Planning by Insider: 8 Cases

- 0–24 Hours: 25.0%
- None: 25.0%
- > 1 Year: 25.0%
- Planned, Time Unknown: 12.5%
- 8–31 Days: 12.5%

Prior Deception by Insider: 7 Cases

- > 1 Year: 42.86%
- None: 28.57%
- 90–365 Days: 28.57%

Time of Insider Attack: 19 Cases

- During Work Hours: 63.16%
- During and Outside of Work Hours: 21.05%
- Outside of Work Hours: 15.79%

Location of Insider Attack: 23 Cases

- On-Site: 69.57%
- Remotely: 21.74%
- On-Site and Remotely: 8.7%

Attack On-Site: 29 Cases

- TRUE: 55.17%
- FALSE: 44.83%

Insider had Remote Access: 29 Cases

- FALSE: 79.31%
- TRUE: 20.69%

Location of Attack Unknown: 29 Cases

- FALSE: 82.76%
- TRUE: 17.24%

Attack During Working Hours: 29 Cases

- TRUE: 51.72%

- FALSE: 48.28%

Attack Outside of Working Hours: 29 Cases

- FALSE: 79.31%
- TRUE: 20.69%

Time of Attack Unknown: 29 Cases

- FALSE: 72.41%
- TRUE: 27.59%

Case Type: 29 Cases

- Fraud: 75.0%
- Sabotage: 21.43%
- Miscellaneous: 3.57%

Sabotage: 29 Cases

- FALSE: 75.86%
- TRUE: 24.14%

Theft: 29 Cases

- FALSE: 75.86%
- TRUE: 24.14%

Affiliated with

- Organized Crime: 7.14%
- Criminal Enterprise: 7.14%

Subject’s Account Used in Attack: 29 Cases

- TRUE: 58.62%
- FALSE: 41.38%

Shared Account used in Attack: 29 Cases

- FALSE: 96.55%
- TRUE: 3.45%

Organization’s Account Used in Attack: 29 Cases

- FALSE: 93.1%
- TRUE: 6.9%

Backdoor Account Used in Attack: 29 Cases

- FALSE: 93.1%
- TRUE: 6.9%

Coworker’s Account Used in Attack: 29 Cases

- FALSE: 89.66%
- TRUE: 10.34%

Unknown IT Account Used in Attack: 29 Cases

- FALSE: 93.1%
- TRUE: 6.9%

Other IT Account Used in Attack: 29 Cases

- FALSE: 89.66%
- TRUE: 10.34%

Financial Impact of Attack: 29 Cases

- $100,000–$999,999: 46.15%
- $10,000–$99,999: 34.62%
- $1,000,000+: 15.38%
- $1–$9,999: 3.85%

Attack Detected by Information Systems: 29 Cases

- FALSE: 96.55%
- TRUE: 3.45%

Attack Detected by System Failure: 29 Cases

- FALSE: 93.1%
- TRUE: 6.9%

Attack Detected by Audit: 29 Cases

- FALSE: 68.97%
- TRUE: 31.03%

Attack Detected by Non-technical Means: 29 Cases

- FALSE: 68.97%
- TRUE: 31.03%

Unknown How Attack Was Detected: 29 Cases

- FALSE: 72.41%
- TRUE: 27.59%

Attack was Self Reported: 29 Cases

- FALSE: 93.1%
- TRUE: 6.9%

Attack Detected by IT Staff: 29 Cases

- FALSE: 86.21%
- TRUE: 13.79%

Other Internal (reported attack): 29 Cases

- FALSE: 65.52%
- TRUE: 34.48%

Attack Detected by a Customer: 29 Cases

- FALSE: 89.66%
- TRUE: 10.34%

Attack Detected by Law Enforcement: 29 Cases

- FALSE: 96.55%
- TRUE: 3.45%

Attack Detected by Unknown Party: 29 Cases

- FALSE: 65.52%
- TRUE: 34.48%

Response to Attack-Incident Response Team: 29 Cases

- FALSE: 96.55%
- TRUE: 3.45%

Response to Attack-Other Technical Response: 29 Cases

- FALSE: 96.55%
- TRUE: 3.45%

Response to Attack—Management: 29 Cases

- FALSE: 86.21%
- TRUE: 13.79%

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS

In this analysis chapter, using the case study method, the author answers the research question: Insiders are committing fraud and embezzlement within organizations, does a connection exist to addiction as a motivating factor? The basis for this research and the nexus to his research question was formed by his current role as the Special Agent in Charge of the USSS, Louisville Field Office. In this role, he began to notice what he believed was an unusual amount of fraud and embezzlement cases in which the defendants were trusted insiders, who had addictive behaviors as the motivating cause for their illegal behavior.[197] He conducted an informal examination of 11 current and open criminal cases of fraud and embezzlement in Kentucky for the years 2010 to 2013 to determine if addiction played a role in the cases. At the time of this review, he observed that six out of the current 11 open and active criminal cases involving insiders within organizations were addicted to either gambling or pain prescription medication, which served as the motivating factor for their illegal behavior against the victims' organizations.

The goal of this research was to answer the research question and identify gaps in the literature on insider threats to organizations, primarily as it relates to trusted insiders committing fraud and embezzlement within private, public, and non-profit organizations, with a connection to addiction as the motivating factor for the insider's illegal behavior. The literature showed that an insider who has an addiction, especially to gambling or pain prescription medication, is susceptible to committing fraud and embezzlement to finance and support this addiction.[198] The research presented a strong correlation between insider

[197] In reviewing an open criminal case in 2013, on a $1.7 million embezzlement investigation, the author discovered from the case agent that a trusted insider, responsible for the finances of a non-profit organization, had used the entire amount of funds he embezzled for the sole purpose of feeding a gambling addiction with which both he and his wife were involved. The investigation had revealed through numerous wire transfers over the period of several months that $1.7 million had been illegally transferred to several casinos and withdrawn by the insider and his spouse.

[198] "About NCPG," accessed February 2, 2014, http://www.npgaw.org/problemgamblinginformation/factsfigures.asp; *National Research Council. Pathological Gambling: A Critical Review. Committee on the Social and Economic Impact of Pathological Gambling, Committee on Law and Justice, Commission on Behavioral and Social Sciences and Education.*

fraud and embezzlement cases with addiction as the motive for the insider's illegal behavior. Also discovered through research was an indication that causation, as well as motivation, is not often specified on police reports of fraud and embezzlement investigations, even when an addiction may be implied as the motivating factor for the criminal offense.

The case study method was used in this paper in which 40 recently closed USSS criminal cases were studied involving trusted insiders convicted of fraud or embezzlement. Four Secret Service Field Offices including the Louisville, Cincinnati, Nashville and Memphis Field Offices examined 10 closed cases each from the years 2002–2013. The research focused on attempting to determine the motivating factors for the defendants' reasons for committing their crimes in each case.

Contributing research conducted by CERT at Carnegie Mellon University's Software Engineering Institute was also used for this thesis. CERT queried its Insider Threat Database that consisted of 680 criminal cases involving IT crimes. This query and subsequent research was used to determine if any of the insider threat cases in the CERT database had addiction identified as a motivating factor for the insider's illegal behavior against the victim organization.[199]

A. SECRET SERVICE CASE STUDIES

In the 40 USSS case reviews, motives for the 45 trusted insiders' conducting fraud or embezzlement against the victim entities varied when the causality of the crime could be determined.[200] The recorded motivations for all 40 cases were: gambling addiction, pain prescription medication addiction, heroin addiction, sex addiction, binge shopping disorder, an enhanced lifestyle, financial pressures, and other unknown motives.

[199] CERT claims to have the largest collection of detailed insider threat cases in the world. CERT used the search term "addiction" in its database to determine if addiction related motives could be measured as contributing factors for the insiders' motives for conducting their illegal behavior. CERT only used addictive behaviors if it was clearly documented in their research database. The author relied solely on CERT to provide this information; Cappelli, Moore, and Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, xix.

[200] In several cases, more than one insider was involved in the criminal activity; for this reason, 45 convicted insiders were convicted in 40 cases.

In all four USSS Field Offices, addiction, primarily to gambling and pain prescription medication combined, was the primary motivating factor for the insiders' illegal behavior when an addiction or addictive behavior was indicated. In fact, as the chart in Figure 7 indicates, 23 out of the 45, or 51% of the convicted insiders, had an addiction related behavior as the insiders' primary motivation for committing the crime.

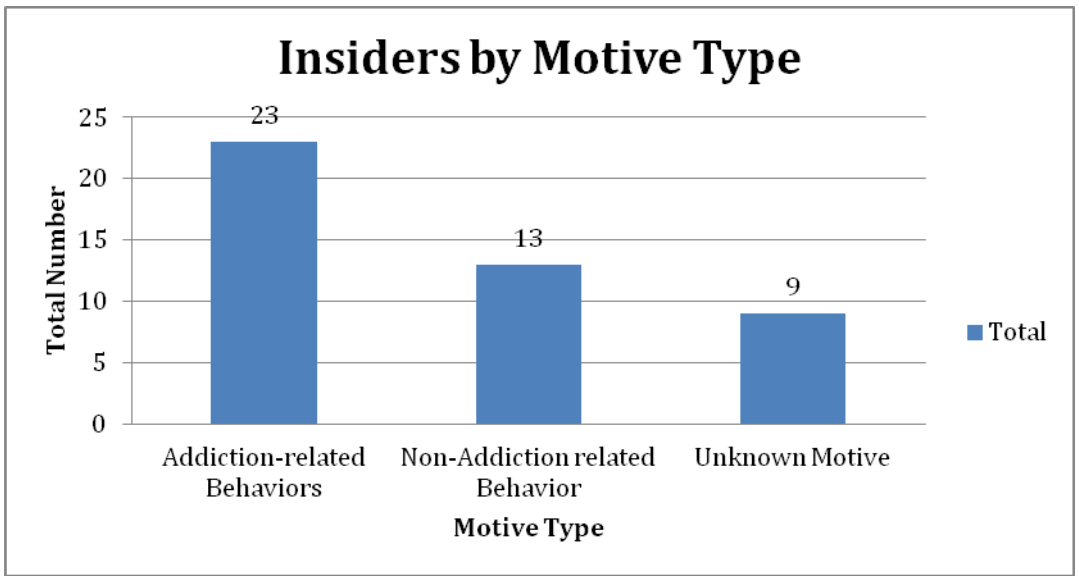

Figure 7. Secret Service Case Studies Showing Addiction Related Behavior in 23/45 Insiders Convicted of Fraud or Embezzlement

In 13 out of the 23 USSS case studies, in which addiction was reported, an addiction to gambling was the predominant motivating factor for the trusted insiders' illegal behavior for conducting fraud or embezzlement within the victim organization. Meyer and Stadler assert with addiction related behaviors in which an individual is addicted to gambling, "The majority of clinical studies on pathological gamblers in outpatient treatment centers and self-help groups indicate that a high percentage of subjects committed offenses in order to finance their gambling."[201] Respected gambling authors and researchers, Richard Rosenthal and Henry Lesieur, argue, "Academic research and numerous criminal cases have shown the existence of a causal relationship

[201] Meyer and Stadler, "Criminal Behavior Associated with Pathological Gambling," 29–43.

between criminal behavior and pathological gambling."[202] Paul and Townsend contend that:

> An estimated 80% of American adults gamble, and as many as 10% may become pathological gamblers. Research on compulsive gamblers indicates that 85% will commit felony crimes of a financial nature during their addiction, 86% are gainfully employed, more than 90% will destroy their family life, 90% will steal from their employers and 95% will have a negative impact on workplace morale and perform poorly on the job.[203]

Virgil Peterson states, "Regardless of whether gambling is the direct or indirect cause of employee dishonesty, it is one of the most important factors contributing to embezzlement."[204] Several fraud and embezzlement academic research texts and articles on the connection between gambling and criminal behavior also support this relationship.[205]

In 1998, Dr. Henry Lesieur, the aforementioned criminology professor at Illinois State University and one of the leading experts on gambling research, told the U.S. National Gambling Impact Study Commission, "that while some problem gamblers commit street crime, the overwhelming majority of them are committing embezzlement, forgery and fraud." Also noted in the Commission Report was the fact that nearly two-thirds of compulsive gamblers surveyed have engaged in illegal activities to pay gambling debts or to continue gambling.[206]

Supportive of the literature on addiction and the commission of financial crimes, it should be noted that in Louisville case 8, the insider had an addiction to both gambling and pain prescription medication as the cause and motivating factor for his illegal

---

[202] Rosenthal and Lesieur, "Pathological Gambling and Criminal Behavior," in *Explorations in Criminal Psychopathology: Clinical Syndromes with Forensic Implications*, 149–169.

[203] Robert J. Paul and James B. Townsend, "Managing Workplace Gambling—Some Cautions and Recommendations," *Employee Responsibilities and Rights Journal* 11, no. 3 (September 1998): 171.

[204] Peterson, "Why Honest People Steal," 96.

[205] Donald R. Cressey, "The Criminal Violation of Financial Trust," *American Sociological Review* 15, no. 6 (December 1, 1950): 738–743, doi:10.2307/2086606; Zietz, *Women Who Embezzle or Defraud: A Study of Convicted Felons*; Ragatz, Fremouw, and Baker, "The Psychological Profile of White-collar Offenders Demographics, Criminal Thinking, Psychopathic Traits, and Psychopathology," 978–997; Wells, *Corporate Fraud Handbook: Prevention and Detection*.

