ADDRESSING THE CYBERSECURITY MALICIOUS INSIDER THREAT

by

Larry E. Schluderberg

A Capstone Project Submitted to the Faculty of

Utica College

December 2014

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Cybersecurity

Abstract

Malicious Insider threats consist of employees, contractors, or business partners who either have current authorized access, or have had authorized access to an organization's critical information and have intentionally misused that access in a manner that compromised the organization. Although incidents initiated by malicious insiders are fewer in number than those initiated by external threats, insider incidents are more costly on average because the threat is already trusted by the organization and often has privileged access to the organization's most sensitive information. In spite of the damage they cause there are indications that the seriousness of insider incidents are underappreciated as threats by management. The purpose of this research was to investigate who constitutes MI threats, why and how they initiate attacks, the extent to which MI activity can be modeled or predicted, and to suggest some risk mitigation strategies. The results reveal that addressing the Malicious Insider threat is much more than just a technical issue. Dealing effectively with the threat involves managing the dynamic interaction between employees, their work environment and work associates, the systems with which they interact, and organizational policies and procedures. Techniques for detecting and mitigating the threat are available and can be effectively applied. Some of the procedural and technical methods include definition of, follow through, and consistent application of corporate, and dealing with adverse events indigenous to the business environment. Other methods include conduct of a comprehensive Malicious Insider risk assessment, selective monitoring of employees in response to behavioral precursors, minimizing unknown access paths, control of the organization's production software baseline, and effective use of peer reporting. Keywords: Cybersecurity, Professor Paul Pantani, CERT, malicious, insider,IDS, SIEMS. FIM, RBAC, ABAC, behavioral, peer, precursors, access, authentication, predictive, analytics, system, dynamics, demographics.

Acknowledgements

I am pleased to acknowledge Professor Joe Giordano and Utica College for providing a challenging and comprehensive cybersecurity program. In addition, I want to express my gratitude to Professor Paul Pantani for leading me through the capstone process and to Dr. David A. Wheeler for his subject matter expertise and insightful comments with respect to the technical content of this paper as my second reader. I would also like to express my gratitude to the staff and instructors at Utica College for all the hard work and preparation that they put forth to challenge each student and ensure that they succeed. Those who have been a particularly positive influence with respect to enhancing my cybersecurity education are Salvador Paladino, Austen Givens, Robert DeCarlo, Jeff Bardin, Leonard Popyak, Tony Martino, and Vernon McCandlish.

Many thanks to my wife Jeanette for putting up with the restrictions on my time imposed by pursuing a Master's degree concurrently with my work as a consulting engineer. Completion of this capstone paper has reinforced a perception I acquired during my cybersecurity coursework from the many practitioners I encountered along the way. The perception, which has become an apparent reality to me, is that while the technical aspects of cyber security are interesting and varied, it is the essentially human nature of both the threat and the solutions that keeps the field ever-changing and challenging. Pursuing knowledge on dealing with the Malicious Insider threat has reinforced the notion that the threat is people centric, and as a result, solutions must address the full spectrum of human psychology that dictates how technical capabilities and procedural and policy shortfalls can be used to inflict damage upon an organization. I hope that by articulating the lessons I have learned that I have in some small way contributed to the emerging body of knowledge necessary to achieve success in the cybersecurity field.

Table of Contents

List of Illustrative Materials

Addressing the Cybersecurity Malicious Insider Threat

The CERT Division of the Software Engineering Institute (SEI) at Carnegie Mellon University, hereafter referred to as CERT, defines the Malicious Insider (MI) threat to an organization 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 (Software Engineering Institute, 2014, para. 2).

While this definition is both succinct and correct in scope the public generally only hears of a few selected MI incidents. The result is a misperception that these types of incidents are an infrequent occurrence. Annual surveys conducted by the U.S. Secret Service, CSO Magazine, Deloitte, and CERT since 2004 have reported that between 37% and 55% of participants experienced an insider incident (Carnegie Mellon University, 2014).

The purpose of this research was to investigate how to address the MI threat by answering the following questions: Who constitutes MI threats? What are the primary motives and methods of malicious insider activity? Can an MI model be defined? What are the legal employment considerations associated with using modeled MI characteristics? What are technical and procedural strategies for mitigating the MI threat given the current state of knowledge about MI motivations and activity?

Justification for Research

At the very least, studies have indicated that the majority of MI incidents are under reported. The 2013 report of the Workshop on Research for Insider Threat (WRIT), which

highlights the challenges and trends specific to the insider threat problem from multiple viewpoints in an annual conference, stated that:

> Organizations suffering insider attacks are often reluctant to share data about those attacks publicly. Studies show over 70% of attacks are not reported externally, including many of the most common, low-level attacks. This leads to uncertainty that available data accurately represents the true nature of the problem. ("WRIT," 2013, para. 7)

Moreover, there are indications that the seriousness of incidents such as unauthorized access to confidential data, unauthorized disclosure of confidential data, execution of fraud and sabotage of systems networks or data are underappreciated as threats even though they represent purposeful action on the part of insiders in opposition to the interests of an organization. An article in *Computer Economics* magazine on May 2010 edition entitled "Malicious Insider Threats Greater Than Most IT Executives Think" ranked the percentage of organizational respondents viewing the four incidents indicated in Figure 1 as major threats (Computer Economics, 2010). Small organizations as indicated in the figure are those with less than fifty million dollars in annual sales.

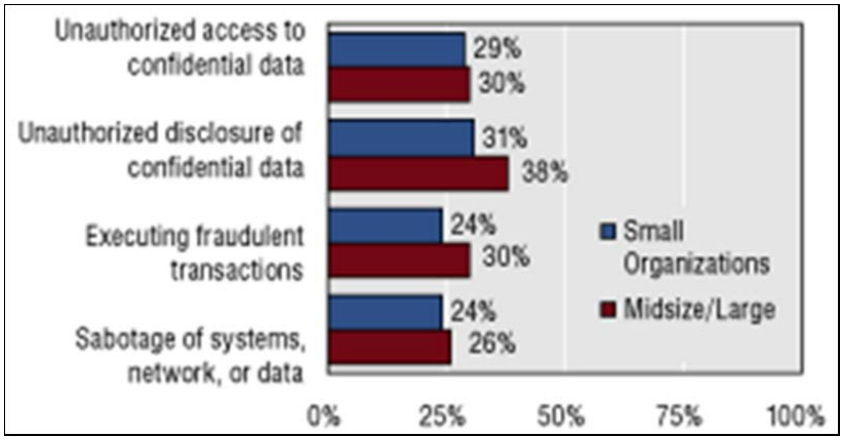

Figure 1. Percentage of Organizations Viewing Each Type of MI Incident as a Major Threat. Most organizations are only moderately concerned about Malicious Insiders. Adapted from "Malicious Insider Threats Greater Than Most IT Executives Think" Computer Economics May 2010, Figure 1.

Figure 2, derived from the *Computer Economics* magazine report, depicts a two year period prior to publishing of the report and shows that 56% of midsize and large organizations experienced unauthorized disclosure of confidential information while 77% experienced an insider gaining unauthorized access to confidential data. Approximately one third experienced incidents of electronic fraud and approximately 20% experienced sabotage of systems or networks.

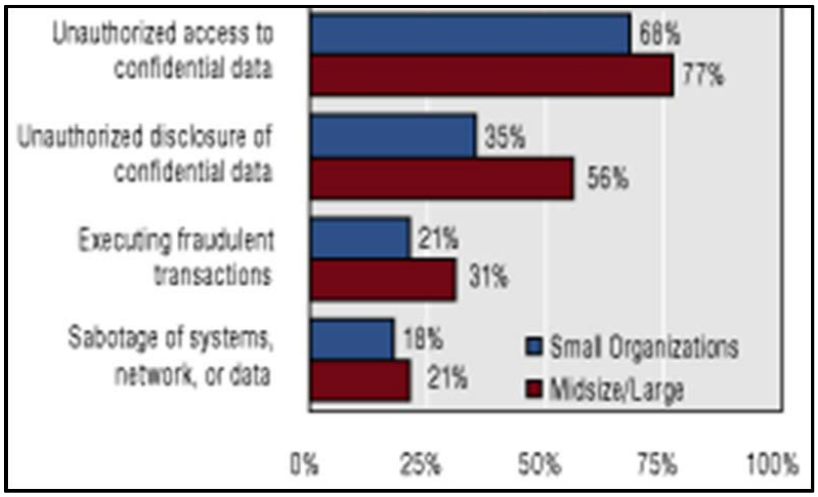

Figure 2. Percentage of Organizations with at Least One Malicious Insider Incident of Each Type Occurring in the Past Two Years. Incident occurrence rates sharply contrast the level of organizational concern. Adapted from "Malicious Insider Threats Greater Than Most IT Executives Think" Computer Economics May 2010, Figure 2.

The concern of organization executives over incidents such as unauthorized disclosure of confidential data and execution of fraudulent transactions lags significantly the occurrence of these types of events within their organizations, and is generally not reported outside the organization.

Notwithstanding that MI incidents have historically been under reported, and the significance of their occurrence underappreciated in terms of organizational risk, their threat today is greater than ever. A 2014 Cybersecurity Survey conducted by the U.S. Secret Service, CSO Magazine, Deloitte, and CERT indicated that although only "28% of electronic crime events were known or suspected of being committed by insiders 46% of the 557 respondents

thought insider crimes were more damaging to their organizations than outside crimes (Carnegie Mellon University, 2014, vg 5-6). Widespread layoffs and loss of job security have resulted from the recent prolonged economic recession. These factors tend to increase the percentage of employees developing malicious intent (Schneirer, 2009). Employees who feel mistreated, or fear unemployment, may plot to sabotage an organization's systems and those experiencing job loss, or otherwise perceive their value to an organization diminishing, may actually follow through on these plans. (Computer Economics, 2010).

IT professionals must develop technical and procedural defensive strategies to mitigate the potential damage that can occur as a byproduct of failing to prevent MI incidents. As security consultant Bruce Schneirer has stated, "Insiders are especially pernicious attackers because they are trusted. They have access; they know how the system and security works and its weak points. They also have opportunity" (Schneirer, 2009, para. 4). As a result the severity of damage inflicted by malicious insiders is significantly worse than that normally inflicted by external threats. For example, even though the number of insider incidents per year is far less than incidents caused by external sources, CERT has reported that based upon its examination of cases related to illicit activity in the U.S. financial services sector the average dollar cost inflicted per insider incident is approximately $800,000 as opposed to the $400,000 cost per external incident (Cummings, Lewellen, McIntire, Moore, & Trzeciak, 2012).

Research Gaps

Research conducted to use predictive analytics to acquire a statistical understanding of potential attacker technical actions, and thereby identify them, has not produced consistent results. The use of behavioral modeling and simulation to produce an Interactive Learning Environment (ILE) to teach executives, managers, technical staff, human resources, and security

officers the complex dynamics of the insider threat problem is still evolving. Results are varied indicating that the psychological, social mores and demographic factors involved may be too complex to provide predictive value though researchers have claimed an ILE may be helpful in providing some level of insight to corporate management. A May 2008 evaluation of the Management and Education of the Risk of Insider Threat (MERIT) simulation produced by CERT concluded that "The simulations accurately mimic the patterns and trends in the majority of the cases in the Insider Threat Study. Further calibration and validation of the model is still necessary before it can be released for educational or training use" (Cappelli et al., 2008, p. 25).

In addition, according to Patrick Reidy, Federal Bureau of Investigation (FBI) Chief Information Security Officer (CISO), initial FBI predictive analysis efforts produced results that were statistically worse than random with respect to detecting MI threats stating, "We would have done better hiring Punxsutawney Phil, waving him in front of someone and saying, Is this an insider or not an insider?" ("5 Lessons from," 2013, para. 10). However, FBI malicious threat researcher Kate Randal claims that ongoing research has identified some high risk indicators such as stress from a divorce, exhibiting retaliatory behavior, and inability to work in a team environment ("5 Lessons from," 2013).

Research shortfalls also exist with respect to defining and evaluating MI defensive strategies. Government organizations like the DOD generally possess sufficient Human Resources (HR), legal, investigative and database assets to adequately screen prospective employees with respect to the potential for MI behavior. However, even these capabilities failed to identify potential insider threats like Major Nidal Hasan, responsible for the Fort Hood shooting attack in 2009, and Aron Alexis, responsible for the shooting attack at the Washington Naval Yard in 2013. Corporations like Raytheon and Hewlett Packard may possess sufficient

resources with respect to HR and legal assets, but may not have sufficient resources to employ quality investigative techniques and database assets in screening employment candidates. Furthermore, small corporations may have little or no capability to adequately screen employment candidates. Corporate budgets impact the use of cost driven technical assets available for implementing sufficient access control within the corporate Information Technology (IT) environment producing variations in security effectiveness. Moreover, the recent trend toward Bring Your Own Device (BYOD) computing environments can also influence technical and procedural approaches to MI risk mitigation because of the risk of employee espionage they engender (Demarco, 2014).

The legal implications of denying employment to candidates with perceived MI tendencies or potentially adverse information, such as criminal records, also needs to be taken into consideration. For example, the Equal Employment Opportunity Commission (EEOC) has held that "an employer's policy or practice of excluding individuals from employment because they have criminal conviction records is unlawful under Title VII of the Civil Rights Act of 1964 unless the policy or practice is justified by a business necessity" (Ryan, 2012, para. 5). Further research into both technical and procedural means of detecting and preventing MI activity is also warranted. An example might be investigation into the effectiveness of two person procedures and interpersonal behavioral observation, such as the Personnel Reliability Program (PRP) employs within DOD nuclear weapons environments. Another example might be investigation of the effectiveness of two factor authentication systems (e.g. something you known as well as something possessed, or some biological attribute) in deterring MI activity (Rosenblatt, 2013, para. 6). Finally, investigation may be warranted into some less tangible aspects of human behavior such as the erosion of social mores which attach stigma to unethical conduct and its

potential effect on MI activity. For example, cheating within the U.S. Air Force with respect to nuclear weapons proficiency examinations and within the U.S. Navy with respect to nuclear reactor plant training (McCaughan, 2014; CBS news, 2014).

Audience

This research assesses existing and emerging definitions of the MI threat and associated MI motives and methods. As a result, it will assist government and industry system administrators, threat awareness trainers, HR recruiters, hiring managers, and government or corporate executives with recognizing some indicators of potential MI activity. By suggesting approaches to defense in depth threat mitigation this research will also assist the same group of organization managers in their efforts to mitigate a difficult to define, and extremely pernicious MI threat.

Literature Review

The literature reviewed for this study consisted of scholarly papers and reports released by CERT. This work represents the critical mass of academic research on the MI threat. Since 2001, the U.S. Secret Service National Threat Assessment Center (NTAC) and CERT have collaborated in a multi-year Insider Threat Study (ITS) with the objective of helping private industry, government, and law enforcement better understand, detect and possibly prevent MI activity. The study has resulted in a series of four early ITS reports (2005-2008) covering illicit cyber activity in the Banking and Finance (B&F) sector, Information Technology and Telecommunication (IT&T) sector, the government sector, and incidents of computer system sabotage in Critical Infrastructure (CI) sectors. A later CERT report on illicit fraudulent activity in the U.S. Financial sector was released in 2012.

This body of academic research was selected for several reasons. First, ITS research attempts to examine insider threat incidents from both behavioral and technical perspectives. Secondly, to increase reliability, the CERT Insider Threat Center has assembled a consistently coded case database enabling extraction of information regarding MI motive, access availability, attack methods, and associated organizational policy and procedures (Cummings, Lewellen, McIntire, Moore, & Trzeciak, 2012). "Case coding is a critical process in which information gathered through case file review and interviews is entered into the database according to a prescribed methodology recorded in a code book" (Cummings, et al, 2012, p. 7). Additionally, CERT has augmented their case study research with simulations enabling testing and exploratory research of hypothetical detection and mitigation methods while minimizing the vagaries introduced by statistical gaps in case evidence (Cummings et al., 2012). Finally, based upon this researcher's ability to review the available literature, the CERT ITS and modeling reports represent the largest, most complete body of MI research available, and consistently reported upon over the past decade.

To date the data library totals over 700 cases maintained at the CERT Insider Threat Center (Cummings et al, 2012). The cases span organizations, within the continental United States, ranging in size from between 1 and 100 employees to over 50,000 employees (Keeney, Kowalski, Cappelli, Shimeall, & Rogers, 2005). Based upon this researcher's investigations, the CERT Insider Threat Center database is unique with respect to both the depth of detail of and breadth of information available on MI threats. The ITS reports and associated modeling results were extremely useful in formulating an understanding of MI motivation, behavior, and methods as well as providing insight into the dynamic relationships between insiders and the policies and procedures of the organizations in which they operate.

The literature review also included articles and reports from the FBI, DOD, and industry cybersecurity and labor law practitioners as well as government legal guidelines regarding equal employment opportunity and Americans with disabilities. These sources were instrumental in understanding the legal context in which pre-employment background information is evaluated, and an understanding the technological tools available to mitigate MI threats and how they work. Discussion of the insights gained through the literature review is presented below grouped according to the four research questions presented above namely: Who constitutes MI threats? What are the primary motives and methods of malicious insider activity? Can an MI model be defined? What are the legal employment considerations associated with using modeled MI characteristics? What are technical and procedural strategies for mitigating the MI threat given the current state of knowledge about MI motivations and activity?

MI Demographics

MI demographics for the B&F sector, for sabotage of CI, and the IT&T and government sectors all exhibited variability. In all cases insider age varied between 17 and 60 (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005). In the IT&T sector 91% of insiders were male (Kowalski, Cappelli, & Moore, 2008). In incidents of sabotage of CI 96% of insiders were male (Keeney et al., 2005, p. 12). The government sector exhibited 50% men and 50% women insiders (Kowalski et al., 2008). In the B&F sector 42% of insiders were female (Randazzo et al., 2005). In all sectors and for sabotage of CI the number of insiders having an arrest record was above the national average. The National Employment Law Project (NELP) reports “one in four adults in America have arrest or conviction records that often follow them throughout their lives” (National Employment Law Project, 2014, para. 1). The sabotage of CI study indicated that 30% of insiders had been previously arrested (Keeney et al., 2005). In the IT&T sector 38% of

insiders had been arrested previously (Kowalski et al., 2008). In the B&F sector 27% of insiders had prior arrests (Randazzo et al., 2005). The government sector report indicated that 31% of insiders had a prior arrest history (Kowalski et al., 2008).