[206] *National Gambling Impact Study Commission, Final Report*, 7–13.

behavior. The trusted insider embezzled over $1.1 million, and as the criminal case report indicated, "His addiction to gambling and pain prescription medication had become out of control."[207] Rosenthal and Lesieur indicate, "there is a significant overlap between pathological gambling and chemical dependency."[208] In Nashville case 8, the insider had an addiction to gambling and a sex addiction indicated as a dual cause or motive for the illegal activity.[209] Again, this finding was also consistent with the literature in which more than one addiction is not uncommon.[210]

Gambling addiction was followed by an addiction to pain prescription medication as the second primary motive in the USSS case studies. In seven of the 23 cases of addiction related behavior, pain prescription medication addiction was indicated as the primary motivation for the insider threat. All seven cases were investigated in Kentucky. As research demonstrates, according to the U.S. Centers for Disease Control and Prevention (CDC), prescription drug abuse is the nation's fastest growing drug problem and has been classified as an epidemic.[211] Kentucky has the third highest drug overdose mortality rate in the United States, with 23.6 per 100,000 people suffering drug overdose fatalities, according to a new report, "Prescription Drug Abuse: Strategies to Stop the Epidemic."[212] "The number of drug overdose deaths—a majority of which are from prescription drugs—in Kentucky quadrupled since 1999 when the rate was 4.9 per 100,000."[213] See Figure 8.

---

[207] See Louisville Case #8 in Chapter III Case studies.

[208] Rosenthal and Lesieur, "Pathological Gambling and Criminal Behavior," in *Explorations in Criminal Psychopathology: Clinical Syndromes with Forensic Implications*, 32.

[209] See Nashville Case #8 in Chapter III Case studies.

[210] Frances, Miller, and Mack, *Clinical Textbook of Addictive*.

[211] The White House, "Office of National Drug Control Policy."

[212] Trust for America's Health, "Prescription Drug Abuse: Issue Report 2013—Strategies to Stop the Epidemic," October 2013, http://healthyamericans.org/assets/files/TFAH2013RxDrugAbuseRptFINAL.pdf.

[213] Trust for America's Health, "Drug Abuse 2013 Data for Kentucky," October 7, 2013, http://healthyamericans.org/reports/drugabuse2013/release.php?stateid=KY.

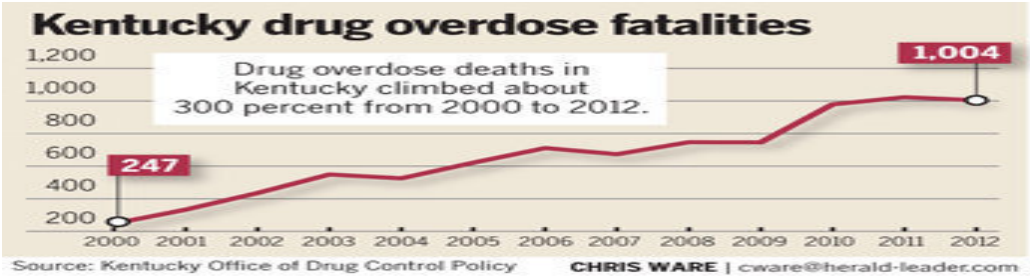

Figure 8. Kentucky Drug Overdoes Fatalities

Also, according to the CDC, "the sharp increase in opioid prescribing has led to parallel increases in opioid addiction and overdose deaths." Since 1999, it was reported that, "overdose deaths have risen steeply in the United States, especially among middle-aged individuals who have been prescribed opioids for chronic pain. Opioid analgesic overdose deaths have increased by 415% in women and 265% in men."[214] To provide a perspective on the significance of drug overdose statistics in the United States, the CDC reports:

> Drug overdose was the leading cause of injury death in 2010. Among people 25 to 64 years old, drug overdose caused more deaths than motor vehicle traffic crashes. In 2010, of the 38,329 drug overdose deaths in the United States, 22,134 (60%) were related to pharmaceuticals. Of the 22,134 deaths relating to prescription drug overdose in 2010, 16,651 (75%) involved opioid analgesics (also called opioid pain relievers or prescription painkillers), and 6,497 (30%) involved benzodiazepines.[215]

These statistics reflect directly on the costs to law enforcement, the medical community, and the employers and families of those individuals affected by prescription opioid drug abuse in this country. The CDC further reports, "more than 60 people die every day in the United States from overdosing on prescription drugs. Prescription opioid abuse resulted in more than 400,000 emergency department visits in 2011, and cost health insurers an estimated $72 billion annually in medical costs."[216] As a comparison,

---

[214] Centers for Disease Control and Prevention, "QuickStats: Number of Deaths From Poisoning,* Drug Poisoning,† and Drug Poisoning Involving Opioid Analgesics§—United States, 1999–2010," March 29, 2013, http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6212a7.htm.

[215] Paulozzi, "Prescription Drug Overdoses: A Review," 283–289.

[216] "CDC—Prescription Drug Overdose Prevention. FY 2015 President's Budget Request|$15.6 Million," accessed March 17, 2014, http://www.cdc.gov/injury/pdfs/budget/NCIPC_PDO_FY2015-a.pdf.

the CDC reports that homicide rates of people killed by firearms in the United States averages 30 per day, compared with 60 people per day dying from overdosing on prescription drugs.[217] An increase in addiction to pain prescription medication in the general population suggests an accordant increase in insider threats because of that upward trend.

In a recent publication of the "Societal Costs of Prescription Opioid Abuse, Dependence, and Misuse in the United States," the authors opined, "The costs of prescription opioid abuse represent a substantial and growing economic burden for the society. The increasing prevalence of abuse suggests an even greater societal burden in the future."[218] According to the study, the costs are significant:

> Total U.S. societal costs of prescription opioid abuse were estimated at $55.7 billion in 2007 (USD in 2009). Workplace costs accounted for $25.6 billion (46%), health care costs accounted for $25.0 billion (45%), and criminal justice costs accounted for $5.1 billion (9%). Workplace costs were driven by lost earnings from premature death ($11.2 billion) and reduced compensation/lost employment ($7.9 billion). Health care costs consisted primarily of excess medical and prescription costs ($23.7 billion). Criminal justice costs were largely comprised of correctional facility ($2.3 billion) and police costs ($1.5 billion).[219]

A 2006 study placed the costs of the misuse and abuse of prescription painkillers for the country at an estimated $53.4 billion a year in lost productivity, medical costs, and criminal justice costs.[220] National statistics suggest that addiction to this type of drug is quite concerning as reported in a recent letter to the Commissioner of the U.S. Food and Drug Administration by the Coalition to End the Opioid Epidemic, in which they contend, "Over the past 15 years, prescriptions for opioids have skyrocketed" in the United States. According to the hydrocodone and oxycodone consumption statistics as reported by the International Narcotics Control Board in 2012, "The United States, with

---

[217] Centers for Disease Control and Prevention, "FASTSTATS—Homicide," 2010, http://www.cdc.gov/nchs/fastats/homicide.htm.

[218] Howard G. Birnbaum et al., "Societal Costs of Prescription Opioid Abuse, Dependence, and Misuse in the United States," *Pain Medicine* 12, no. 4 (2011): 657 doi:10.1111/j.1526-4637.2011.01075.x.

[219] Ibid., Abstract.

[220] "Drug Abuse 2013 Data for Kentucky."

about 5% of the world's population, is now consuming more than 84% of the world's entire oxycodone supply and more than 99% of the hydrocodone supply."[221]

USSS Louisville Case 2 was a public sector, insider threat case, which was widely reported in the news, and involved the former executive director of a city-county convention center convicted of embezzlement along with a co-conspirator. "They devised a scheme to steal money that was intended for the greater good of the community," stated the U.S. Attorney for the Western District of Kentucky. "In doing so, they violated the public's trust and harmed an important community asset." The trusted insider embezzled $250,000 of taxpayer's money to support his addiction to pain medication.[222] It is important to note that this incident offers insight into the overriding nature of an addiction to pain prescription medication. In a review of the criminal case notes and file, as well as interaction with the case agent during the course of the investigation, the insider in this incident, "possessed an all consuming desire to do anything, in order to finance his addiction." The insider admitted to taking 40 to 60 Lortab pain pills per day. Had an alert bank employee in this case not followed up on suspicions of an unusual check deposit by the convicted insider, this criminal conduct may have continued costing the taxpayers in Western Kentucky an unknown sum of money through his ongoing embezzlement.[223] As a homeland security concern, anytime a trusted insider working within a government agency has an addiction, that government agency is vulnerable to compromising behavior by the insider who can significantly affect the reputation, integrity, and ultimately, threaten the public's trust of a community organization.

---

[221] FED Up Coalition Steering Committee, "Zohydro Letter with Signatures Final," February 26, 2014, http://www.citizen.org/documents/2185.pdf.

[222] USDOJ, "Convention Center's Former Executive Director Sentenced to 24 Months in Prison for Embezzlement."

[223] As the case agent's supervisor during the course of the criminal investigation in Louisville Case 2, the author was able to have first hand knowledge of the convicted insider's motivation for his criminal behavior and was able to gain insight from the criminal case file on the insider's conduct concerning his addiction.

B. CERT CASE STUDIES

The contributing research conducted for this thesis by CERT at Carnegie Mellon University from its Insider Threat Database consisted of a data search on 680 criminal cases involving IT crimes. The research revealed that 29 insiders indicated that addiction was a primary motivator for conducting their criminal behavior. In 24 out the 29 insider threat cases, drug use and gambling was indicated as the addiction behavior trait. Drug use was indicated as the addiction motivation in 15 cases, followed by gambling in six cases.[224] Alcohol and drug use was indicated in three of the cases, and in five cases, alcohol use was the indicator for the causation of the insiders' illegal behavior.[225] See Figure 9. As previously noted in Chapter III from the CERT research was the fact that the primary area for addiction related behavior came from the fraud category, with 21 out of the 29 instances coming from that classification.[226] This fact is important as it is aligned with the literature on addiction, as trusted insiders who have addictions are often compelled with the need to continue financing their addiction.[227]

[224] CERT was unable to break down the exact types of drug use in its database so it is unknown what the specific drug type was that was indicated by the insider.

[225] CERT conducted a data search of its insider threat database as a request by the author for research conducted on this thesis. Data and figures were provided by CERT as a result of its data search. See Chapter III CERT Insider Threats Case Studies.

[226] As noted in Figure 4 from the CERT section in Chapter III, 300 fraud cases were found in the CERT database; thus, the 21 cases would be out of a total of 300 total fraud cases.

[227] Green, "White-Collar Crime and the Study of Embezzlement," 95–106; Lesieur, *The Chase: Career of the Compulsive Gambler*, vol. xxi; Griffin, "Major Embezzlement Cases on the Rise."

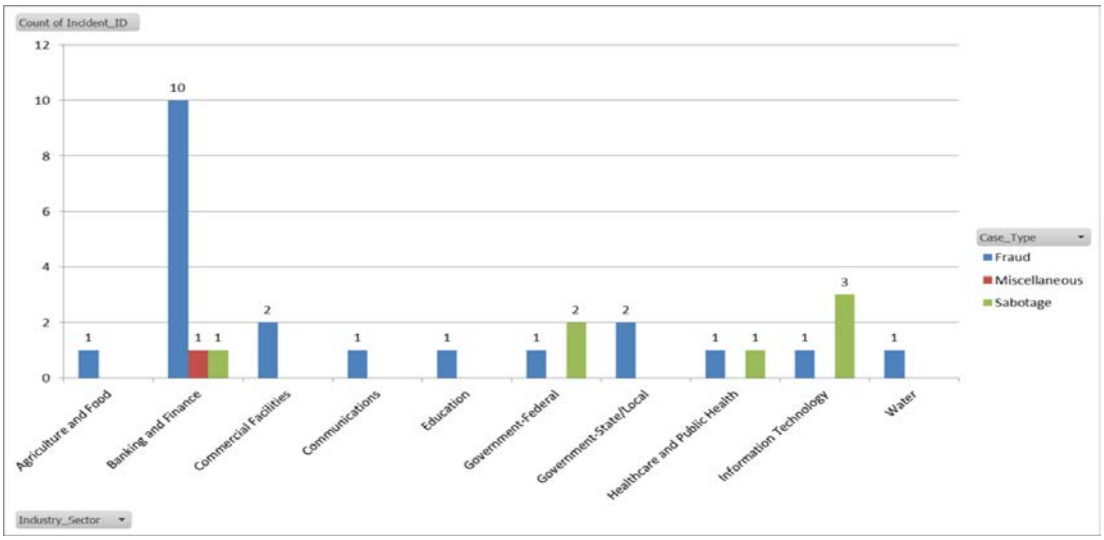

Figure 9. CERT Insider Threat Cases with Addiction As a Motivating Factor Broken Down by Sectors.[228]

C. CONCLUDING SUMMARY OF CASE STUDIES: SHOULD THIS NATION BE CONCERNED ABOUT ADDICTION?

As seen from the 29 aforementioned CERT cases, as well as the USSS cases involving fraud or embezzlement by trusted insiders, 23 out of the 45 convicted insiders had an addiction related motive behind their illegal behavior. Although addiction is not the only cause for a trusted insider to commit fraud or embezzlement against an organization, research shows it is clearly an important cause. Also discerned from the research is that fraud and embezzlement can occur for many other reasons: financial pressures, greed, an enhanced lifestyle, or in some cases, unknown reasons. However, it is seen that in cases in which addiction was established prior to the fraud or embezzlement occurring, the insiders committed their illegal behavior out of the need to feed that addiction financially.

1. Recent Criminal Cases That Should Concern Homeland Security Officials about Addiction and Trusted Insiders

As was the case with the former tax clerk and trusted insider from Chapter I who embezzled $50 million over an 18 year time period from the taxpayers of the District of

[228] This graph was provided by CERT for this thesis research.