In the government sector 90% of the insiders were current employees of the organization working full-time schedules (Kowalski et al., 2008). In the B&F sector 83% of insider threat cases involved attacks from within the insider's organization (Randazzo et al., 2005). However, in the IT&T sector 53% of the insiders were current employees or contractors of the organization and 47% were former employees or contractors (Kowalski et al., 2008). In cases involving sabotage of CI, 59% of the insiders were former employees or contractors and 41% were current employees or contractors (Keeney et al., 2005).

In the government and B&F sectors incident perpetrators were not technically sophisticated. In the B&F sector "only 23% of the insiders were employed in technical positions" (Randazzo et al., 2005, p. 10). In the government sector "26% of the insiders worked in positions such as system administrator, programmer, or IT specialists that require technical skills" (Kowalski et al., 2008, p. 15). In the IT&T sector "63% of the insiders were employed in technical positions such as system administrator, programmer, or IT specialist" (Kowalski et al., 2008, p. 16) In cases involving sabotage of CI "86% of the insiders were employed in technical positions" (Keeney et al., 2005, p. 11).

Motives and Methods of Malicious Insider Activity

CERT insider threat workshop participants agreed that it is helpful to understand the motivations and methods of insider attacks (Moore, Cappelli, & Trzeciak, 2008). Motives for MI action and attack methods varied based upon the sector in which the insiders functioned. The

level of system access afforded to insiders also varied based upon sector. However, in all sectors actual malicious activity was triggered by a workplace related event.

MI Attack Motives and Triggering Events. Motives and goals for MI attacks exhibit variability from sector to sector. In the IT&T sector 56% of all insiders were motivated at least partially by a desire to seek revenge (Kowalski, et al, 2008). In the B&F sector, the motive for 81% of insiders studied was the prospect of financial gain (Randazzo et al., 2005). Fraud was also prevalent in the government sector with 54% of insiders motivated by financial gain (Kowalski et al., 2008). In those incidents resulting in an active sabotage against CI 84% of the incidents were motivated by a desire to seek revenge (Keeney, et al., 2005).

While perceived financial need and revenge were consistently referenced as motives in the ITS papers, the FBI has compiled a list of personal factors that increase the likelihood that someone will engage in MI activity. These factors are articulated in an "FBI Insider Threat Brochure" published in October 2012. Some of the factors such as a lack of recognition at work, disagreement with co-workers or managers, dissatisfaction with the job, or a pending layoff directly contribute to the revenge motive while others tend to span the gamut of human psychology. Examples are:

> A desire to help the underdog or a particular cause; Allegiance to another person company or country; A need for intrigue or clandestine activity to add excitement to life; Vulnerability to blackmail engendered by extramarital affairs, gambling, or fraud; Ego or self-image inflation engendered by either an above the rules attitude or a desire to repair self-esteem; A desire to win the approval of someone who could benefit from insider information; Compulsive, destructive behaviors such as alcohol or drug abuse; and

Family problems such as marital conflicts or separation from loved ones. (Federal Bureau of, 2012, p. 2)

ITS reports for the government and IT&T sectors and for sabotage of CI indicate that even though the motivation for MI activity exists for an individual, in most cases a specific event or series of events triggers these individuals into action. In the IT&T sector 73% of cases were triggered by a specific event. Sixty seven percent of those cases were initiated by a work related events such as employment termination; disputes with a current or former employer, or employment related discipline, and 33% were not employment related (Kowalski et al., 2008). For incidents related to sabotage of CI, 92% of cases were triggered by events identical to those in the IT&T sector (Keeney et al., 2005). In the government sector 56% of the cases were triggered by an event identical to those in the IT&T sector, and 40% were triggered by financial hardship or bribe (Kowalski et al., 2008). The B&F sector ITS study did not emphasize the events that triggered insider action, but did cite termination as a trigger event under cases in which insider's activities were conducted for other reasons (Randazzo et al., 2005).

Methods of MI Attacks. In all sectors the majority of MI planned their attacks in advance. For the B&F sector, in 81% of the incidents, the insiders planned their actions in advance (Randazzo et al., 2005). For government sector cases, 88% of insiders developed plans prior to carrying out their illicit activities. In 36% of government sector cases insiders planned their activities in collusion with others. For the IT&T sector 76% of the insiders developed plans in advance (Kowalski et al., 2008). For cases involving sabotage of CI, 62% of insiders developed plans to harm the organization (Keeney et al., 2005). Moreover, in all sectors insider malicious planning was noticed by others. For the B&F sector:

> In 85% of the incidents, someone other than the insider had full or partial knowledge about the insider's intentions plans and activities. These included individuals involved in the incident, or beneficiaries of the insider activity, co-workers, friends, and family members (Randazzo et al., 2005, p. 12).

In the government sector "The majority (60%) of insiders engaged in preparatory or planning activities that were noticeable to others" (Kowalski et al., 2008, p. 18). For the IT&T sector:

> In 46% of the cases, other individuals had information about the insiders' plans, intentions, and/or activities prior to the attacks. These others included individuals who were involved in and benefited from the attacks, co-workers, acquaintances, family members, and friends (Kowalski et al., 2008, p. 20).

For cases involving sabotage of CI, in "31% of the cases others had information about the insiders plans and/or activities" (Keeney et al., 2005, p. 16).

In advancing their attacks insiders exhibited both similarities and differences across sectors with respect to their access, methods, and how they were detected. In cases of sabotage of CI:

> The majority, (57%) of insiders, were granted system administrator access at the time they were hired, but 85% of those granted administrator privileges no longer legitimately retained that access at the time of the incident. Most of the attackers had either resigned or been terminated. In 38% of the cases their access had been disabled and in 27% of the cases it had not been disabled. An additional 33% of sabotage insiders were hired with privileged access, but 60% of these privileged users no longer retained legitimate privileged access at the time of the incident. Of those with privileged access 20% had

their access disabled and 33% did not have their access disabled. (Keeney et al., 2005, p. 17)

The net result was that in cases of sabotage of CI most attacks occurred after the MI had left the organization. For sabotage of CI "61% of the cases were limited to relatively unsophisticated methods" (Keeney et al., 2005, p. 17). The remaining "39% of sabotage of CI insiders used one or more relatively sophisticated methods of attack which included a script or program, an autonomous agent, a toolkit, flooding, probing, scanning, and spoofing" (Keeney et al., 2005, p. 18).

In 60% of the sabotage cases the insider compromised an account to carry out the attack. These compromises used relatively technically unsophisticated techniques including use of another's username and password or use of an unauthorized account created by the insider. In many of these cases the insiders used shared accounts such as administrator accounts or their own accounts to carry out the attack. In 56% of the sabotage of CI cases, the attacks were conducted solely via remote access. Thirty five percent took place solely from within the workspace, and 8% took place both from within the workplace and remotely. During sabotage of CI insiders took steps to conceal their identities and their activities. In sabotage of CI cases 63% of attacks were only detected once an irregularity in system information became noticeable, or a system failure occurred, and most of the attacks were detected by non-security personnel. The means of identifying the perpetrators employed manual procedures and review of system logs in 75% of those cases (Keeney et al., 2005).

Unlike sabotage of CI insider incidents, in the IT&T sector, half of the insiders had authorized access at the time of the incidents (Kowalski et al., 2008).

> In 29% of the cases, insider's access had been disabled by their employers prior to the incidents. In 23% of the cases, insiders were able to carry out illicit activities after their termination because their employers did not disable their access. (Kowalski et al., 2008, p. 22)

In the IT&T sector "58% of insiders used one or more relatively sophisticated methods of attack" (Kowalski et al., 2008, p. 22). The sophisticated techniques employed were identical to those employed by only 39% of insiders in cases of sabotage of CI. In 38% of the IT&T cases, insiders compromised an account to carry out the incidents (Kowalski et al., 2008). Overall, the compromising techniques in the IT&T sector were identical to those employed in cases of sabotage of CI and remote access was used to initiate the attack. In 42% of the cases, the insider's actions were limited to relatively unsophisticated methods of attack such as user commands, information exchanges, and physical security vulnerabilities (Kowalski et al., 2008). Similarly to insiders who sabotaged CI, IT&T "insiders took steps to conceal their identities and their activities" (Kowalski et al., 2008, p. 24). The majority of attacks (86%) were only detected once an irregularity in system information became noticeable or a system failure occurred and most of the attacks were detected by non-security personnel. The means of identifying the perpetrators "employed manual procedures and review of system logs in 80% of the cases" (Kowalski et al., 2008)

In the government sector 60% of insiders were granted authorized, unprivileged access, 17% were granted authorized, privileged access and 17% were granted administrator access. At the time illicit activities were committed 50% were authorized, unprivileged users, 24% were authorized, privileged users, and 12% had administrator access (Kowalski et al., 2008).

Unlike the sabotage of CI and IT&T sectors, Government insiders used a variety of non-technical methods to compromise accounts including coercing or intimidating co-workers into revealing their passwords, sharing passwords, using co-workers computers left logged on without a screen lock, and keeping the organization's laptop after resignation (Kowalski et al., 2008). "Access control gaps facilitated most of the insider incidents" (Kowalski et al., 2008, p. 35).

> These access control gaps included: policy or procedural oversights such as password sharing, social engineering resulting in password sharing, poor implementation of access controls providing employees with excessive capabilities not consistent with their jobs, insufficient technical controls enabling insiders to violate separation of duties and business policies, poor system configuration that failed to provide the ability to associate all actions of the individual user, and inefficient account management practices enabling a small percentage of technical users to create a backdoor account for later use. (Kowalski et al., 2008, p. 35)

"Half of government sector insiders exploited deficiencies in a business process to commit their activities. Ineffective separation of duties provided the opportunity for insider activity" (Kowalski et al., 2008, p 41). In some incidents, "physical security records, computer system log information, and personal observations were instrumental in identifying the insider" (Kowalski et al., 2008, p. 45).

The ITS for the B&F sector indicated that in 87% of the cases studied, insiders employed simple, legitimate user commands to carry out the incidents. Additionally, in 70% of the cases studied, the insiders exploited or attempted to exploit systemic vulnerabilities in applications and/or processes or procedures (Randazzo et al., 2005). In 78% of the incidents, the insiders

were authorized users with active computer accounts at the time of the incident. In 43% of the cases, the insider used his or her own username and password to carry out the incident (Randazzo et al., 2005). In the B&F sector a significant difference was noted in the methods used by supervisory personnel as opposed to non-managers like accountants, and customer service clerks. In general the duration of crimes by managers was longer, resulting in more financial damage per incident because in many instances their actions were less auditable than those of subordinate employees. In many cases supervisors were able to change an organization's business practices to suit their needs and remain undetected (Cummings et al., 2012).

B&F "insider incidents were detected by a range of people both internal and external to the organization" (Randazzo et al., 2005, p. 17). In 61% of the cases, the insiders were detected by persons who were not responsible for security (Randazzo et al., 2005). Within this 61% of cases insiders were caught through manual procedures, including an inability to login, customer complaints, manual account audits, and notification by outsiders (Randazzo et al., 2005). In 74% of the cases, after detection, the insider's identities were obtained using system logs while in 30% of the cases forensics examination of the targeted network, system, or data of the insiders' home work environment provided identification (Randazzo et al., 2005).

MI Modeling

Attempts to model MI activity to date have fallen into two general categories consisting of those techniques which attempt to predict MI activity and those techniques which attempt to characterize MI behavior with the objective of improving organizational response to that behavior. As mentioned in the Research Gaps section, the FBI initially attempted to establish statistical methods to predict MI behavior and then shifted to analysis of behavioral traits that might be indicative of a predisposition to MI activity ("5 Lessons from," 2013). CERT invested

efforts into studying behavioral activity associated with MI cases with the intent of developing insight into the dynamics associated with MI incidents, as well as modeling, to develop an ILE to support teaching organizations about MI activity (Cappelli et al., 2008).

Analytic Modeling Approaches. Some research efforts have attempted to use a subset of business analytics known as predictive analytics to determine the probability that a MI incident will occur. "Predictive analytics is the practice of extracting information from existing data sets in order to determine patterns and predict future outcomes and trends" (Beal, 2014, para. 1). The Defense Advanced Research Project Agency (DARPA) in a program called Anomaly Detection at Multiple Scales (ADAMS) has collected a database of computer usage activity of approximately 5500 people in various business organizations which is not disclosed publicly. Science Applications International Corporation (SAIC) in conjunction with Georgia Institute of Technology, Oregon State University, University of Massachusetts, and Carnegie Mellon University have pursued the use of predictive analytics in conjunction with the ADAMS database to detect MI threat anomalies that can be provided to analysts for use in predicting MI activity. The project called PROactive Detection of Insider threats with Graphic Analysis and Learning (PRODIGAL) has developed, applied, and evaluated multiple Anomaly Detection (AD) algorithms and supporting technologies capable of extracting features associated with MI goals and stages of activity in order to predict the occurrence of MI incidents (Senator et al., 2013). Detection of MI activity in a computer network environment is problematic "because malicious activity by insiders is a small but critical portion of the overall activity on such systems" (Senator et al., 2013, p. 1). The resulting low signal-to-noise ratio is difficult for AD algorithms to overcome. The PRODIGAL research report concluded that:

> The work reported here demonstrates the feasibility of detecting the weak signals characteristic of insider threats using a novel set of algorithms and methods. However, additional research and engineering is needed to enable these techniques to be useful for real analysts in an integrated system. (Senator et al., 2013, p. 8)

The FBI has also put significant effort into the use of predictive analytics to help predict insider behavior prior to malicious activity. At the 2013 RSA security conference the FBI reported that their predictive analytics efforts came up with a system that was "statistically worse than random at ferreting out bad behavior" ("5 Lessons from," 2013, para. 8). The FBI reported that having failed to develop effective predictive analytic techniques they had moved toward a behavioral detection methodology that they believed to be more effective ("5 Lessons from," 2013). Kate Randal, an FBI insider threat researcher indicated that one of the issues with the slow growth of insider threat detection and deterrence is that many research efforts "just focus on looking at data from the bad guys" ("5 Lessons from," 2013, para. 17). As a result, the FBI has focused its diagnostic approach on collecting data from and comparing it between a known group of bad actors and a control group of assumed good insiders.

MITRE Corporation and Georgetown University also pursued the use of predictive analytics to detect MI threats. The prototype system resulting from the effort was called Exploit Latent Information to Counter Insider Threats (ELICIT). In addition to development of the ELICIT software the study conducted a structured experiment using a MITRE intranet with approximately 1600 users, and MITRE employees playing roles as both benign users and MI threats. The study avoided the potential for bias errors that concerned the FBI by employing double blind experimental techniques and using the benign user group as a control group to avoid misinterpretation of normal user actions as indicative of MI activity. The ELICIT tool was

employed to process network traffic to produce information use events. A team of 7 Subject Matter Experts (SME) was used to evaluate ELICIT results (Caputo, Maloof, & Stephens, 2009).

With respect to the ELICT software the study encountered signal-to-noise problems similar to those experienced by the PRODICAL program and concluded that "although our preliminary analysis revealed interesting and significant patterns of malicious behavior, we haven't identified any one behavior that distinguishes malicious users from benign ones" (Caputo et al., 2009, p. 20). However, the study concluded that the use of the double-blind, controlled experiment was valuable stating that "we lowered the false alarm threshold, helped analysts identify misuse patterns that require attention, and provided new insights for what the common operational picture could look like for cyberspace" (Caputo et al., 2009, p. 20). The Caputo study also noted that controlled experiments were time consuming and costly as well as effective (Caputo et al., 2009). One valuable finding resulting from the MITRE study was that "making employees aware of monitoring mechanisms, either through educational awareness or pop-up reminders could help deter malicious users" (Caputo et al., 2009, p. 19). The study also concluded that "most insider research today lacks a carefully controlled baseline group for real comparison and makes statistical analyses and interpretation of findings challenging" (Caputo et al., 2009, p. 19).

Patrick Reidy, CISO for the FBI commented on a common misperception that MI threats were inside hackers stating that:

> You're dealing with authorized users doing authorized things for malicious purposes. In fact, going over 20 years of espionage cases, none of those involve people having to do something like run hacking tools or escalate privileges for the purpose of espionage. ("5 Lessons from," 2013, para. 3)

The ITS studies conducted by CERT also confirmed that the majority of insider attacks, particularly in the government and financial sectors, were not technically sophisticated, but instead were perpetrated by insiders using access to normal system functions within their daily, authorized span of control stating "The data in our research overwhelmingly points to employees in non-technical positions" (Cummings et al., 2012, p. 16).

Behavioral Modeling Approaches. The FBI has more recently focused on applying controlled experimentation methodology in three realms that they term "cyber, contextual, and psychosocial" ("5 Lessons from," 2013, para. 18). Randal has indicated that some of the factors the FBI thought would be most diagnostic such as disgruntlement or workplace issues were less informative than more innate psychological predisposition conditions when comparing the bad insiders with the control group. Some examples of these predispositions were conditions such as "stress from a divorce, inability to work in a team environment, and exhibiting retaliatory behavior" ("5 Lessons," 2013, para. 20).

While Randall acknowledges that corporate enterprises may not be able to do the same kind of psychological screening that the FBI does with their employees, she has suggested that this information may be elicited in other ways. Some examples are "behavioral manifestations, making supervisors more aware of the insider threat problem, and creating an environment where they may be more willing to report some of these things as they see them" ("5 Lessons from," 2013, para. 22). FBI experience employing both statistically based predictive analysis techniques and behavior analysis has resulted in Randal stating at the 2013 RSA security conference that unlike many other issues in information assurance, the risk from insider threats is not a technical problem, but a people-centric problem requiring a people centric multidisciplinary approach ("5 Lessons from," 2013). She stated that MI risk identification should "start by focusing efforts at

identifying and looking at your internal people, you're likely enemies, and the data that would be at risk" ("5 Lessons from," 2013, para. 7).