Columbia, it is important to recognize some considerations.[229] A trusted insider with authority and access to operate freely within any organization who is intent on committing criminal acts to finance an addictive behavior should concern not only law enforcement professionals, but leadership from all across private, non-profit, and public sector organizations.[230]

The research has indicated that individuals who are addicted to gambling or pain prescription medication will commit fraud and embezzlement to continue financing their addiction if they have no other means to do so.[231] Chapter II demonstrated cases of trusted insiders who have committed treason against the United States financially to support their addiction to gambling.[232] Research has shown former FBI agents who had access to national security secrets and who worked on some of the nation's most sensitive foreign counter intelligence investigations having been convicted of embezzling funds from the government to finance their addiction to gambling.[233] These individuals include a former senior FBI supervisor who oversaw a major metropolitan drug task force and embezzled funds from the government over a long period of time to finance his gambling addiction. This trusted insider also lied to a federal judge for the promise of money to pay off gambling debts by an organized crime figure.[234]

Former major city mayors have been convicted of embezzling money due to their gambling addiction.[235] Consider the former mayor of San Diego who embezzled over $2 million due to her gambling addiction.[236] Mayors are trusted insiders with access to

---

[229] Southall, "17-Year Term for Official in Tax Scam."

[230] "2012 Report to the Nations—Key Findings and Highlights."

[231] Rosenthal and Lesieur, "Pathological Gambling and Criminal Behavior," in *Explorations in Criminal Psychopathology: Clinical Syndromes with Forensic Implications*; "Prescription Drugs Elevate Crime Rate," accessed March 6, 2014, http://narconongeorgia.hubpages.com/hub/Prescription-Drugs-Elevate-Crime-Rate; Green, "White-Collar Crime and the Study of Embezzlement."

[232] Herbig and Wiskoff, "Espionage Against the United States by American Citizens 1947–2001, PERSEREC Technical Report 02–5."

[233] Clay, "Ex-FBI Agent in Oklahoma Gets Six Months in Prison for Embezzling."

[234] Lebowitz, "Ex-FBI Agent Sentenced to Five Years in Prison."

[235] Annie Karni, "Real Mayors of New Jersey," *New York Post*, June 24, 2012, http://nypost.com/2012/06/24/real-mayors-of-new-jersey/.

[236] Spagat, "Ex-San Diego Mayor's Gambling Wagers Top $1B."

highly sensitive information regarding critical infrastructure, vulnerable city financial documents and contracts, and authorization to make and influence decisions that affect the entire community, because of their trusted position in the government.[237] The U.S. military is not immune from gambling issues as well; in a recent incident, the second highest-ranking officer of the nation's nuclear forces was arrested for passing counterfeit poker chips at a local casino. The former Vice Admiral was "suspended from oversight of nuclear weapons or any responsibilities involving classified material."[238]

The question that must be asked is how to recognize and understand that trusted insiders with addictions are potentially capable of compromising national security within public sector organizations or causing catastrophic financial harm, even to the point of bankrupting some firms to feed their addiction? What are the warning signs of a trusted insider with an addiction? Gambling and using prescribed pain prescription medication by Americans in a responsible way is both legal and common all across the homeland; however, committing fraud and embezzlement against organizations to finance an addiction to gambling or pain prescription medication is not. Simply being aware that a trusted insider is gambling or using pain prescription medication is a start.

2. Causes and Motives for Committing Fraud and Embezzlement Matter

The research and literature illuminated a gap in the reporting of causes and motives in fraud and embezzlement cases reporting by law-enforcement agencies. Currently, 18,000 participating local, state, and federal law enforcement agencies in the United States are annually required to provide to the FBI Uniformed Crime Report (UCR) statistics concerning acts of crime, by age, gender, race, and location under the traditional Summary Reporting System (SRS). However, motive and causality are not statistical data required by the UCR in criminal cases. This fact is especially true in fraud and embezzlement crimes, as it is a Schedule 2 offense, and the only required reporting

---

[237] "Homeland Security Blog," accessed March 18, 2014, http://www.dhs.gov/blog.

[238] Steve Liewer, "StratCom Deputy Chief Fired as Nation's No. 2 Nuclear Commander," *Omaha.com*, October 10, 2013, http://www.omaha.com/apps/pbcs.dll/article?AID=/20131009/NEWS/131008617.

of those offenses is age, sex and race.[239] This type of reporting is a significant concern for anyone conducting research on causes of crimes, since the information is not always recorded and preserved with the case.

Another weighty issue with the UCR reporting is that it is also very difficult to provide accurate white-collar criminal offense statistics, which typically include fraud and embezzlement cases as noted by the FBI:

> Under the traditional Summary Reporting System (SRS), there is a limited amount of information available on white-collar crime. The white-collar offenses that are measured are fraud, forgery/counterfeiting, embezzlement, and all other offenses. Because white-collar crimes are not Index crimes, the only information available on these offenses is arrest information, which includes age, sex, and race of the arrestee. Additionally, the all other offenses arrest category is very limited in its ability to measure the white-collar offenses included in its counts. This is due to the inability to differentiate the white-collar offenses from the others that also fall in this category. Based upon the most recently published data from the FBI, the arrest rates for the offenses of embezzlement, fraud, and forgery/counterfeiting are much lower than the arrest rates for property crime or for total crimes in general.[240]

Fortunately, the FBI and Department of Justice have created the FBI UCR Program's National Incident-Based Reporting System (NIBRS) with the intent to improve the quantity and quality of crime data collected by law enforcement. The NIBRS captures more detailed information for each single crime occurrence than the traditional SRS.

> The NIBRS identifies when and where crime takes place, what form it takes, and the characteristics of its victims and perpetrators. As more law enforcement agencies (LEAs) submit their crime data via the NIBRS, they—along with legislators, municipal planners and administrators,

239 "Offenses in Uniform Crime Reporting—Crime in the United States 2004."

240 Cynthia Barnett, "The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data," *U.S. Department of Justice Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Division*, accessed March 14, 2014, http://www.fbi.gov/stats-services/about-us/cjis/ucr/nibrs/nibrs_wcc.pdf.

> academicians, researchers, and the general public—will be better able to assess the scope of the nation's crime problem.[241]

In its second year, the recently published *NIBRS 2012* report shows crime details captured through incident-based reporting.

> This second compilation of annual NIBRS data represents crime reported for calendar year 2012 by 6,115 Law Enforcement Agencies (LEAs) around the nation, approximately 33 percent of all agencies that submit data to the FBI UCR Program. The data include information on incidents, offenses, victims, and known offenders for 46 specific crimes in 22 major offense categories. The report details the age, sex, and race of victims, offenders, and arrestees; crime locations and times of day; and the type of weapons and force involved. Comprised of 97 tables, *NIBRS 2012* features 32 offense tables about crimes against persons, crimes against property, and crimes against society; 24 tables on sex offenses; 36 tables that list offenses by state by individual law enforcement agency; and 5 tables focusing on the demographics of the arrestees connected to NIBRS incidents.[242]

Only 15 states participate in the NIBRS, but it is a remarkable improvement for crime statistics and collection of incident-based reporting. Although currently a category for law enforcement agencies does not exist to report motive and cause of a crime for an offender committing a fraud or embezzlement case, "the agencies that submit data via the NIBRS can report an offender's suspected involvement with drugs/narcotics, alcohol, or gangs in committing an offense."[243]

This issue is important for researchers to note, as Smith et al. have expressed in their study on gambling and crime, "The fact that official police statistics and court records do not show gambling-related crime to be a serious problem, yet knowing that police and court databases are incomplete to the extent that gambling is seldom identified

---

[241] Federal Bureau of Investigation, Criminal Justice Information Services Division, "2012 National Incident-Based Reporting System," accessed March 17, 2014, http://www.fbi.gov/about-us/cjis/ucr/nibrs/2012/nibrs-2012-home.

[242] Ibid.

[243] Federal Bureau of Investigation, Criminal Justice Information Services Division, "2012 National Incident-Based Reporting System," accessed March 17, 2014, http://www.fbi.gov/about-us/cjis/ucr/nibrs/2012/nibrs-2012-home.

as a motive or precipitating factor for crime."[244] The implications of this finding are significant for law enforcement agencies to recognize that causation and motives are critical to document and account for in police reports. The significance for homeland security and the role that law enforcement plays in recognizing that motives, especially documenting addiction as a motive for committing criminal offenses, are essential for building accurate databases. It is critical for law enforcement professionals and researchers to understand what the prevalence of addiction is in contributing to causing fraud and embezzlement within organizations. Needless to say, it is also important to understand what role addiction plays in causing all types of crime.

The USSS investigates thousands of financial crimes cases each year across the United States and abroad. More specifically, it closes approximately 500 criminal investigations under the categories of fraud, embezzlement, and misappropriation on an annual basis.[245] As has been previously discussed in this paper, this category is most closely indicative of a trusted insider committing a financial crimes offense within or against an organization in which the insider is employed or within which has authorized access and authority to operate.[246]

The USSS does not require its investigators to report cause of a financial crime in a format that can be captured electronically for statistical recording purposes. Also, no requirement exits for a USSS Special Agent investigating a financial crimes case to report an individual's motive for committing the crime. The USSS investigates numerous financial crimes cases committed against organizations by trusted insiders conducting fraud or embezzlement each year, yet no mechanism is currently in place to require an investigating Special Agent to capture or report when the defendant may have had an

[244] Smith, Wynne, and Hartnagel, *Examining Police Records to Assess Gambling Impacts: A Study of Gambling-related Crime in the City of Edmonton*.

[245] Management and Organization Division, *United States Secret Service Annual Statistical Report—Fiscal Year 2013*.

[246] This category of financial crimes investigation most closely aligns with investigations of insiders conducting fraud and embezzlement offenses within organizations and does not encompass all Secret Service financial crimes investigations against individuals or organizations.

addiction to gambling, pain prescription medication, or any other addiction related behavior as the reason for conducting the illegal activity.[247]

This lack of reporting is important to consider as it relates directly to anyone conducting research on gambling and gambling related criminal offenses. Blaszcynski and Silove note that:

> Accurate rates of the prevalence and extent of gambling-related criminal behaviors are difficult to obtain. Arrest and conviction rates are inadequate because gambling is not necessarily identified on conviction records as underlying the offense, and not all gambling related offenses are detected or offenders apprehended. Therefore, the true prevalence rate is likely to be underestimated.[248]

As Blaszcynski and Silove contend in their argument of recording accurate rates of the prevalence and extent of gambling-related criminal behaviors, a similar contention should be made with regard to obtaining documentation on any addictive behavior as a motive in law enforcement records.[249] One way to advance awareness is to require such reporting by law enforcement and make this information widely available.

The KSP is responsible for retaining criminal police records and traffic offense reports for over 400 city and county law enforcement agencies throughout the Commonwealth of Kentucky. The KSP is also charged with compiling the annual statistics on crimes within the Commonwealth of Kentucky and reporting those to the UCR at the FBI. The KSP currently does not participate in the FBI UCR Program's NIBRS.[250]

---

[247] As the Special Agent in Charge of the U.S. Secret Service, Louisville Field Office, with over 25 years of experience in criminal investigations, the author can report that no requirement exists for Special Agents to include in their case reports, causality or motive, for a perpetrator of a criminal offense in a financial crimes investigation, as to their reason for committing a criminal offense.

[248] Blaszczynski and Silove, "Pathological Gambling: Forensic Issues."

[249] The author's experience as a law enforcement professional and senior executive suggests that law enforcement agencies are generally more concerned with accurately reporting statistics on how much crime is occurring in their districts, where it is occurring, and by what method is it occurring. It is also his contention in financial crimes investigations, law enforcement officials tend to care more about discovering who is conducting criminal behavior, proving a criminal case against them, providing the necessary documentation and evidence for prosecuting them, and moving on to the next case, than they are in trying to determine why the perpetrators committed the criminal act and what motivated them to do so.

[250] Kentucky Legislature, "Kentucky Revised Statutes," 2013, http://www.lrc.ky.gov/statutes/index.aspx.

The KSP Records Division reports that modus operandi (MO) is captured in the report only if the reporting officers include it in their narrative. MO is generally defined in relationship to how a criminal act occurred. An example of MO would be the method used to embezzle funds from a business, such as writing fraudulent checks on a business account. This data is not recoverable via an electronic report search and would only be recoverable by an individual record search of the case file. Furthermore, this information could only be retrieved if the reporting officer recorded it in the police report. The record does not report the causation or motive of why a crime occurred.[251]

The KSP Records Division advises that it is not currently able to capture causes (motives) of criminal offenses as it relates to Chapter 514 of the Kentucky Penal Code, Theft and Related Offenses. Chapter 514 encompasses theft, fraud and embezzlement offenses under the Kentucky Revised Statutes. The KSP also confirms that it is unable to capture cause or motive of criminal offenses for most criminal offenses, with the exception of fatal traffic accidents.[252] Addiction related causes or motives for a criminal offense, such as an addiction to gambling, pain prescription medication or alcohol, is not currently captured under reporting statistics in the Commonwealth of Kentucky.[253]

As one state official reported, "We are very good at telling you what caused a traffic accident. We can provide you with what the road conditions were at the time of the accident, if the driver was impaired or not, if the vehicle had faulty equipment, or if there was excessive speed as a mitigating factor in an accident, but we have no way of providing statistical analysis of causes or motives for an individual committing a criminal offense in the Commonwealth of Kentucky."[254]

---

[251] Ibid.; Kentucky State Police, "Commonwealth of Kentucky 2012 Crime Report."

[252] Ibid.

[253] Kentucky State Police, "Commonwealth of Kentucky 2012 Crime Report"; Kentucky Legislature, "Kentucky Revised Statutes."

[254] This information was derived from anonymous subject matter experts within the Kentucky State Police during the research phase of this thesis on determining if the agency was able to provide motive or causation of criminal offenses, specifically fraud and embezzlement investigations, to determine if addiction was a possible contributor in the motive for individuals conducting their illegal behavior.