The first two CERT ITS reports on MI incidents in the B&F sector and for cases of sabotage of CI revealed that MI activity involved a dynamic interaction of personal elements, technical elements, and organization policies and practices. To detect insider threats or mitigate the effects of their activity "managers, IT staff, human resources, security officers, and others in the organization must understand the psychological, organizational and technical aspects as well as how they coordinate their actions over time" (Cappelli et al., 2008, p. 2). The CERT staff felt strongly that an important next step for MI research was the development of education and training materials to address the issue. Shortly after publication of the *Computer System Sabotage in Critical Infrastructure Sectors* ITS report the U.S. Department of Defense Personnel Security Research Center (PERSEREC) requested CERT assistance in comparing and contrasting cases of sabotage of CI with cases of espionage (Cappelli et al., 2008).

Organizations employing computerized networks in business represent a complex system involving both people and technology. Employees operate systems with an assigned level of access and a set of authorized abilities which may change over time. Organizations exercise policies designed to optimize productivity while guaranteeing security. Sometimes these policies are well developed and implemented and sometimes they are not (Cappelli et al., 2008).

After a good deal of research CERT decided to employ system dynamics modeling as a viable mechanism for developing the desired education and training material with respect to insider threat risks and to support the training with an ILE. The project was named MERIT. The project goal was to develop a systems dynamics model that could be used for hands-on analysis of the effects of policy, technical, and countermeasure decisions on malicious insider activity.

The MERIT modeling effort was structured not to predict MI activity but rather to provide managers, IT staff, human resources, and security officers with an ILE capable of providing insight into the dynamic interaction of personal elements, technical elements, and organization policies and practices. In order to maximize synergy between initial MERIT development and PERSEREC goals of comparing and contrasting sabotage of CI incidents with espionage cases it was decided to initially focus upon the well-defined subset of the 49 cases from the sabotage of CI Insider Threat Study. The approach taken was to develop two system dynamics models, one that focused on sabotage of CI, and a second that focused upon espionage with the objective of eventually comparing and contrasting results of the two models to support PERSEREC goals (Cappelli et al., 2008).

During the study, "CERT's technical security expertise was augmented with expertise from several organizations in the areas of psychology, insider threat, espionage, and cybercrime" (Cappelli et al., 2008, p. 5). The system dynamics modeling methodology employed in MERIT has been used to gain insight into some of the most challenging strategy questions facing businesses and government for several decades (Moore et al., 2008). The methodology decomposes "the causal structure of the problematic behavior into its feedback loops to understand which loop is strongest (i.e. which loop's influence on behavior dominates all others) at particular points through time" (Moore et al., 2008, p. 25). The loops can be implemented via computer simulation or other means such as role playing or gamming. MERIT employs computer simulation. Such simulations produce a level of knowledge less precise than a statistical prediction would be, but significantly better than the level of knowledge obtainable through purely mental models (Moore et al., 2008).

An example of how the system dynamics methodology deals with the interaction between personal psychological factors, organizational policy and procedure, and the potential for unanticipated consequences is depicted in Figure 3. As shown in the black boxes, Insider disgruntlement represents the insider's internal feelings of discontent due to restrictions imposed by the organization that he perceives as unacceptable or unfair. Behavioral precursors are observable aspects of the insider's off-line social behavior inside and outside the workplace that might be deemed inappropriate or disruptive in some way. Sanctions are the organization's punitive response to inappropriate behaviors. They can be technical, like restricting system privileges or the right to use the organization's equipment at home, or nontechnical such as demotion or formal reprimand. The gray text in Figure 3 represents insider modeled predispositions to certain characteristics such as disgruntlement. Inherent predispositions vary between individuals. Some people are disposed to become disgruntled in the face of negative events while others are not. Orange text represents organizational actions. Red text represents external influences such as the passage of time or a specific precipitating event. On-line behaviors occur within the organization's technical environment while off-line behaviors occur in social settings (Cappelli et al., 2008).

In cases of sabotage of CI, insiders expected to have technical freedom to use and control the organization's computing environment (Cappelli et al., 2008). Loop R2 of Figure 3 characterizes escalation of insider disgruntlement in response to increasingly unmet expectations as a result of sanctions imposed in response to inappropriate offline behavior exhibited by employees with a predisposition to disgruntlement. The severity of the insider's inappropriate actions is impacted by the time for the organization to realize the insider is responsible as shown in red. This scenario shows how sanctions imposed by an organization to increase security in

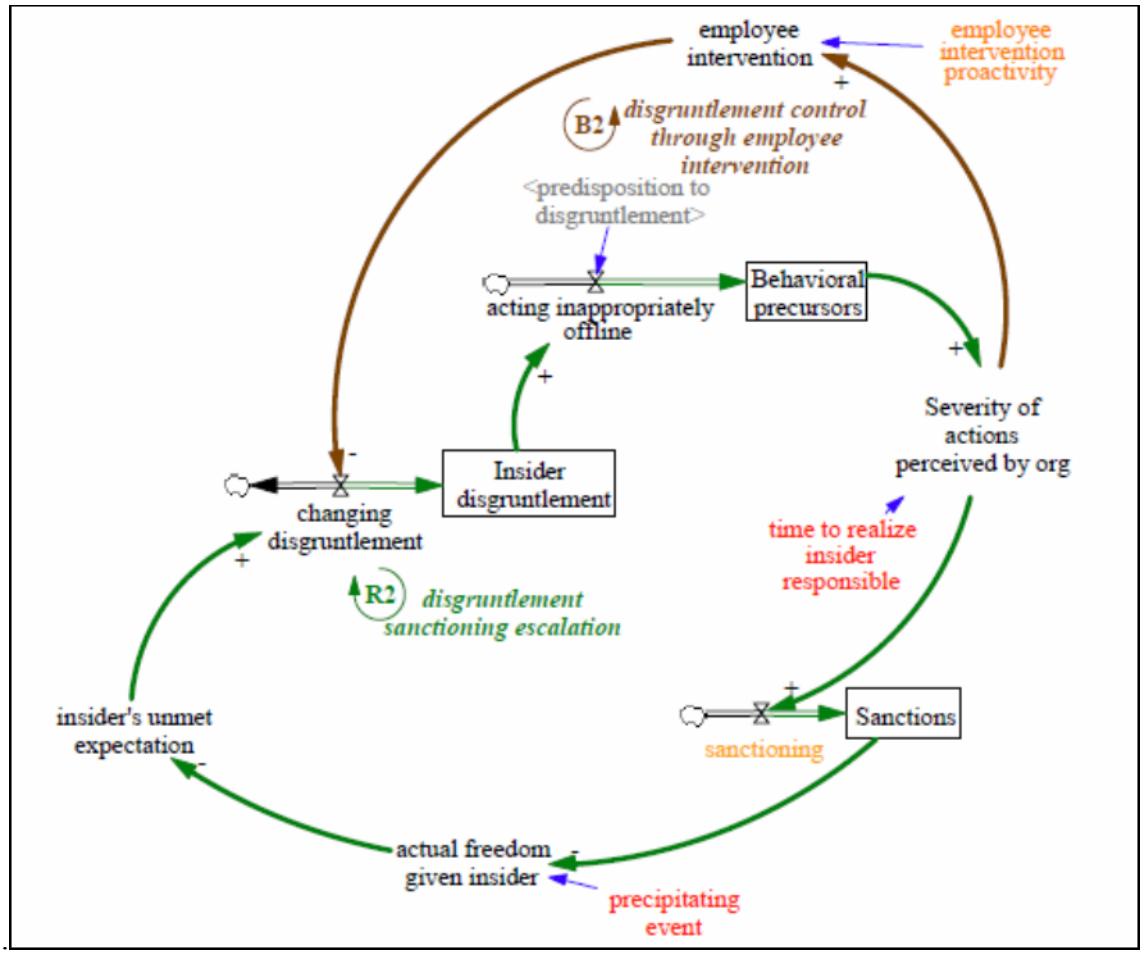

Figure 3. Interplay between Escalation of Disgruntlement and Sanctioning. Organization security policies sometimes have unintended consequences. Green loop (R2) represents escalation of employee disgruntlement in response to corporate sanctions. Brown loop (B2) represents mitigation of disgruntlement through proactive employee intervention. Plus signs represent increasing trends for enclosed parameter. Minus signs represent decreasing trends. Adapted from "Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System." CMU White Paper/2008_019_001_52338.

response to inappropriate insider behavior can actually accelerate progression toward a precipitating event which might trigger an insider incident because they restrict actual insider freedom to control the organization's computing environment thus increasing his unmet expectations and associated disgruntlement.

In some instances increasing disgruntlement will trigger technical precursor actions on the part of the employee such as setting up backdoor paths for later malicious use, or exploiting

discovered system technical vulnerabilities and maintaining them unknown to the organization. Discovery of this type of clandestine activity requires monitoring and auditing discipline on the part of the organization. On the other hand, loop B2 depicts how appropriately structured and proactive employee intervention can potentially reduce insider disgruntlement and prevent an incident (Cappelli et al., 2008). Intervention techniques may consist of educating employees on appropriate usage policy and the consequences if equipment is misused or other techniques such as counseling and mentoring (Moore et al., 2008).

Driven by the research of John D. Sterman (Sterman, 2006) and David C. Lane (Lane, 1995) the MERIT team developed a generic training case named the iAssemble Case in order to "test the impact of policies without the distortion of statistical error" (Cappelli et al., 2008, p. 4). Lane points out that the low cost and unambiguous feedback afforded by the model can be more helpful than reality as long as certain requirements are considered (Moore et al., 2008). In order for the generic training case to be effective, the model should represent the relevant environment with fidelity, the simulation instruction should be clear, the simulation objectives measurable and known to the user, and there must be an opportunity for debriefing or reflection (Moore et al., 2008).