A revealing fact discovered throughout the research of this thesis is the USSS as a federal agency, as well as most local and county law enforcement agencies throughout the Commonwealth of Kentucky including the Kentucky State Police, are not recording cause or motive for perpetrators committing their crimes, which is especially true for fraud and embezzlement cases conducted by trusted insiders within organizations. However, it should be noted that in spite of the inability to determine cause and motive of these crimes in the Commonwealth of Kentucky it is important to notice that addiction does play a role.

In a recent report from the Kentucky Department of Corrections, drug offenses account for a significant role in the current prison population, as well as in its current parolee population as Table 3 and Figure 10 show.[255] It would be helpful for law enforcement practitioners and researchers to know how many of these individuals are incarcerated due to an addiction to drugs or how many prisoners or parolees committed crimes to feed their addiction to drugs.

TYPE	TOTAL	DRUG OFFENSE	
		COUNT	PERCENTAGE
Active Parolee	14237	7895	55.45%
Active Inmate	20664	6808	32.95%
TOTAL	34901	14703	42.13%

Table 3. Kentucky Department of Corrections 2014

[255] Figures provided by the Kentucky Department of Corrections for current March 2014 inmate and parole populations who have a drug related conviction.

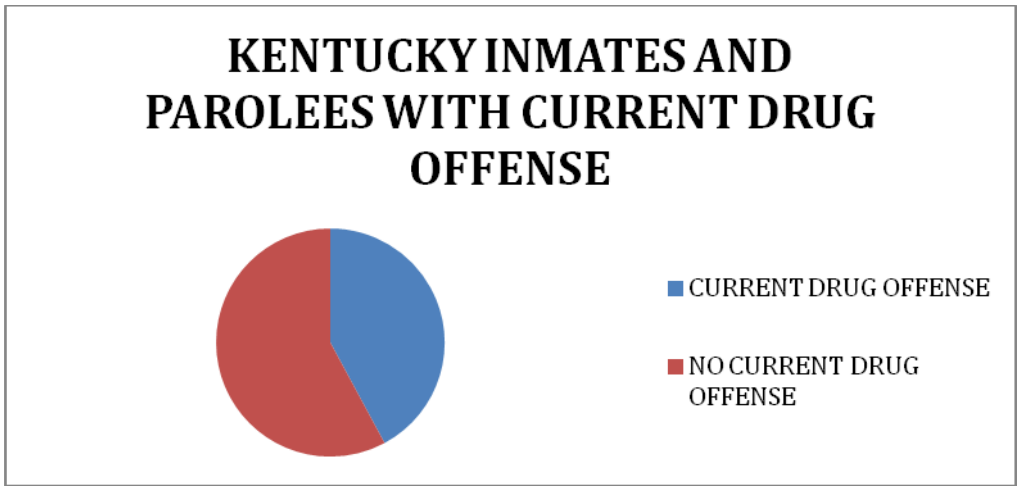

Figure 10. Kentucky Department of Corrections 2014

The reality is that in most cases, motive for an offender conducting illegal behavior or activity is not required on law enforcement reports. In the event that this information is recorded in law enforcement reports, it is not easily recoverable, and does not provide the ability to research individual case files for statistical reporting or research purposes. The gap in this type of reporting is one worth investigating, as cause and motive matter, when it comes to reporting fraud and embezzlement cases.[256]

It was reported that $193 billion is the estimated cost of drug use to the U.S. society in lost productivity, health care, and criminal justice costs in 2007.[257] Therefore, it is important to determine how much criminal activity individuals conduct due to an addiction, as the primary motive for committing fraud and embezzlement, or for that matter any criminal behavior.

[256] Blaszczynski and Silove, "Pathological Gambling"; P. Crofts, *Gambling & Criminal Behavior: An Analysis of Local & District Court File*, 2002.

[257] U.S. Department of Justice, National Drug Intelligence Center, "National Drug Threat Assessment 2011," August 2011, http://www.justice.gov/archive/ndic/pubs44/44849/44849p.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS AND CONCLUSIONS

This concluding chapter highlights the research finding that trusted insiders are committing fraud and embezzlement against organizations and indicate a connection exists to addiction as a primary cause or motive for many convicted insiders who have conducted illegal behavior within their organizations. This research indicates that insiders with addictions will embezzle or commit fraud to provide a funding mechanism to continue financing their addiction. What is clear is that insider threats are a reality that will continue to be a concern to any organizations that contain valuable assets. This paper has noted that valuable assets are not only located in company bank accounts and financial data resources, but are also deemed to be anything of worth that could be compromised or stolen, including intellectual property, sensitive proprietary data or any information or resources controlled by an organization. These assets can also involve access to classified data networks and to government secrets.

History has shown that the effects of a successful fraud or embezzlement scheme perpetrated against any institution can cause enormous financial harm, damaging its reputation, and even bankrupting some organizations. This finding is significant for homeland security officials to be cognizant of, as this research indicates that trusted insiders within government agencies are also committing criminal offenses to sustain addiction.

The author discusses a strategy for providing recommendations aimed at addressing the problem of insider threats to organizations in which addiction is determined to be a cause or motivating factor for conducting fraud and embezzlement. He suggests that the research is indicative of a lack of reporting by law enforcement agencies in investigative reports in which addictive behavior as a motive or cause of a crime is not being reflected, captured, or recorded. This lack of detailed reporting on motives for criminal activity is unfortunately a part of standard operating practice for most law enforcement agencies, and in fact, is not required for national reporting standards for the UCR or the NIBRS. This factor was especially evident in the fraud and embezzlement cases examined as a part of this research. The author suggests that law enforcement

agencies, such as the USSS and the Kentucky State Police, begin a program of assessing and collecting motives, as well as causes of criminal acts, and specifically, measure whether addiction plays a role in motive and causes of criminal behavior, especially in the area of fraud and embezzlement committed against organizations by trusted insiders. This pilot program could illuminate in a fact-based manner the utility of broadening the required capture of relevant information in police reporting if a correlation exists between addiction and insider threat and or the masking of other criminal activity. Moreover, if the results are compelling, an opportunity may present itself for the implementation at a national level and the revamping of existing standards related to the UCR and the NIBRS.

A. IS ADDICTION, AS A MOTIVE FOR CRIMINAL BEHAVIOR, ACCURATELY REPORTED?

Research indicates that addiction is one of the most serious and expensive public health problems in the United States. "Addiction is a disease in and of itself, characterized by compulsion, loss of control, and continued use in spite of adverse consequences."[258] Addiction is a problem that organizations need to understand and factor throughout the hiring, evaluation, and retention of personnel.

This research indicates that addiction to gambling and pain prescription medication is an increasingly common issue, and a principally unrecognized problem that is a catalyst for a previously trusted individual to commit illegal acts to maintain the semblance of a successful work ethic while sustaining the addiction. Interestingly, the illegal acts were not committed for self-enrichment or personal gain, but as a mechanism to fund the insiders' addiction.[259] The research along with numerous criminal case examples cited in this paper clearly indicates that addiction to gambling and pain prescription medication is a problem at all levels of society to include small, medium, and

[258] Brian W. Jackson, "Financial Cost of Addictive Disorders," *Journal of Addictive Disorders*, 2010, http://breining.edu/JAD10BWJ.pdf.

[259] USDOJ, "Convention Center's Former Executive Director Sentenced to 24 Months in Prison for Embezzlement"; Patrick, "Former Brentwood Official Admits Embezzling Money, Gambling It Away."

large corporations,[260] as well as non-profit organizations,[261] and at all levels of the government.[262] The author suggests that one of the defining issues in this paper is the fact that addiction is a cause or motive for a trusted insider conducting illegal behavior within organizations, and further submits that the literature suggests motives are also not being accurately recorded in police reports and documentation from victim organizations. His research from the USSS Case Studies Section in Chapter III noted that in two separate instances, the case agents did not document that addiction was tied into the motive for the insiders' illegal behavior because they did not think that the information was relative or necessary to report.

An insider threat to an organization in which fraud and embezzlement is occurring is a continuing area of concern for most entities. The statistics are staggering when a tabulation of the estimated dollar loss to businesses and organizations each year due to insider fraud and embezzlement is calculated. As the research has reflected, the estimated costs of white-collar crime in the United States may reach as much as $1 trillion annually.[263] Studies lack the exact correlation directly tied to how much of the estimated $1 trillion in annual losses caused by insiders each year to specific addiction related motives; however, from the following listed costs to society of drug and gambling addiction, the percentage is significant.

Addiction costs society as a whole an enormous amount of financial resources on an annual basis. Illicit drug use alone accounts for $181 billion in health care, productivity loss, crime and incarceration, and drug enforcement.[264] Overdosing is now

---

[260] Bruce Lambert and Valerie Cotsalas, "Bookkeeper Admits Embezzling $2.3 Million for Lottery Habit," *New York Times*, August 24, 2006, sec. New York Region, http://www.nytimes.com/2006/08/24/nyregion/24theft.html.

[261] Gary Snyder, "Nonprofit Imperative: Nonprofit Fraud: The Effects of Addictions on Charities," *Nonprofit Imperative*, April 8, 2013, http://nonprofitimperative.blogspot.com/2013/04/nonprofit-fraud-effects-of-addictions.html.

[262] Lebowitz, "Ex-FBI Agent Sentenced to Five Years in Prison."

[263] Ragatz, Fremouw, and Baker, "The Psychological Profile of White-collar Offenders Demographics, Criminal Thinking, Psychopathic Traits, and Psychopathology," 978–97.

[264] National Institute on Drug Abuse (NIDA), "Drug Abuse Costs the United States Economy Hundreds of Billions of Dollars in Increased Health Care Costs, Crime, and Lost Productivity," accessed March 20, 2014, http://www.drugabuse.gov/publications/addiction-science-molecules-to-managed-care/introduction/drug-abuse-costs-united-states-economy-hundreds-billions-dollars-in-increased-health.

the leading cause of accidental death in the United States, which accounts for more deaths than traffic fatalities or gun homicides and suicides. Fatal overdoses from opiate medications, such as oxycodone, hydrocodone, and methadone, have quadrupled since 1999 and accounted for an estimated 16,651 deaths in 2010.[265] The CDC calls pain prescription addiction an epidemic. Pain prescription drug addiction alone shows costs to society between $55-$70 million a year.[266] Numerous studies have documented the strong relationship between substance use and crime, and although causality between the two has not been conclusively established, U.S. statistics show that more than 50% of state and federal inmates used drugs in the month prior to committing the offense for which they were incarcerated, and that more than a quarter of all offenders were using drugs at the time of their offense.[267]

Gambling addiction also has a tremendous negative societal impact in this country. According to some experts, the cost of pathological and problem gambling has soared to nearly half the annual cost of drug abuse in the United States. Earl L. Grinols, an Illinois economist, has written in *Gambling in America: Costs and Benefits*, "The social costs of gambling, such as increased crime, lost work time, bankruptcies and financial hardships faced by the families of gambling addicts, have reached epidemic proportions, costing the economy as much as $54 billion annually."[268] Put differently, Grinols said, "The costs of problem and pathological gambling are comparable to the value of the lost output of an additional recession in the economy every four years."[269]

---

[265] Centers for Disease Control and Prevention, "QuickStats: Number of Deaths From Poisoning,* Drug Poisoning,† and Drug Poisoning Involving Opioid Analgesics§—United States, 1999–2010."

[266] Centers for Disease Control and Prevention, "CDC Grand Rounds: Prescription Drug Overdoses—A U.S. Epidemic," January 13, 2012, http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6101a3.htm.

[267] Kathryn E. McCollister, Michael T. French, and Hai Fang, "The Cost of Crime to Society: New Crime-Specific Estimates for Policy and Program Evaluation," *Drug and Alcohol Dependence* 108, no. 1–2 (April 1, 2010): 98–109, doi:10.1016/j.drugalcdep.2009.12.002.

[268] Earl L. Grinols, *Gambling in America: Costs and Benefits* (New York, NY: Cambridge University Press, 2004), 108–109.

[269] Mark Reutter, "Social Costs of Gambling Nearly Half That of Drug Abuse, New Book Concludes|Archives|News Bureau|University of Illinois," March 8, 2004, http://news.illinois.edu/news/04/0308grinols.html.

According to a recent report by Baylor University, "The social costs of gambling—crime costs, business and employment costs, bankruptcy, suicide, illness related to pathological gambling, social service costs, direct regulatory costs, family costs, and abused dollars—are "hidden" only to the extent that they are often misunderstood or overlooked."[270] Some of those "hidden" contributors to the costs of this type of addiction need to acknowledge a problem exists and experts in the field state, "80 to 90 percent of people in Gamblers Anonymous will tell you they did something illegal in order to get money to gamble. A lot of them do white collar crimes, fraud, credit card and employee theft."[271]

This information should command everyone's attention, including members of the homeland security community. Data clearly indicates that addiction related behaviors cause a great deal of harm for society in many tangible and intangible ways. The research and data in this thesis suggests that in spite of this certainty, clear indications are apparent that addiction as a motive for criminal behavior is not accurately being recorded as the primary indication for an individual's reason for committing the illegal activity, especially in the area of fraud and embezzlement crimes.

B. SHOULD MOTIVES MATTER FOR UNDERSTANDING FRAUD AND EMBEZZLEMENT CRIMES?

Most every organization is faced with the potential need to defend against a trusted individual on the inside as a possible threat. Fortunately, not every employee is a threat. However, as noted criminologist, Donald Cressey has implied, those individuals who have a problem or need that is "un-shareable" are potentially vulnerable to committing fraud or embezzlement within an organization. Cressey's fraud triangle theory holds that for fraud to occur, three dimensions must all be present: pressure, opportunity, and rationalization.[272] The author suggests that removing opportunity is the

[270] Robert B. Kruschwitz, "The Hidden Social Costs of Gambling," *Center for Christian Ethics, Baylor University*, 4, 2011, http://www.baylor.edu/content/services/document.php/145417.pdf.