Lessons Learned from Modeling MI behavior. Recalling the characteristics of sabotage of CI cases described above the following general observations regarding the risk of MI committing sabotage of CI are offered:

- Most insiders had personal predispositions that contributed to the risk of committing sabotage.
- Most insiders who committed sabotage were disgruntled due to unmet expectations.
- In most cases a stressful trigger event, including organizational sanctions, contributed to the likelihood of sabotage.

- Behavioral precursors were often observable in individuals prior to the attack, but were often ignored by coworkers and the organization.
- In many cases the organization failed to detect technical precursors.
- Insiders created or used access paths unknown to management to set up their attack and conceal their identity and actions. The majority of insiders attacked after termination.
- Lack of procedural and electronic access controls facilitated the sabotage.

(Moore et al, 2008, p. 3-6)

Additionally, based upon the general observations evolving from the sabotage of critical CI study the MERIT team developed two important lessons to be conveyed to organizations in the envisioned ILE. The first of these lessons is that "disabling access following termination is important; in order to do so effectively organizations must have full awareness of all access paths available to each of their employees" (Cappelli et al., 2008, p. 6). Many of the attacks in the sabotage of CI study were possible because the employer did not know all of the access paths available for their employees. Many attacks were actually conducted long after the employee had left the organization. This was facilitated because "system administrators created backdoor accounts with system administrator privileges, knowing that because account audits were not conducted the account would not be detected" (Cappelli et al., 2008, p. 6). Secondly, management must "carefully consider concerning behavior by an employee who appears to be disgruntled following a negative work-related event, possibly increasing monitoring of the employee's on line activity" (Cappelli et al., 2008, p. 7). Since it is not practical for organizations to monitor all online activity for all employees all the time, determining the appropriate balance between proactive system monitoring and other essential IT duties is a must.

The MERIT team felt confident that an effective model that conveys important lessons regarding sabotage of CI type insider threats had been created (Cappelli et al., 2008). However,

they stated that "further calibration and validation of the model is still necessary before it can be released for educational or training use" (Cappelli et al., 2008, p. 25). In accordance with the goals of the PERSEREC contract the MERIT team was able to develop two models one for sabotage and one for espionage. Furthermore, they were able to develop an "abstracted common model that illustrated high parallels between the two models" (Band, Cappelli, Fischer, Moore, & Shaw, 2006, p. 9).

Legal Considerations in use of MI Profiling and Modeling Information

CERT advocates organizations reducing MI threat risk starting with the hiring process by conducting background checks on perspective employees, verifying their credentials and discussing with prior employers the individual's competence and approach to dealing with workplace issues. They also recommend that prior to making employment decisions based upon background information that due consideration be given to legal issues associated with the use of such information (Silowash et al., 2012). These cautions relate to employment screening questions that could be asked and information that could be sought based upon psychosocial or behavioral traits derived from MI profiling and modeling. When asking pre-employment questions and conducting background checks the following federal pre-screening issues, in addition to any applicable state and local regulations are worthy of consideration and may need to be revisited if further evaluation is required as employees move to more sensitive roles within the organization (Silowash et al., 2012).

Considerations for Pre-screening Based on Psychological Predispositions. The ability of employers to pre-screen jobs applicants for psychosocial traits that would reveal the existence of personal psychological predispositions to MI activity or criminal background information is limited by existing federal legislation. The Americans with Disabilities Act (ADA) of 1990 and

amendments thereto enacted through 2008 protects individuals from employment discrimination based upon both physical and psychological disabilities. In doing so the law places restrictions upon the type of questions employers may ask of job applicants. Specifically, "Prior to an offer of employment, the ADA prohibits all disability-related inquiries and medical examinations, even if they are related to the job" (Equal Employment Opportunity, 2000, para. 4). A disability-related inquiry is "a question (or series of questions) that is likely to elicit information about a disability" (Equal Employment Opportunity, 2000, para. 9). Even though the types of psychological predispositions discussed in the CERT ITS may not qualify as psychological disabilities under the ADA, due diligence must be exercised to ensure the questions required to investigate the existence of these predispositions do not place the employer asking them in the position of asking questions likely to elicit information about a psychological disability. "After an applicant is given a conditional job offer, but before she or he starts work, an employer may make disability-related inquiries and conduct medical examinations, regardless of whether they are related to the job, as long as it does so for all entering employees in the same job category" (Equal Employment Opportunity, 2000, para. 4). The term medical examination encompasses psychological examination. After employment begins, an employer may make disability-related inquiries and require medical examinations "only if they are job-related and consistent with business necessity" (Equal Employment Opportunity, 2000, para. 4).

Considerations for Pre-screening Based on Criminal Record. Employers also experience restrictions in their ability to reject an employment candidate based upon their having a record of criminal conviction. "The EEOC enforces Title VII of the Civil Rights Act of 1964 (Title VII) which prohibits employment discrimination based on race, color, religion, sex, or national origin" (Equal Employment Opportunity, 2012, p. 3). Since having a criminal record is

not listed as a protected basis in title VII, whether an employer's reliance on a criminal record to deny employment violates title VII is dependent on whether it is part of a claim of employment discrimination based on race, color, religion, sex, or national origin. The EEOC states "liability for employment discrimination is determined using two analytic frameworks disparate treatment and disparate impact" (Equal Employment Opportunity, 2012, p. 6).

Under the disparate treatment framework "A covered employer is liable for violating Title VII when the plaintiff demonstrates that it treated him differently because of his race, national origin, or another protected basis" (Equal Employment Opportunity, 2012, p. 6). Title VII also prohibits employment decisions based upon stereotyped thinking. Therefore, "an employer's decision to reject a job applicant based on racial or ethnic stereotypes about criminality rather than qualifications and suitability for the position violates title VII" (Equal Employment Opportunity, 2012, p. 7).
Under the disparate impact framework:

> A covered employer is liable for violating title VII when the plaintiff demonstrates that the employer's neutral policy or practice has the effect of disproportionately screening out a title VII protected group and the employer fails to demonstrate that the policy or practice is job-related for the position in question and consistent with business necessity. (Equal Employment Opportunity, 2012, p. 8)

The EEOC cites national data that shows that African-Americans and Hispanics are "incarcerated at rates disproportionate to their numbers in the general population" which supports a finding that criminal records exclusions have a disparate impact based on race and national origin (Equal Employment Opportunity, 2012, p. 9-10). When asking a background investigating company for a criminal history report, the Fair Credit Reporting Act requires employers to obtain applicants' permission and to provide applicants with a copy of the report (U.S. Department of Labor, 2012). Some of the nation's largest companies have been successfully sued by the EEOC under title VII for

improper initiation and use of background checks and blanket employment exclusions for the existence of criminal records including Bank of America, Aramark, Lowe's, Accenture, Domino's pizza, RadioShack, and Omni Hotels ("65 million need not apply," 2014, p. 2).

Approaches to MI Threat Mitigation

Mechanisms for mitigating the MI threat fall into generic categories including technical methods, organizational policies, and procedural methods. Most organizations find it impractical to implement 100% protection from every threat to every organizational resource. Instead they should expend their security efforts commensurately with the criticality of the information or other resource being protected (Silowash et al., 2012).

Policy and Procedural Methods for MI Mitigation. A comprehensive MI defense strategy begins with a technical and business process based upon an insider risk assessment that includes trusted business partners given authorized access to the organizations computing environment (Silowash et al., 2012). "An information technology and security solution that does not explicitly account for potential insider threats often gives the responsibility for protecting critical assets to the malicious insiders themselves" (Silowash et al., 2012, p. 8). Virtually every risk assessment methodology including National Institute of Standards and Technology (NIST) SP 800-30, Control Objectives for Information and Related Technology (COBIT), Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE), and others begins with acquiring an understanding of the business value of the data an organization uses, the processing assets that host the data, and where it is specifically stored (Kouns & Minoli, 2010). "Organizations need to work closely with system administrators to become fully aware of the logical assets contained within each piece of hardware" (Silowash et al., 2012, p. 32).

Having established the critical information assets that need to be protected from MI threats, organizations should clearly document and consistently enforce policies and controls

regarding the use of those assets. Organizations should be particularly clear on policies regarding:

- Acceptable use of the organization's systems, information, and resources
- Use of privileged or administrator accounts
- Ownership of information created as a work product
- Evaluation of employee performance, including requirements for promotion and financial bonuses
- Processes and procedures for addressing employee grievances

(Silowash et al., 2012, p. 13)

Organizations should also "retain evidence that each individual has read and agreed to organizational policies" (Silowash et al., 2012, p. 13). They should also ensure that employees are made aware that they are being monitored for insider activity either through training or pop-ups as it tends to deter malicious activity (Silowash et al., 2012; Caputo et al., 2009).

However, the mere existence of such policies and procedures is not enough. Organizations must anticipate and manage negative issues in the work environment. For example, if management knows in advance that the organization will not be able to provide raises or promotions as expected, they should inform employees as soon as possible and offer an explanation. Additional times of uncertainty and employee anxiety include the end of a contract performance period without any clear indication if the contract will be renewed and any time the organization reduces its workforce (Silowash et al., 2012). External sources of employee stress such as financial and personal stressors are also contributors to MI activity. Cases in the CERT insider threat database show that "financial and personal stressors appear to have motivated many of the insiders who stole or modified information for financial gain" (Silowash et al., 2012, p. 29). In periods of heightened uncertainty or disappointment, the organization should be on

heightened alert to any abnormal behavior and enact enhanced security measures (Silowash et al., 2012).

The behavior of all employees placed in positions of trust with respect to critical organization information cannot be monitored continuously, but "beginning with the hiring process those employees engaging in suspicious or disruptive behavior should be monitored closely" (Silowash et al., 2012, p. 23). Monitoring is particularly appropriate for those employees exhibiting behavioral precursors to insider attack such as threats or boasts about malicious activity, open aggression toward other employees, or excessive work activity during normal off hours with associated large transfers of data. Since financial gain is a motive for fraud, organizations need to be alert to indications from employees of financial problems or unexpected financial gain. Background checks on prospective employees may include previous criminal convictions, a credit check, verification of credentials and past employment. They may also include discussions with prior employers regarding the individual's competence and approach to dealing with workplace issues. "Prior to making any employment decisions based on background information, organizations must consider legal guidance, including EEOC best practices and state and local regulations limiting the use of criminal or credit checks" (Silowash et al., 2012, p. 23).

Research by CERT has indicated that "organizations should have policies and procedures for employees to report concerning or disruptive behavior by co-workers" (Silowash et al., 2012, p. 24). The CERT research report also states organizations ensure that they do not convey a sense of watching over every employee's action, which can reduce morale and affect productivity (Silowash et al., 2012). There can be difficulties associated with effective use of peer reporting. The U.S. Personnel Reliability Program (PRP) began in the 1960's and screens military, civilian

and contractor personnel whose duties give them access to nuclear weapons, components of nuclear weapons, or the codes, computer tapes and communications equipment used to launch them. It is a primary method of countering insider threats (Crow, 2004). In a 1992 report, the Government Accounting Office (GAO) argued that "Efforts to increase the frequency of peer reporting should be undertaken with vigor. This method of gathering information is seen as highly valuable, yet grossly under-utilized due to people's inherent reluctance to report on their friends and associates" (Crow, 2004, p. 4).

The GAO report went on to cite two cases reported on by the U. S. Navy in 1991 which illustrated the need to address peer reporting.

> In one case, an individual committed suicide while on guard duty. Fellow servicemen interviewed after the individual's death stated they did not report the individual's discussion of suicide and reincarnation to his superiors because the individual was always "joking around". In the other case, an individual was known by his peers to carry an unauthorized handgun, drink excessively, and talk about not having a problem killing anyone. This information did not reach PRP supervisors and the individual killed three people before committing suicide. In this case, the Navy investigation concluded that the PRP continuing evaluation process clearly failed to operate properly. (U.S. Government Accountability, 1992, p. 5-6)

To limit the damage malicious insiders can inflict, organizations must make every effort to implement least privilege and separation of duties in their business processes and for technical modifications to systems (Silowash et al., 2012).

> The Principle of Least Privilege states that no entity within a system should be accorded privileges greater than those required to carry out its tasks. For example, a manager

> should be able to authorize an employee's access to a system but does not need the privileges to implement the actual change. For the actual implementation, a system administrator should have the privileges to make the change but only after having received authorization from a manager. Segregation of Duties is a fundamental principle of control that no individual should be able to process a transaction from initiation to completion. In electronic funds transfer systems, for example, two or more individuals are involved in the input and execution of a payment out its tasks. (Ruppert, 2009, p. 9)

One of the challenges to an organization achieving segregation of duties and least privilege is achieving a balance between security and the organization's mission. Smaller organizations may find this difficult because organizational size and funding do not facilitate achieving the proper balance. At some point even larger organizations have to strike a balance between their risk appetite, cost and mission performance. (Silowash et al., 2012)

An organization's "full awareness of access paths available to an insider is critical to being able to disable those access paths when needed" (Moore et al., 2008, p. 15). Unknown access paths provide a mechanism that can be used by the insider to facilitate a future attack, even following termination. The ability to conceal malicious activity by the insider decreases as a function of the unknown access paths (Silowash et al., 2012). The number of unknown access paths is a function of both how an organization discovers unknown paths and how it forgets them. For example, a manager might authorize a software developer's request for the system administrator password during a time of heavy development crating a known access path. If a formal list of employees with access to that password is not maintained, the manager could forget that decision. The manager may also resign from the organization, leaving no

organizational memory of the decision. In either case, the software developer's knowledge of the system administrator password has become an unknown access path (Moore et al., 2008).

MI can also create unknown access paths through any number of system access vulnerabilities such as discovery of unknown system software vulnerabilities, use of a coworker's logged in and unlocked computer, or technical creation of backdoor accounts using password crackers and other hacking type tools. The primary mechanisms for an organization discovering unknown access paths are either through monitoring network traffic or by computer system account auditing. Monitoring of suspicious network traffic can reveal MI activity indigenous to hidden accounts. Account auditing can directly reveal the existence of unauthorized accounts (Moore et al., 2008). For privileged users and system administrators with access to critical system information and processes "organizations should consider implementing the two-person rule, which requires two people to participate in a task in order for it to be executed successfully" (Silowash et al., 2012, p. 50). CERT also recommends centralization of access control functionality as discussed under Technical Methods for MI Mitigation (Silowash et al., 2012, p. 91). With respect to system backup and recovery CERT recommends both separation of duties and use of the two-person rule (Silowash et al., 2012). If an organization deems it necessary to allow the use of removable media in support of its mission, CERT has suggested that authorization for information transfer be limited to a "trusted agent, or at least a second person, using the two-person rule, who reviews, approves, and conducts the copy" (Silowash et al., 2012, p. 91).

Technical Methods for MI Mitigation. Technical means of dealing with MI activity center around support of monitoring for potential MI activity, access control, auditing of user accounts and configuration management and monitoring of the production software baseline

used to support the organization's mission. Many of the tools used to protect organizations from the Advanced Persistent Threat (APT) and other outside threats can be used equally well to monitor for MI activity. Raytheon Corporation cites the necessity of maintaining the ability "to analyze user activity on both the internal network as well as on the endpoint devices. This requires deploying a network device to inspect network traffic as well as agents on individual computers" (Raytheon, n.d., p. 4).

Shabbir Bashir a Program Manager for Identity and Access Management for Verizon has presented methods for employing an open source, real time network Intrusion Detection System (IDS) named Snort to monitor for MI activity on an organization's internal network inside the firewall protecting the interface from the Internet Service Provider (ISP). Bashir recommends using Snort to monitor prohibited activities included in an organization's Acceptable Use Policy (AUP). (Bashir, n.d.) Examples of these activities are:

- Port scanning of internal or external hosts for vulnerabilities.
- Launching a denial of service attack against an internal or external host.
- Setting up unauthorized wireless access points.
- Setting up unauthorized services such as web DHCP and DNS servers
- Surfing the Internet for potentially offensive sites.
- Attempting to log in to a host by using another users network credentials

(Bashir, n.d., vg 10)

Bashir also advocates the use of what he calls Honey Tokens to assist in the monitoring process. A Honey Token "is an information system resource whose value lies in unauthorized or illicit use of that resource" (Bashir, n.d., vg 30). If accessing the Honey Token is in clear violation of the organization's AUP, Bashir claims that IDS detection of network packets containing

references to the Honey Token "can be used to detect insider's accessing information they shouldn't" (Bashir, n.d., vg 31). When using Honey Tokens to attract MI action it is necessary to ensure that potential MI do not have access to information that would alert them to the existence of the Honey Token. They need to perceive the Honey Token as real corporate information. Bashir believes that Snort and associated IDS front ends such as Analysis Console for Intrusion Detection. (ACID) provide "an inherent advantage over closed source IDSs, in that the IDS itself can be tailored and customized for each individual deployment" (Bashir, n.d., vg 4) However, similar results may be attainable with informed use of closed source IDS products in a specific environment. One major issue associated with the many means of technically monitoring for MI activity is the potential for false positives. A false positive is "any normal or expected behavior that is identified as anomalous or malicious" (Owen, n.d., para. 1).

However, an organization's network is not the only means by which information can be exfiltrated. The allowed use of removable media provides many potential avenues for information exfiltration. Raytheon has stated that "The reality is that technologies are readily available now that allow an enterprise to get visibility into previously unmonitored incident vectors such as USB storage, offline activities, or encrypted data" (Raytheon, n.d., p. 1).

In many instances of MI detection the primary means of detection was through "review of system logs" (Keeney et al., 2005, p. 19). Monitoring the large volume of data associated with IDS collected network activity and system logs is often technically supported through the use of Security Information and Event Management (SIEM) software. SIEM systems collect logs and other security-related documentation for analysis, aggregate the data, and provide for correlation and display of the information as useful intelligence through the use of correlation engines which

process multiple forms of data and provide alerts as dictated by rule sets. (Rouse, 2012; Jansen, n.d.)