[271] Edward Looney, *Testimony Before The National Gambling Impact Study Commission* (Atlantic City, NJ, 1998).

[272] Cressey, *Other People's Money; A Study in the Social Psychology of Embezzlement*.

best way to deconstruct the fraud triangle. Security layering and awareness of addictive signs help minimize opportunity.

One proposed strategy for law enforcement agencies is to recognize that motives and causation for committing financial crimes cases, especially in the fraud and embezzlement arena, is important to include in training to enhance understanding and awareness. Developing a more comprehensive, and in this case, accurate reporting protocol, is of equal importance.

As has been learned, most trusted insiders who commit fraud and embezzlement do not have any previous criminal record. They are in most cases perceived as stalwarts of society and law abiding citizens who many people would be proud to call neighbors and friends.[273] They are after all, "trusted" for a reason. What happens when an insider goes rouge within an organization? Many Americans are familiar with the names, Edward Snowden,[274] Robert Hannsen,[275] and Aldrich Ames[276] in the world of "trusted government insiders" who committed treasonous crimes for ideological reasons, and in the case of Hannsen and Ames, financial gain as a motivating factor. However, what about the Washington, DC tax office manager whole stole over $48 million documented in Chapter I, and the other trusted insiders discussed in this paper who committed serious financial crimes to fund an addiction?[277]

This paper has cited numerous examples of trusted insiders committing fraud and embezzlement within organizations to provide a funding mechanism for sustaining their addiction. Unfortunately, some of these trusted insiders are operating at all levels of government organizations as well. Should officials in the homeland security enterprise concern themselves with causes and motives when trusted insiders within government

[273] Cressey, *Other People's Money; A Study in the Social Psychology of Embezzlement*.

[274] Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations," *The Guardian*, June 9, 2013, sec. World news, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

[275] Gary McGraw and J. Viega, "The Ultimate Insider Threat," *Software Development* 11, no. 7 (July 2003): 49.

[276] David Johnston, "How the F.B.I. Finally, Caught Aldrich Ames," *New York Times*, January 27, 1995, sec. U.S., http://www.nytimes.com/1995/01/27/us/how-the-fbi-finally-caught-aldrich-ames.html.

[277] Southall, "17-Year Term for Official in Tax Scam."

agencies commit fraud and embezzlement when addiction is the motivating factor for committing criminal behavior? These trusted insiders have come from all levels of local, state, and federal government organizations including: city administrators,[278] county convention center managers,[279] county commissioners,[280] community health system administrators,[281] large city mayors,[282] police officers,[283] fire fighters,[284] school district employees,[285] athletic directors,[286] public university administrators,[287] state senators,[288] TSA employees,[289] FBI agents,[290] federal judges,[291] National Guard Commanders,[292] and active duty high ranking military officers,[293] all trusted within their local communities, none with previous criminal records, and all with addictions that caused them to commit crimes to finance their dependencies, which ultimately, became enslavements.

---

[278] Patrick, "Former Brentwood Official Admits Embezzling Money, Gambling It Away."

[279] USDOJ, "Convention Center's Former Executive Director Sentenced to 24 Months in Prison for Embezzlement."

[280] Collins, "Calif. Politician Pleads Guilty to Misusing Funds."

[281] Heather Abraham, "Man Accused Of Stealing $700K from WPAHS Appears in Court « CBS Pittsburgh," March 5, 2013, http://pittsburgh.cbslocal.com/2013/03/05/man-accused-of-stealing-700k-from-wpahs-appears-in-court/.

[282] Spagat, "Ex-San Diego Mayor's Gambling Wagers Top $1B."

[283] Lisa Redmond, "Lowell Police Officer Found Guilty of Illegal Gambling, Extortion—Lowell Sun Online," June 20, 2009, http://www.lowellsun.com/ci_12654723.

[284] Amy Taxin, "Ex-fire Captain Pleads Guilty in Gambling Case," *The Washington Times*, January 27, 2014, http://www.washingtontimes.com/news/2014/jan/27/ex-firefighter-pleads-guilty-to-illegal-gambling/.

[285] CBS News, "Pa. School 'Lunch Ladies' Allegedly Stole $94K to Gamble."

[286] Associated Press, "Tulsa Fires Athletic Director over Gambling Probe."

[287] Fagen, "Twisted Sister in Nun Jail."

[288] Funk, "Neb. AG: Senator Misused Campaign Cash at Casinos."

[289] Barry Leibowitz, "Report: TSA Workers Fired for Gambling at Pittsburgh Airport," *CBS News*, September 23, 2013, http://www.cbsnews.com/8301-504083_162-57603982-504083/tsa-workers-fired-or-suspended-for-gambling-ring-at-pittsburgh-airport-report-says/.

[290] Lebowitz, "Ex-FBI Agent Sentenced to Five Years in Prison."

[291] Christina Jewett, "Judge Who Faces Impeachment Took Cash, Gifts from Lawyers with Pending Cases," *ProPublica*, September 16, 2009, http://www.propublica.org/article/judge-who-faces-impeachment-took-cash-gifts-from-lawyers-with-pending-916.

[292] Associated Press, "Retired Colonel Sentenced for Embezzling Millions."

[293] Schwirtz and Somaiya, "Vice Admiral Is Suspended in Gambling Investigation."

The research has identified specific examples of trusted government insiders with access to very sensitive city, county, state, and federal information, and in several instances, individuals with access to some of this nation's most sensitive and classified material with addiction as a motivating factor for conducting their illegal activities. The nation, and most certainly the homeland security enterprise, depends on trusted government officials who have taken an oath to defend the Constitution and uphold the laws of the land. When trusted insiders operating freely within a government agency compromises their integrity to commit fraud or embezzlement due to an addiction, an undue and worrisome level of risk is placed upon the overall safety and security of this nation's cities, counties, and states, as well as potentially damaging the overall security of the United States.

The author suggests that motives should and do matter, especially in the case of trusted government officials committing fraud and embezzlement crimes due to the need to finance an addiction. This type of behavior is concerning for any organization that must contend with an insider threat. However, in reality, this conduct is potentially very damaging if government employees with access to sensitive or classified information were to become compromised and were selling government secrets, or allow access to classified programs or installations, to nefarious actors to maintain an addiction.

Trusted insiders are the linchpins of homeland security efforts at the local, state, and federal levels. The secure and delicate nature of the entire homeland security project requires a dedication to patriotism and collective protection antithetical to the self-focused nature of the addict, either to gambling or pain medication. Homeland security positions are unique in their reliance on the trusted insider. Military, law-enforcement, fire, health and safety positions are easily defined by their focus on protecting and giving to others and require trusted insiders; thus, the homeland security project in general is at risk if addiction is spreading into this arena.

Culturally, and in large measure, members of the military, law-enforcement and the first responder community selflessly symbolize by the nature of their service that they are trusted and above reproach, which in fact, may contribute to the likelihood that less scrutiny on such individuals is less rigorous.

As previously cited, Donald Cressey talked about the fraud triangle and the need for three things to be present, opportunity, pressure, and rationalization.[294] Causality and motives matter in understanding why people do what they do when it comes to criminal behavior. Law enforcement agencies, as well as state and federal legislators, need to become involved to mandate the need to change the way criminal behavior is recorded in police reports and investigations. Accurate statistics are critical when it comes to reporting crime rates and a myriad of decisions are made regarding community planning, hiring, grant award, and research based upon the UCR. However, the law enforcement community, academic researcher, or criminologist needs to know and understand what is motivating a criminal to act and conduct their illegal activity. Without accurate statistics on the causality of crime, organizations may not have a correct assessment on actual crime being committed by those insiders who have an addiction when it comes to fraud and embezzlement being committed against victim establishments. This inaccuracy is a significant gap in the literature and the available reported criminal statistics of law enforcement agencies and private sector organizations reporting fraud and embezzlement.

Calculating the addiction rates for Americans is not an exact science; however, research indicates it is a significant cost to society. These statistics are collected in many ways by researchers; however, actual police statistics on reported crimes in which causality is a discernable item is clearly an area lacking a comprehensive method for accurate accounting. The lack of accurate statistics on causality of crimes perpetrated because of an addiction is clearly an important measurement that researchers, criminologists, and homeland security officials should be able to capture. More compelling is the need for these same officials to be able to draw clear conclusions on accurate statistics surrounding causes and motives for not only fraud and embezzlement cases regarding trusted insiders, but additionally, all criminal acts reported to law enforcement. This lack of accurate reporting on causes and motives for criminal behavior indicates serious gaps in the overall crime reporting in this country, and a gap analysis including the comprehensive examination of motivating causes of crime, to include addiction is warranted.

[294] CBS News, "Pa. School 'Lunch Ladies' Allegedly Stole $94K to Gamble."

C. FUTURE RESEARCH

1. U.S. Secret Service

Initially, future research should begin with the author's own agency, the USSS. As indicated in this thesis, the USSS investigates thousands of financial crimes cases each year, and more specifically, investigates hundreds of cases under the category of fraud, embezzlement and miss-appropriation, which is most closely aligned to trusted insiders committing fraud and embezzlement within organizations.[295]

The USSS would be an excellent federal agency to conduct an in-depth case review of all its closed fraud, embezzlement, and misappropriation cases investigated in the last five years, to determine and document the trusted insiders' motive or causality of the criminal behavior. The USSS could take the lead in research as a federal agency under the DHS that has a primary mandate to investigate complex financial crimes cases. The USSS could provide a comprehensive analysis of causation and motives for trusted insiders committing fraud and embezzlement against organizations. This documentation could provide valuable data to researchers on causation of financial crimes cases. This information would also provide an opportunity to determine what if any effect addiction plays in determining insider's motive for conducting their illegal activity.

As the research indicated in the Case Studies section in Chapter III, the fact that in a relatively small sampling of four USSS field offices in which 40 closed criminal cases were reviewed indicated that in 23 out of 45 instances or 51% of the time, the trusted insiders committing the fraud and embezzlement within the victim organization had an addiction as their motivating reason for committing the crime. This review may indicate an important statistical discovery not currently being documented or analyzed in a proper format on a national scope.

The USSS has demonstrated its capabilities in the past in its unique protective mission on how it conducts in-depth research on individuals who have threatened the president of the United States and other world leaders. The USSS has an extensive

[295] Management and Organization Division, *United States Secret Service Annual Statistical Report—Fiscal Year 2013*.

research capability within its National Threat Assessment Center (NTAC).[296] The USSS should utilize this research capability to identify and track motives and causes for trusted insiders committing criminal acts within organizations and provide this data to researchers studying this phenomenon.

2. Kentucky State Police—Expansion of Causes and Motives of Crime Reporting

The KSP is the primary police records retention and reporting agency for the Commonwealth of Kentucky. KSP would be an excellent state agency to take on the role of requiring its 400 city and county law enforcement agencies to document and record the causality and motives of crimes committed in Kentucky. Kentucky is a state known for its high levels of addiction to pain prescription medication and methadone drugs.[297] Furthermore, Kentucky would be a useful state to document and study how much "addiction" plays a role in the motives or causes of individuals committing crimes.[298]

Local police departments and law enforcement agencies in Kentucky should require their officers to notate motives and causality of crime on every case when known. This information should also be in a retrievable format for statistical data collection for accurate reporting purposes. It should also be an important requirement to notate if perpetrators of any criminal offense have an addiction as a motivating factor for their criminal behavior.

3. Expansion of the FBI Uniform Crime Report and the National Incident-Based Reporting System)

The FBI and the UCR should require police agencies to report causality. This issue may need to be raised with the Department of Justice to seek requirements for causation reporting in the NIBRS under the UCR for communities to have a larger

---

[296] The National Threat Assessment Center is a primary research arm for protective intelligence assessments and functions within the Protective Intelligence Division at the USSS. www.SecretService.gov.

[297] Stephanie Smith and Nadia Kounang, "Prescription Drugs 'Orphan' Children in Eastern Kentucky," *CNN*, December 3, 2013, http://www.cnn.com/2012/12/14/health/kentucky-overdoses/index.html.

[298] "Drug Abuse 2013 Data for Kentucky."

understanding on reported motives for criminal behavior. This reporting is especially important for municipal leaders and planners, the homeland security community, and researchers to understand to assess the issue of addiction as it relates to crime accurately.

Researchers in many cases are left with general statistics for the reporting of crime and crime statistics from the UCR; they know what crimes are being reported and the amount of crime reported, but for all practical purposes, do not know the cause or motive of the criminal committing the crime. Again, motives should and do matter when it comes to understanding why the actor committing the crime being reported is doing it, especially in cases of fraud and embezzlement in which trusted insiders of organizations are committing criminal offenses.

4. Training and Awareness for Private, Non-Profit, and Government Sector Agencies on Recognizing Insider Threats to Organizations Concerning Fraud and Embezzlement

Excellent programs are available to organizations for training and education on the insider threat. A number of programs exist concerning "best practices" that organizations of all sizes should adhere to and incorporate as a part of their internal security policies and procedures regarding potential insider compromises. CERT at Carnegie Mellon University, PERSEREC, the DOD, the Defense Security Service, the Nuclear Regulatory Commission, the U.S. Secret Service Electronic Crimes Task Forces, Deloitte, Lockheed Martin, and many other government, non-profit, and private sector organizations have resources available for any size sector entity to draw from in formulating a security plan surrounding the insider threat.

People are an organization's greatest asset and most critical vulnerability. The key is recognizing that all organizations must consider the very real challenge of defending against the insider threat. Prevention, detection, and mitigation strategies are paramount for any organization to have in place before the insider attack occurs. Establishments must also take a proactive approach in understanding that addiction and addiction related behavior might be a contributing factor to insider threats posed against an organization.

D. CONCLUSION

The DOD defines risk as follows:

> Risk is the probability of loss or damage. Risk management is a function of three variables: criticality, vulnerability and threat. The first element is criticality; how important is this asset to the mission or organization? The second element is vulnerability; in what ways can the asset be compromised, exploited, damaged or destroyed? The third element is threat; who intends to exploit vulnerability, against what, and what capabilities do they possess to do so? Risk occurs at the intersection of criticality, vulnerability and threat.[299]

Insider threats to organizations will continue to occur within organizations for the foreseeable future and need to be calculated in assessing risk. All organizations are vulnerable to the trusted insider who has authority and access to operate safely within its boundaries. Law enforcement agencies will continue to investigate and prosecute these crimes, and it is important for line officers and investigators to identify, document, and report possible causes and motives for the insider's illegal activity, especially if addiction is a primary cause or motive.

A problematic issue with those individuals who have an addiction, and are conducting fraud and embezzlement within organizations, is they are committing their crimes to finance the addiction, and generally not to enrich themselves. This viewpoint is challenging in the sense that an addict will sacrifice anything to continue the addiction, which potentially places the trusted insiders in a situation in which they may compromise the entire organization. In some instances, this breach of trust could lead to compromising national security secrets if a nefarious outside government or organization was able to leverage the insiders to provide information for payments to continue their addiction.

In this thesis, the author has endeavored to capitalize on his extensive experience in investigating and managing complex financial crimes cases, especially in the area of fraud and embezzlement committed by "trusted insiders" against private, non-profit, and

[299] *Final Report of the Insider Threat Integrated Process Team, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence),* 7–8.

public sector organizations for well over a quarter century. He has identified a threat to homeland security by identifying the larger threat to all organizations from trusted insiders committing these crimes due to addiction as a primary cause and motivating factor for their illegal behavior. He has highlighted the need for law-enforcement agencies to report causes and motives in their criminal reporting, and for a more complete analysis of trusted insiders conducting financial crimes against organizations. Additionally, he has noted the fact that the UCR and the NIBRS do not require capturing causation and motive in their reporting of Schedule 2 crimes, which encompass fraud and embezzlement cases most closely connected with trusted insiders committing financial crimes against organizations while making the case that this information should be captured. He has further strived to make a compelling argument for the need for law enforcement agencies to be required to report motives and causes of all criminal offenses in the UCR and NIBRS. The increased reporting of causation or motives will allow for a more accurate picture of addictive related behaviors and allow for an increased knowledge base of the threat that insiders may pose to an organization's vulnerabilities due to an addiction.

The ultimate goal of this thesis was to answer the author's research question and he is able to definitively conclude, "trusted insiders" are committing fraud and embezzlement within all organizational sectors, and a connection to addiction does exist, as a motivating factor for their illegal behavior.

LIST OF REFERENCES

Abbott, Max W., Brian G. McKenna, and Lynne C. Giles. "Gambling and Problem Gambling Among Recently Sentenced Male Prisoners in Four New Zealand Prisons." *Journal of Gambling Studies* 21, no. 4 (Winter 2005): 537–58. doi:10.1007/s10899-005-5562-6.

Abraham, Heather. "Man Accused Of Stealing $700K from WPAHS Appears in Court « CBS Pittsburgh." March 5, 2013. http://pittsburgh.cbslocal.com/2013/03/05/man-accused-of-stealing-700k-from-wpahs-appears-in-court/.

Achenbach, Joel. "Philip Seymour Hoffman's Death Points to Broader Opioid Drug Epidemic." *The Washington Post*, February 8, 2014, sec. National. http://www.washingtonpost.com/national/health-science/philip-seymour-hoffman-heroin-death-points-to-broader-opioid-drug-epidemic/2014/02/07/42dbbc5a-8e61-11e3-b46a-5a3d0d2130da_story.html.

Albanese, Jay. "White Collar Crimes and Casino Gambling: Looking for Empirical Links to Forgery, Embezzlement, and Fraud." *Crime, Law & Social Change* 49, no. 5 (June 2008): 333–47. doi:10.1007/s10611-008-9113-9.

Albrecht, Steve W., Conan C. Albrecht, Chad O. Albrecht, and Mark F. Zimbleman. *Fraud Examination*. Stamford, CT: Cengage Learning, 2008.

American Gaming Association. "How Many Pathological Gamblers Are There?" Accessed February 1, 2014. http://www.americangaming.org/industry-resources/faq/how-many-pathological-gamblers-are-there.

Anderson, Robert H. "Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems: Results of a Three-Day Workshop. RAND CF-151-OSD." *RAND Corporation*, 1999. http://citeseer.uark.edu:8080/citeseerx/showciting;jsessionid=66C66F7E33D77E8C7241750AD878F092?cid=252875.

Anderson, Robert H., Thomas Bozek, Tom Longstaff, Wayne Meitzler, Michael Skroch, and Ken Van Wyk. "Research on Mitigating the Insider Threat to Information Systems—#2 Proceedings of a Workshop Held August, 2000." RAND Corporation, 2000. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA386077.

Arthur, Jennifer N., Robert J. Williams, and Yale D. Belanger. "The Relationship Between Legal Gambling and Crime in Alberta1." *Canadian Journal of Criminology & Criminal Justice* 56, no. 1 (January 2014): 49–84. doi:10.3138/cjccj.2012.E51.

Ashley Larry L., and Karmen K. Boehlke. “Pathological Gambling: A General Overview.” *Journal of Psychoactive Drugs* 44, no. 1 (March 2012): 27–37. doi:http://dx.doi.org.libproxy.nps.edu/10.1080/02791072.2012.662078.

Associated Press. “Retired Colonel Sentenced for Embezzling Millions.” *KTVK Azfamily.com*, March 28, 2012. http://www.azfamily.com/news/Retired-colonel-sentenced-for-embezzling-millions-144694985.html.

———. “Tulsa Fires Athletic Director over Gambling Probe.” December 4, 2012. http://bigstory.ap.org/article/tulsa-fires-athletic-director-over-gambling-probe.

Associated Press in Washington. “U.S. Nuclear Commander Tim Giardina Fired Amid Gambling Investigation.” *The Guardian*, October 9, 2013. http://www.the guardian.com/world/2013/oct/09/us-nuclear-commander-tim-giardina-fired-amid-gambling-investigation.

Association of Certified Fraud Examiners. “2012 Report to the Nations—Key Findings and Highlights.” Accessed January 17, 2014. http://www.acfe.com/rttn-highlights.aspx.

Band, Steven, Dawn Cappelli, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, and Randall F. Trzeciak. “Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis|SEI Digital Library.” *Software Engineering Institute, Carnegie Mellon University*, 2006. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8163#.

Barnett, Cynthia. “The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data.” *U.S. Department of Justice Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Division*. Accessed March 14, 2014. http://www.fbi.gov/stats-services/about-us/cjis/ucr/nibrs/nibrs_wcc.pdf.

Birnbaum, Howard G., Alan G. White, Matt Schiller, Tracy Waldman, Jody M. Cleveland, and Carl L. Roland. “Societal Costs of Prescription Opioid Abuse, Dependence, and Misuse in the United States.” *Pain Medicine* 12, no. 4 (2011): 657. doi:10.1111/j.1526-4637.2011.01075.x.

Bishop, Matt, and Carrie Gates. “Defining the Insider Threat.” Presented at the Fourth Annual Cyber Security and Information Intelligence Research Workshop. Davis, CA: ACM Press, 2008. doi:10.1145/1413140.1413158.

Bishop, Matt, Sophie Engle, Deborah A. Frincke, Carrie Gates, Frank L. Greitzer, Sean Peisert, and Sean Whalen. “A Risk Management Approach to the ‘Insider Threat.’” In *Insider Threats in Cyber Security*, edited by Christian W. Probst et al. Advances in Information Security 49. New York: Springer U.S., 2010. http://link.springer.com/chapter/10.1007/978-1-4419-7133-3_6.

Blaszczynski, Alex. “Criminal Offences in Pathological Gamblers.” *Psychiatry, Psychology and Law* 1, no. 2 (1994): 129–38. doi:10.1080/13218719409524836.

Blaszczynski, Alex, and Eimear Farrell. “A Case Series of 44 Completed Gambling-related Suicides.” *Journal of Gambling Studies* 14, no. 2 (1999): 93–109.

Blaszczynski, Alex P., and Neil McConaghy. “Criminal Offenses in Gamblers Anonymous and Hospital Treated Pathological Gamblers.” *Journal of Gambling Studies* 10, no. 2 (June 1, 1994): 99–127. doi:10.1007/BF02109935.

Blaszczynski, Alex, and Derrick Silove. “Pathological Gambling: Forensic Issues.” *Australian and New Zealand Journal of Psychiatry* 30, no. 3 (June 1, 1996): 358–69. doi:10.3109/00048679609065000.

Blaszczynski, Alex, Neil McConaghy, and Anna Frankova. “Crime, Antisocial Personality and Pathological Gambling.” *Journal of Gambling Behavior* 5, no. 2 (June 1, 1989): 137–52. doi:10.1007/BF01019760.

Blodgett, Nancy. “Stealing Your Practice Blind.” *ABA Journal* 73, no. 8 (August 1, 1987): 78–82.

Brackney, Richard, and Robert Andersen. “Understanding the Insider Threat: Proceedings of a March 2004 Workshop R. Understanding the Insider Threat: Proceedings of a March 2004 Workshop.” In *Proceedings of a March 2004 Workshop*. Santa Monica, CA: RAND Corporation, 2004. http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2005/RAND_CF196.pdf.

Brown, Iain (R I F). “Pathological Gambling and Associated Patterns of Crime: Comparisons with Alcohol and Other Drug Addictions.” *Journal of Gambling Behavior* 3, no. 2 (June 1, 1987): 98–114. doi:10.1007/BF01043449.

Cappelli, Dawn M., Andrew Moore, and Randall Trzeciak. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Boston, MA: Addison-Wesley Professional, 2012.

Cappelli, Dawn M., Andrew P. Moore, Randall F. Trzeciak, and Timothy J. Shimeall. “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, Dawn, Andrew P. Moore, and Timothy J. Shimeall. *Common Sense Guide to Prevention and Detection of Insider Threats*. Pittsburgh, PA: Carnegie Mellon University Cy Lab, July 2006.

Cappelli, Dawn, Andrew P. Moore, Marissa R. Randazzo, Michelle Keeney, and Eileen Kowalski. “Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector.” *U.S. Secret Service and CERT Coordination Center/Software Engineering Institute*, 2004. http://www.cert.org/archive/pdf/bankfin040820.pdf.

CBS News. “Pa. School ‘Lunch Ladies’ Allegedly Stole $94K to Gamble.” February 27, 2013. http://www.cbsnews.com/8301-504083_162-57571435-504083/school-lunch-ladies-accused-of-stealing-$94k-to-gamble/.

Centers for Disease Control and Prevention. “CDC Grand Rounds: Prescription Drug Overdoses—A U.S. Epidemic.” January 13, 2012. http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6101a3.htm.

———. “CDC—Prescription Drug Overdose Prevention. FY 2015 President’s Budget Request|$15.6 Million.” Accessed March 17, 2014. http://www.cdc.gov/injury/pdfs/budget/NCIPC_PDO_FY2015-a.pdf.

———. “FASTSTATS—Homicide.” 2010. http://www.cdc.gov/nchs/fastats/homicide.htm.

———. “QuickStats: Number of Deaths From Poisoning,* Drug Poisoning,† and Drug Poisoning Involving Opioid Analgesics§—United States, 1999–2010.” March 29, 2013. http://www.cdc.gov/mmwr/preview/mmwrhtml/mm6212a7.htm.

CIA, Freedom of Information Act Electronic Reading Room. “Project Slammer Interim Report (U).” Director of Central Intelligence, 1992. http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000218679.pdf.

City Town Info. “San Diego, California—City Information, Fast Facts, Schools, Colleges, and More.” Accessed May 27, 2014. http://www.citytowninfo.com/places/california/san-diego.

Clay, Nolan. “Ex-FBI Agent in Oklahoma Gets Six Months in Prison for Embezzling.” *NewsOK.com*. Accessed March 14, 2014. http://newsok.com/ex-fbi-agent-in-oklahoma-gets-six-months-in-prison-for-embezzling/article/3738422.

Cole, Eric, and Sandra Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft: Protecting the Enterprise from Sabotage, Spying, and Theft*. Maryland Heights, MO: Syngress, 2005.

Collins, Terry. “Calif. Politician Pleads Guilty to Misusing Funds.” *Associated Press*. Accessed September 30, 2013. http://bigstory.ap.org/article/ex-n-calif-politician-pleads-guilty-felonies.

Colwill, Carl. “Human Factors in Information Security: The Insider Threat—Who Can You Trust These Days?.” *Information Security Technical Report* 14, no. 4 (November 2009): 186–96. doi:10.1016/j.istr.2010.04.004.

Cressey, Donald R. “The Criminal Violation of Financial Trust.” *American Sociological Review* 15, no. 6 (December 1, 1950): 738–743. doi:10.2307/2086606.

———. *Other People’s Money; A Study in the Social Psychology of Embezzlement*. Montclair, NJ: Patterson Smith, 1973.

CSO Magazine et al. “2013 State of Cybercrime Survey.” *PwC*, 2013. http://www.pwc.com/us/en/press-releases/2013/cybercrime-threats-continue.jhtml.

Cummings, Adam, Todd Lewellen, David McIntire, Andrew P. Moore, and Randall F. Trzeciak. “Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector.” *Software Engineering Institute, Carnegie Mellon University and CyLab*, 2012. http://repository.cmu.edu/cgi/viewcontent.cgi?article=1688&context=sei.

Dale, Maryclaire. “Pa. Church’s Ex-CFO Gets 2–7 Years in $900k Theft.” Accessed September 30, 2013. http://bigstory.ap.org/article/pa-churchs-ex-cfo-gets-2-7-years-900k-theft.

Davis, Louis M., Daniela Golinelli, Robin Beckman, Sarah K. Cotton, Robert H. Anderson, Anil Bamezai, Christopher R. Corey, Megan Zander-Cotugno, John L. Adams, Roald Euller, and Paul Steinberg. “The National Computer Security Survey (NCSS): Final Methodology–RAND_TR544.pdf.” *The RAND Corporation*, 2008. http://www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR544.pdf.

De Avila, Joseph. “Financial Scandal Strains Community in Winsted, Conn.” October 16, 2013. http://online.wsj.com/news/articles/SB10001424052702304561004579137440704100238?KEYWORDS=+embezzlement+and+gambling+.

Delfabbro, Paul. “Problem and Pathological Gambling: A Conceptual Review.” *Journal of Gambling Business & Economics* 7, no. 3 (September 2013): 35–53.

Dorrell, Darrell D., and Gregory A. Gadawski. “Investigating Embezzlement: Three Don’ts.” *Value Examiner*, August 7, 2012.

el-Guebaly, Nady, Tanya Mudry, Joseph Zohar, Hermano Tavares, and Marc N. Potenza. “Compulsive Features in Behavioral Addictions: The Case of Pathological Gambling.” *Addiction* 107, no. 10 (October 2012): 1726–1734. doi:10.1111/j.1360-0443.2011.03546.x.

Fagen, Cynthia R. “Twisted Sister in Nun Jail.” *New York Post*, November 13, 2011. http://www.nypost.com/p/news/local/twisted_sister_in_nun_jail_gZfMQUNa031kduaErl9htM.

FED Up Coalition Steering Committee. “Zohydro Letter with Signatures Final.” February 26, 2014. http://www.citizen.org/documents/2185.pdf.

Federal Bureau of Investigation. “Offenses in Uniform Crime Reporting—Crime in the United States 2004.” Accessed March 7, 2014. https://www2.fbi.gov/ucr/cius_04/appendices/appendix_02.html.

———. Criminal Justice Information Services Division. “2012 National Incident-Based Reporting System.” Accessed March 17, 2014. http://www.fbi.gov/about-us/cjis/ucr/nibrs/2012/nibrs-2012-home.

Final Report of the Insider Threat Integrated Process Team, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). Washington, DC: Department of Defense, April 24, 2000.

Forcier, Krista. “Project Slammer: Why Spies Are Spying.” *National Security Training Institute*, November 12, 2013. https://www.nstii.com/content/project-slammer-why-spies-are-spying.

Frances, Richard J., Sheldon I. Miller, and Avram H. Mack. *Clinical Textbook of Addictive Disorders*. New York: Guilford Press, 2005.

———. *Clinical Textbook of Addictive Disorders, Third Edition*. Illustrated. New York: Guilford Press, 2011. http://books.google.com/books/about/Clinical_Textbook_of_Addictive_Disorders.html?id=JJk52UeE6hYC.

Funk, Josh. “Neb. AG: Senator Misused Campaign Cash at Casinos.” Accessed September 30, 2013. http://bigstory.ap.org/article/neb-ag-senator-misused-campaign-cash-casinos.

Gazel, Ricardo C., Dan S. Rickman, and William N. Thompson. “Casino Gambling and Crime: A Panel Study of Wisconsin Counties.” *Managerial & Decision Economics* 22, no. 1–3 (January 2001): 65–75.

Geary, Jason. “Dentist Gets Probation in Prescription Drug Case|TheLedger.com.” July 20, 2013. http://www.theledger.com/article/20130720/NEWS/130729923?p=1&tc=pg.

Gelles, Michael G., David L. Brant, and Brian Geffert. “Building a Secure Workforce: Guard Against Insider Threat.” *Deloitte Federal Government Services*, 2008. https://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_ps_insiderthreat_100108.pdf.

Green, Gary S. “White-Collar Crime and the Study of Embezzlement.” *Annals of the American Academy of Political and Social Science* 525 (January 1, 1993): 95–106.

Greenwald, Glenn. “Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations|World News.” *The Guardian*, June 9, 2013. http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. “Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations.” *The Guardian*, June 9, 2013, sec. World news. http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Greitzer, Frank L., Lars J. Kangas, Christine F. Noonan, Angela C. Dalton, and Ryan E. Hohimer. “Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats.” In *2012 45th Hawaii International Conference on System Science (HICSS)*, 2012. doi:10.1109/HICSS.2012.309.

Greitzer, Frank, Andrew P. Moore, Dawn M. Cappelli, Dee H. Andrews, Lynn A. Carroll, and Thomas D. Hull. “Combating the Insider Cyber Threat.” *IEEE Security Privacy* 6, no. 1 (January/February 2008): 61–64. doi:10.1109/MSP.2008.8.

Griffin, Joel. “Major Embezzlement Cases on the Rise.” *SecurityInfoWatch.com*, May 20, 2013. http://www.securityinfowatch.com/article/10946366/marquet-international-report-finds-major-embezzlement-cases-increased-in-2012.

Griffin, Marty. “Dozens of TSA Employees Fired, Suspended for Illegal Gambling Ring at Pittsburgh Int’l Airport.” *CBS Pittsburgh*. September 19, 2013. http://pittsburgh.cbslocal.com/2013/09/19/dozens-of-tsa-employees-fired-suspended-for-illegal-gambling-ring-at-pittsburgh-intl-airport/.

Grinols, Earl L. *Gambling in America: Costs and Benefits*. New York, NY: Cambridge University Press, 2004.

Hanley, Michael, Tyler Dean, Will Schroeder, Matt Houy, Randall F. Trzeciak, and Joji Montelibano, *An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, February 2011.

Hansen, R. N., G. Oster, J. Edelsberg, G. E. Woody, and S. D. Sullivan. “Economic Costs of Nonmedical Use of Prescription Opioids.” *The Clinical Journal of Pain* 27, no. 3 (2011): 194. doi:10.1097/AJP.0b013e3181ff04ca.

Herbig, Katherine L., and Martin F. Wiskoff. “Espionage Against the United States by American Citizens 1947–2001, PERSEREC Technical Report 02–5.” *Defense Personnel Security Research Center, Monterey, CA*, July 2002. http://www.fas.org/sgp/library/spies.pdf.

HubPages. “Prescription Drugs Elevate Crime Rate.” Accessed March 6, 2014. http://narconongeorgia.hubpages.com/hub/Prescription-Drugs-Elevate-Crime-Rate.

Hunker, Jeffrey, and Christian W. Probst. “Insiders and Insider Threats—An Overview of Definitions and Mitigation Techniques.” *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 2, no. 1 (2011): 6–7.

“Insider Fraud Is Common and Often Flies Under Corporate Radar.” *Security: Solutions for Enterprise Security Leaders* 48, no. 11 (November 2011): 12–15.

Jackson, Brian W. “Financial Cost of Addictive Disorders.” *Journal of Addictive Disorders*, 2010. http://breining.edu/JAD10BWJ.pdf.

Jewett, Christina. “Judge Who Faces Impeachment Took Cash, Gifts from Lawyers with Pending Cases.” *ProPublica*, September 16, 2009. http://www.propublica.org/article/judge-who-faces-impeachment-took-cash-gifts-from-lawyers-with-pending-916.

Johnston, David. “How the F.B.I. Finally, Caught Aldrich Ames.” *The New York Times*, January 27, 1995, sec. U.S. http://www.nytimes.com/1995/01/27/us/how-the-fbi-finally-caught-aldrich-ames.html.

Jones, Andy. “Catching the Malicious Insider.” *Information Security Technical Report* 13, no. 4 (November 2008): 220–24. doi:10.1016/j.istr.2008.10.008.

Karni, Annie. “Real Mayors of New Jersey.” *New York Post*, June 24, 2012. http://nypost.com/2012/06/24/real-mayors-of-new-jersey/.

Keating, Dan. “Tax Suspect’s Guidance on Software Left D.C. at Risk.” *The Washington Post*, June sec. Metro, 10, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/06/09/AR2008060902879_2.html.

Keeney, Michelle, Eileen Kowalski, Dawn Cappelli, Andrew Moore, Timothy Shimeall, and Stephanie Rogers. *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*. Pittsburgh, PA: U.S. Secret Service and CERT Coordination Center, Carnegie Mellon Software Engineering Institute, 2005.

Kentucky Legislature. “Kentucky Revised Statutes.” 2013. http://www.lrc.ky.gov/statutes/index.aspx.

Kentucky State Police. “Commonwealth of Kentucky 2012 Crime Report.” 2013. http://www.kentuckystatepolice.org/pdf/cik_2012.pdf.

Kindt, John Warren. “The Costs of Addicted Gamblers: Should the States Initiate Mega-Lawsuits Similar to the Tobacco Cases?.” *Managerial and Decision Economics* 22, no. 1/3 (January 1, 2001): 22.

Kowalski, Eileen F., Dawn Cappelli, Bradford J. Willke, and Andrew P. Moore. “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/insiderthreat_gov2008.pdf.

Kowalski, Eileen, F. Dawn M. Cappelli, and Andrew P. Moore. “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/insiderthreat_it2008.pdf.

Kramer, Lisa A., Richards J. Heuer, Jr., and Kent S. Crawford. “Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage.” Defense Personnel Security Research Center, *Federation of American Scientists*, May 2005. http://www.fas.org/sgp/othergov/dod/insider.pdf.

Kruschwitz, Robert B. “The Hidden Social Costs of Gambling.” *Center for Christian Ethics, Baylor University*, 2011. http://www.baylor.edu/content/services/document.php/145417.pdf.

Ladouceur, Robert, Jean-Marie Boisvert, Michel Pepin, Michel I. Loranger, and Caroline Sylvain. “Social Cost of Pathological Gambling.” *Journal of Gambling Studies* 10, no. 4 (1994): 399–409.

Lambert, Bruce, and Valerie Cotsalas. “Bookkeeper Admits Embezzling $2.3 Million for Lottery Habit.” *The New York Times*, August 24, 2006, sec. New York Region. http://www.nytimes.com/2006/08/24/nyregion/24theft.html.

Lebowitz, Larry. “Ex-FBI Agent Sentenced to Five Years in Prison.” *Sun Sentinel*, November 24, 1998. http://articles.sun-sentinel.com/1998-11-24/news/9811240441_1_sentence-sullivan-s-role-gambling-debts.

Ledgerwood, David M., Jeremiah Weinstsock, Benjamin J. Morasco, and Nancy M. Petry. “Clinical Features and Treatment Prognosis of Pathological Gamblers with and Without Recent Gambling-Related Illegal Behavior.” *Journal of the American Academy of Psychiatry and the Law Online* 35, no. 3 (September 1, 2007): 294–301.

Leibowitz, Barry. “Report: TSA Workers Fired for Gambling at Pittsburgh Airport.” *CBS News*, September 23, 2013. http://www.cbsnews.com/8301-504083_162-57603982-504083/tsa-workers-fired-or-suspended-for-gambling-ring-at-pittsburgh-airport-report-says/.

Lesieur, Henry R. “Gambling, Pathological Gambling and Crime.” In *Handbook on Pathological Gambling*, edited by Thomas Galski, 89–110. Springfield, IL: Charles C. Thomas, 1987.

———. *The Chase: Career of the Compulsive Gambler*, vol. xxi. Oxford, England: Anchor, 1984.

Lesieur, Henry R., and Robert L. Custer. "Pathological Gambling: Roots, Phases, and Treatment." *American Academy of Political and Social Science* 474, no. 1 (July 1, 1984): 146–56.

Liewer, Steve. "StratCom Deputy Chief Fired as Nation's No. 2 Nuclear Commander." *Omaha.com*, October 10, 2013. http://www.omaha.com/apps/pbcs.dll/article?AID=/20131009/NEWS/131008617.

Looney, Edward. *Testimony Before The National Gambling Impact Study Commission*. Atlantic City, NJ, 1998.

Management and Organization Division, *United States Secret Service Annual Statistical Report—Fiscal Year 2013*. Washington, DC: Department of Homeland Security, 2013.

Manchikanti, Laxmaiah. "Prescription Drug Abuse: What Is Being Done to Address This New Drug epidemic? Testimony before the Subcommittee on Criminal Justice, Drug Policy and Human Resources." *Pain Physician* 9, no. 4 (2006): 287.

Marketwire. "2011 CyberSecurity Watch Survey: Organizations Need More Skilled Cyber Professionals to Stay Secure." Accessed February 10, 2014. http://www.marketwired.com/press-release/2011-CyberSecurity-Watch-Survey-Organizations-Need-More-Skilled-Cyber-Professionals-1387863.htm.

Marquet International, Ltd. "The 2012 Marquet Report on Embezzlement: A White Collar Fraud Study of Major Embezzlement Cases Active in the U.S. in 2012." May 14, 2013. http://www.marquetinternational.com/pdf/the_2012_marquet_report_on_embezzlement.pdf.

McCollister, Kathryn E., Michael T. French, and Hai Fang. "The Cost of Crime to Society: New Crime-Specific Estimates for Policy and Program Evaluation." *Drug and Alcohol Dependence* 108, no. 1–2 (April 1, 2010): 98–109. doi:10.1016/j.drugalcdep.2009.12.002.

McGraw, Gary, and J. Viega. "The Ultimate Insider Threat." *Software Development* 11, no. 7 (July 2003): 49.

Merriam Webster. "Embezzle." Accessed January 20, 2014. http://www.merriam-webster.com/dictionary/embezzle.

———. "Fraud." Accessed January 20, 2014. http://www.merriam-webster.com/dictionary/fraud?show=0&t=1390187912.

Metcalfe, John. “Rita Crundwell vs. Harriette Walters: Who Embezzled Better?.” *The Atlantic Cities*, April 18, 2012. http://www.theatlanticcities.com/neighborhoods/2012/04/rita-crundwell-vs-harriette-walters-who-embezzled-best/1797/.

Meyer, Gerhard, and Michael A. Stadler. “Criminal Behavior Associated with Pathological Gambling.” *Journal of Gambling Studies* 15, no. 1 (March 1, 1999): 29–43. doi:10.1023/A:1023015028901.

Meyers, Carol, Sarah Powers, and Daniel Faissol. “Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches.” *Lawrence Livermore National Laboratory*, April 2009. https://e-reports-ext.llnl.gov/pdf/379498.pdf.

Moore, Andrew, Dawn Capppelli, Thomas C. Caron, Eric D. Shaw, Derrick Spooner, and Randall F. Trzeciak. “A Preliminary Model of Insider Theft of Intellectual Property.” *Software Engineering Institute*, June 1, 2011. http://repository.cmu.edu/sei/726.

National Atlas of the United States. “Summary of the Uniform Crime Reporting Program.” Accessed March 7, 2014. http://nationalatlas.gov/articles/people/a_crimereport.html#two.

National Gambling Impact Study Commission, Final Report. Washington, DC: Impact Study Commission, June 1999.

National Institute on Drug Abuse (NIDA). “Drug Abuse Costs the United States Economy Hundreds of Billions of Dollars in Increased Health Care Costs, Crime, and Lost Productivity.” Accessed March 20, 2014. http://www.drugabuse.gov/publications/addiction-science-molecules-to-managed-care/introduction/drug-abuse-costs-united-states-economy-hundreds-billions-dollars-in-increased-health.

National Research Council. *Pathological Gambling: A Critical Review. Committee on the Social and Economic Impact of Pathological Gambling, Committee on Law and Justice, Commission on Behavioral and Social Sciences and Education*. Washington, DC: National Academy Press, 1999.

Noonan, Thomas, and Edmund G. Archuleta. “The National Infrastructure Advisory Council’s Final Report and Recommendations on–The Insider Threat to Critical Infrastructures.” *Department of Homeland Security*, April 8, 2008, 11. http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.

Overman, Stephenie. “Addiction: Odds Are Gamblers Cost Companies.” *HRMagazine* 35, no. 4 (April 1990): 50.

Patrick, Robert. “Former Brentwood Official Admits Embezzling Money, Gambling It Away.” *Stltoday.com*, June 29, 2011. http://www.stltoday.com/news/local/crime-and-courts/former-brentwood-official-admits-embezzling-money-gambling-it-away/article_210f8282-a269-11e0-84b8-0019bb30f31a.html.

Patzakis, John. “IRBestPractices.pdf.” *Guidance Software*, September 2003. http://faculty.usfsp.edu/gkearns/Articles_Fraud/IRBestPractices.pdf.

Paul, Robert J., and James B. Townsend. “Managing Workplace Gambling—Some Cautions and Recommendations.” *Employee Responsibilities and Rights Journal* 11, no. 3 (September 1998): 171.

Paulozzi, Leonard J. “Prescription Drug Overdoses: A Review.” *Journal of Safety Research* 43, no. 4 (September 2012): 283–89. doi:10.1016/j.jsr.2012.08.009.

Pavlo Walter. “Fmr Dixon, IL Comptroller, Rita Crundwell, Sentenced to 19 1/2 Years in Prison.” *Forbes*, February 14, 2013. http://www.forbes.com/sites/walterpavlo/2013/02/14/fmr-dixon-il-comptroller-rita-crundwell-sentenced-to-19-12-years-in-prison/.

Peterson, Virgil W. “Why Honest People Steal.” *Journal of Criminal Law and Criminology* 38, no. 2, art. 2 (1947): 94–103.

Pfleeger, Shari Lawrence, and Salvatore Stolfo. “Addressing the Insider Threat.” *IEEE Security & Privacy* 7 (2009). http://academiccommons.columbia.edu/catalog/ac:125619.p.10.

Phillips, Denise. “Gambling: The Hidden Addiction.” *Behavioral Health Management* 25, no. 5 (October 2005): 32–37.

Probst, Christian W., Jeffrey Hunker, Dieter Gollmann, and Matt Bishop. “Aspects of Insider Threats.” In *Insider Threats in Cyber Security*, edited by Christian W. Probst et al., Advances in Information Security 49, *Springer U.S.*, 2010. http://link.springer.com/chapter/10.1007/978-1-4419-7133-3_1.

Ragatz, Laurie L., William Fremouw, and Edward Baker. “The Psychological Profile of White-collar Offenders Demographics, Criminal Thinking, Psychopathic Traits, and Psychopathology.” *Criminal Justice and Behavior* 39, no. 7 (July 1, 2012): 978–97. doi:10.1177/0093854812437846.

Randazzo, Marissa R., Michelle Keeney, Eileen Kowalski, Dawn Cappelli, and Andrew P. Moore. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. Pittsburg, PA: Software Engineering Institute, June 2005.

Redmond, Lisa. “Lowell Police Officer Found Guilty of Illegal Gambling, Extortion—Lowell Sun Online.” June 20, 2009. http://www.lowellsun.com/ci_12654723.

Reese, Shawn. *The U.S. Secret Service: An Examination and Analysis of Its Evolving Missions*, Report for Congress. CRS Report RL34603. Washington, DC: Congressional Research Service, January 8, 2013. http://www.fas.org/sgp/crs/homesec/RL34603.pdf.

Reilly, M. B. "Surprising Survey: Most Small Businesses Remain Silent Rather Than Report Employee Theft." February 18, 2014. http://phys.org/news/2014-02-survey-small-businesses-silent-employee.html.

Reutter, Mark. "Social Costs of Gambling Nearly Half That of Drug Abuse, New Book Concludes|Archives|News Bureau|University of Illinois." March 8, 2004. http://news.illinois.edu/news/04/0308grinols.html.

Richards, Kathleen. "RSA 2013: FBI Offers Lessons Learned on Insider Threat Detection." *Search Security*, March 5, 2013. http://searchsecurity.techtarget.com/news/2240179082/RSA-2013-FBI-offers-lessons-learned-on-insider-threat-detection.

Richardson, Robert. "CSI FBI Survey 2003—Fbiraportti.pdf." *yle*, 2003. http://www.yle.fi/mot/kj040524/fbiraportti.pdf.

———. "The 12th Annual Computer Crime and Security Survey." *Computer Security Institute*, 2007. http://gocsi.com/sites/default/files/uploads/2007_CSI_Survey_full-color_no%20marks.indd_.pdf.

Rosenthal, Richard J., and Henry R. Lesieur. "Pathological Gambling and Criminal Behavior." In *Explorations in Criminal Psychopathology: Clinical Syndromes with Forensic Implications*, edited by Louis B. Schlesinger, 149–169. Springfield, IL: Charles C. Thomas Publisher, 1996.

Savitz, Eric, and Kevin Cunningham. "Insider Attacks Are Impacting Your Bottom Line." *Forbes.com*, December 23, 2011.

Schriffen, John. "Ex-Comptroller Faces Jail in $53M Scam." *ABC News*, November 15, 2012. http://abcnews.go.com/Business/comptroller-rita-crundwell-pleads-guilty-stealing-53m-illinois/story?id=17723699.

Schwirtz, Michael, and Ravi Somaiya. "Vice Admiral Is Suspended in Gambling Investigation." *The New York Times*, September 28, 2013. http://www.nytimes.com/2013/09/29/us/vice-admiral-is-suspended-in-gambling-investigation.html?_r=0.

Shaffer, Howard J., Matthew N. Hall, and Joni Vander Bilt. "Estimating the Prevalence of Disordered Gambling Behavior in the United States and Canada: A Research Synthesis." *American Journal of Public Health* 89, no. 9 (September 1999): 1369–75.

Shaw, Eric D. "'Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders,' Report 2—Case Studies. Technical Report 05–05." *Defense Personnel Security Research Center, Monterey, CA*, 2005. http://www.dhra.mil/perserec/reports.html.

Shaw, Eric D., and Lynn F. Fischer. "Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations." Defense Personnel Security Research Center, Monterey, CA, September 2005. http://www.dhra.mil/perserec/reports/tr05-13.pdf.

Silowash, George, Dawn M. Cappelli, Andrew P. Moore, Randall F. Trzeciak, Timothy Shimeall, and Lori Flynn. "Common Sense Guide to Mitigating Insider Threats, 4th Edition." *Software Engineering Institute*, December 1, 2012. http://repository.cmu.edu/sei/677.

Smith, Bryan. "Rita Crundwell and the Dixon Embezzlement." *Chicago Magazine*, December 2012, cagomag.com/Chicago-Magazine/December-2012/Rita-Crundwell-and-the-Dixon-Embezzlement/.

Smith, G., H. Wynne, and T. Hartnagel. *Examining Police Records to Assess Gambling Impacts: A Study of Gambling-related Crime in the City of Edmonton*. Edmonton, Alberta, Canada: The Alberta Gaming Research Institute, 2003.

Smith, Stephanie, and Nadia Kounang. "Prescription Drugs 'Orphan' Children in Eastern Kentucky." *CNN*, December 3, 2013. http://www.cnn.com/2012/12/14/health/kentucky-overdoses/index.html.

Snyder, Gary. "Nonprofit Imperative: Nonprofit Fraud: The Effects of Addictions on Charities." *Nonprofit Imperative*, April 8, 2013. http://nonprofitimperative.blogspot.com/2013/04/nonprofit-fraud-effects-of-addictions.html.

Southall, Ashley. "17-Year Term for Official in Tax Scam." *The New York Times*, July 1, 2009, sec. U.S. http://www.nytimes.com/2009/07/01/us/01embezzle.html.

Spagat, Elliot. "Ex-San Diego Mayor's Gambling Wagers Top $1B." Accessed September 30, 2013. http://bigstory.ap.org/article/ex-san-diego-mayor-faces-money-laundering-charge.

Steele, Sean. "VA Breach Shows Growing Insider Threats." *Network World* 23, no. 24 (June 19, 2006): 43–43.

Taxin, Amy. "Ex-fire Captain Pleads Guilty in Gambling Case." *The Washington Times*, January 27, 2014. http://www.washingtontimes.com/news/2014/jan/27/ex-firefighter-pleads-guilty-to-illegal-gambling/.

Thompson, Carolyn. “James Bagarozzo, Buffalo Parking Meter Mechanic, Jailed In $210K Scam.” *Huffington Post*, August 17, 2013. http://www.huffingtonpost.com/2013/08/17/theft-of-840k-coins-sends_0_n_3772807.html.

Trust for America’s Health. “Drug Abuse 2013 Data for Kentucky.” October 7, 2013. http://healthyamericans.org/reports/drugabuse2013/release.php?stateid=KY.

———. “Prescription Drug Abuse: Issue Report 2013—Strategies to Stop the Epidemic.” October 2013. http://healthyamericans.org/assets/files/TFAH2013RxDrugAbuseRptFINAL.pdf.

Trzeciak, Randall. “The CERT Insider Threat Database|Insider Threat.” *CERT Insider Threat Center*, August 15, 2011. http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=76.

Turner, Nigel, Denise L. Preston, Crystal Saunders, Steven McAvoy and Umesh Jain. “The Relationship of Problem Gambling to Criminal Behavior in a Sample of Canadian Male Federal Offenders.” *Journal of Gambling Studies* 25, no. 2 (June 2009): 153–69. doi:10.1007/s10899-009-9124-1.

U. S. Attorney’s Office (USAO). “Health Care Professional Pleads Guilty to Product Tampering Demerol Diverted at Bellevue, WA Surgery Clinic.” May 28, 2009. http://www.justice.gov/usao/waw/press/2009/may/gibson.html.

———. “U.S. Attorney’s Office—U.S. Department of Justice.” September 7, 2012. http://www.justice.gov/usao/waw/press/2012/September/bowman.html.

U.S. Department of Justice. National Drug Intelligence Center. “National Drug Threat Assessment 2011.” August 2011. http://www.justice.gov/archive/ndic/pubs44/44849/44849p.pdf.

University of North Texas University. “National Gambling Impact Study Commission Final Report.” 1999. http://govinfo.library.unt.edu/ngisc/reports/fullrpt.html.

USDOJ. “Convention Center’s Former Executive Director Sentenced to 24 Months in Prison for Embezzlement.” *U.S. Attorney’s Office—Western District of Kentucky*, June 7, 2012. http://www.justice.gov/usao/kyw/news/2012/20120607-01.html.

Wells, Joseph T. *Corporate Fraud Handbook: Prevention and Detection*. Hoboken, NJ: John Wiley & Sons, 2011.

White House, The. “Office of National Drug Control Policy.” 2012. http://www.whitehouse.gov/ondcp.

Wilber, Del Quentin. “Tax Scam Leader Gets More Than 17 Years.” *The Washington Post*, sec. Metro, July 1, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/06/30/AR2009063001652.html?sid=ST2008091700125.

Wood, Suzanne, and Martin F. Wiskoff. *Americans Who Spied Against Their Country Since World War II*. Monterey, CA: Defense Personnel Security Research Center, 1992.

Ziegler, Stephen J., and Nicholas P. Lovrich. "Pain Relief, Prescription Drugs, and Prosecution: A Four-State Survey of Chief Prosecutors." *The Journal of Law, Medicine & Ethics* 31, no. 1 (2003): 75–100. doi:10.1111/j.1748-720X.2003.tb00060.x.

Zietz, Dorothy. *Women Who Embezzle or Defraud: A Study of Convicted Felons*. New York: Praeger Publishers, 1981.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California