> The underlying principle of a SIEM system is that relevant data about an enterprise's security is produced in multiple locations, and the ability to look at all the data from a single point of view makes it easier to spot trends and see patterns that are out of the ordinary. (Rouse, 2012, para. 2)

Most SIEM systems work by "deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers, network equipment, and even specialized security equipment like firewalls, antivirus or intrusion prevention systems" (Rouse, 2012, para. 3). Effective use of SIEM capabilities requires baselining of normal network activity to provide a basis of comparison to anomalous events. (Sawyer, 2011) FBI CISO Patrick Reidy recommends "a minimum of six months of baseline data prior to even attempting any detection analysis" ("5 Lessons from," 2013, para. 15). "SIEM systems are typically expensive to deploy and complex to operate and manage" (Rouse, 2012, para. 5).

> System logs will build up very rapidly so it is important to establish filters or alerts to notify security teams in the event of a critical change or incident. Due to the overwhelming amount of data that can be logged, these filters should be tuned to ignore standard business operations but highlight anomalous activity. This can be a very difficult task that will require some highly trained individuals and will require a serious investment of time. Having a tool may help with some of this noise reduction but it will still be a challenging task regardless because every business and infrastructure is slightly different. (Ruppert, 2009, p. 24)

CERT calls filter and rule sets employed by a SIEM signatures. They state that signatures should be designed to be applied to a particular user or group of system users based upon behavioral precursors exhibited in the organization's environment. They state that "signatures are not intended to be applied to all users across the enterprise, as doing so will generate a large number of false positives" (Software Engineering Institute, 2012, p. 3).

With respect to network endpoint management, CERT studies indicate that "remote access provides a tempting opportunity for insiders to attack with less perceived risk" (Silowash et al., 2012, p. 60). Mobile devices are not new to organizations, which have historically relied upon laptops and cell phones provided by the organization for quick access to corporate email or sensitive company information while on the go. However, with more employees demanding to use a device of their choosing, a practice known as Bring Your Own Device (BYOD), the risk of malicious insider activity may increase. The CERT Insider Threat Center sees mobile devices as an emerging attack platform for malicious insiders stating: "Organizations may provide remote access to email and noncritical data, but they should strongly consider limiting remote access to the most critical data and functions and only from devices that are administered by the organization" (Silowash et al., 2012, p. 60).

"Gaps in access control have often facilitated insider crimes. Employees can easily circumvent separation of duties if they are enforced by policy rather than by technical controls" (Silowash et al., 2012, p. 41). "Organizations must prevent employees from gaining online access to information or services that are not required for their job" (Silowash et al., 2012, p. 41). Logical access controls are technical methods of implementing access control policies defined in terms of subjects, the objects upon which those subjects are allowed to perform operations, and in some cases the environment in which those operations can be performed. A subject is either a

human or a non-person entity such as an autonomous service or application. Major differences between technical access methods affect the ease with which each method can be established and maintained as well as the flexibility of the method in adapting to unanticipated new subjects.

Access control systems implementing a Mandatory Access Control (MAC) policy provide "A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e. clearance) of subjects to access information of such sensitivity" (Ferraiolo & Kuhn, 1992, p. 3).

> An example of such a system would be a multi-level security system based upon the individual subject's security clearance and the security classification of the objects (Secret, Top-secret, etc.). MAC security policies provide tight security control because they can only be modified by a system administrator, but the requirement for fixed object labels makes them less flexible when interfacing with external systems that may not conform to their labeling conventions and more labor intensive for system administrators. (Jansen, n.d., para. 4)

Discretionary Access Control (DAC) policies provide "A means of restricting access to objects based on the identity of subjects and/or groups to which they belong" (Ferraiolo & Kuhn, 1992, p. 2). DAC permits the granting and revoking of access privileges to be left to the discretion of the individual users (Ferraiolo & Kuhn, 1992). DAC is not highly secure because "it cannot prevent one authorized user from copying a piece of information and then allowing another subject (whom previously might not have the appropriate rights) access to that information" ("Security models strengths," n.d., para. 3). Therefore, its use does not readily support technical enforcement of separation of duties.

In Role Based Access Control (RBAC) policies, access decisions are determined by the roles individual users take on as part of an organization. Roles are usually assigned on the basis of duties, responsibilities, and qualifications. This allows for more fine-grained control of access that supports separation of duties. Unlike DAC policies, under RBAC access controls "users cannot pass access permissions on to other users at their discretion" (Ferraiolo & Kuhn, 1992, p. 3). RBAC also supports a hierarchical structure, which allows supervisory roles to inherit the permissions of the roles beneath it. (i.e. a supervising programmer inheriting permissions of his subordinate programmers)" ("Security models strengths," n.d.). While RBAC has some distinct advantages in terms of its fine grained support of separation of duties, "the implementation of RBAC is different in every operating system" (SANS Institute, 2014, p. 6). There is currently little or no standardization for implementation. This makes single console management and compliance difficult in enterprises that must administer heterogeneous systems. As networks grew, the need to limit access to specific protected objects spurred the growth of Identity Based Access Control (IBAC) capabilities. IBAC employs mechanisms such as Access Control Lists (ACLs) to capture the identities of those allowed to access the object. If a subject presents a credential that matches the one held in the ACL, access is granted to the object. Individual privileges of the subject to perform operations are managed on an individual basis by the object owner. Each object needs its own ACL and a set of privileges assigned to each subject. In the IBAC model, the authorization decisions are made prior to any specific access request and result in the subject being added to the ACL (Hu et al., 2014). Management of RBAC and IBAC access control engenders a good deal of administrator and object owner overhead labor and is "often cumbersome to manage" (Hu et al., 2014, p. 5).

Attribute Based Access Control (ABAC) is a logical access control policy where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environmental conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes (Hu et al., 2014). ABAC "avoids the need for explicit authorizations to be directly assigned to individual subjects prior to a request to perform an operation on the object" (Hu et al., 2014, p. 6). Moreover, this model enables flexibility in a large enterprise where management of access control lists or roles and groups would be time consuming and complex. Over the past decade, vendors have begun implementing Attribute Based Access Control (ABAC) like features in their security management and network operating system products, without general agreement as to what constitutes an appropriate set of ABAC features.

Due to the lack of consensus on ABAC features, users cannot accurately assess the benefits and challenges associated with current ABAC implementations, especially with respect to interoperability. However, until January of 2014 when NIST published its Guide to Attribute Based Access Control (ABAC) there has not been a comprehensive effort to formally define or guide the implementation of ABAC within the federal government (NIST Computer security, 2013). Additionally, vendors of ABAC like solutions (e.g. Axiomatics) have indicated that unless the ABAC is architected correctly "it will lead to performance issues, especially if fine grained access is being sought" (StackExchange, 2014, para. 3). The Gartner Group is optimistic about the evolution of ABAC recently stating that ABC is the way to go and predicting that "70% of businesses will adopt ABAC by 2020" (Avatier.com, 2014, para. 9).

"Authentication is a process that ensures and confirms a user's identity" (Janssen, Authentication, n.d., para 1). Authentication is related to access control because it is a gating

process where the subject must prove their access rights and identity. For extremely sensitive system operations, such as backup and recovery, authentication also provides the necessary technical credentials for effective implementation of separation of duties and for operation authorization, or execution of two person control operations. In order to institute stringent access controls on privileged users and system administrators CERT recommends that organizations use multifactor authentication for privileged user or system administrator accounts stating that "Requiring multifactor authentication will reduce the risk of a user abusing privileged access after an administrator leaves the organization, and the increased accountability of multifactor authentication may inhibit some currently employed, privileged users from committing acts of malfeasance" (Silowash et al., 2012, p. 51).

Multifactor authentication is also recommended by CERT for controlling and monitoring remote access. (Silowash et al., 2012)

Two factor authentication is the most commonly used form of multifactor authentication. Two factor authentication requires a user to have two out of three types of credentials before being able to access an account. The three types of credentials are:

- Something you know, such as a personal identification number password, or a pattern.
- Something you have, such as an ATM card, Common Access Card (CAC), RSA SecurID token, or electronic key fob etc.
- Something you are such as a biometric like a fingerprint, retina scan, or voiceprint.

(Rosenblatt, 2013).

Overuse or injudicious application of two factor authentication can be problematic with respect to the overhead it requires with respect to device accountability, cost, and organizational

efficiency. Additionally two factor authentication can be hacked, especially in password recovery scenarios (Rosenblatt, 2013).

In order to facilitate easy creation, management, and especially removal of access privileges and authentication mechanisms it is advisable to centralize control over these security mechanisms. Multiple access and authentication databases within an enterprise exacerbate secure maintenance of access control and facilitate the creation of unknown access paths. Centralization of control can be achieved by various means including use of Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-in User Service (RADIUS), or Terminal Access Controller Access Control System (TACAS) protocols to coordinate communication between and control of multiple access or authentication information repositories. With centralized control all accesses can be removed simultaneously from the same centralized control point when an employee is terminated (Silowash et al., 2012).

In order to prevent technically competent system users who might gain unauthorized privileged or administrator access, or who might already have been granted such access, from creating backdoor access paths in an organization's production software baseline, tools supporting strict configuration management of an organization's production software baseline and online monitoring of the executing production software may prove necessary. Software Configuration Management (SCM) tool capabilities vary depending upon which part of the software life cycle they are required to support. For example, during software development when the baseline changes rapidly, SCM tools need to provide strict version control so that independent software coders can have the latest versions of their code modules integrated successfully into a development build. Examples of development phase, open source SCM tools with version control are Subversion, git and Mercurial (hg) (Wheeler, 2005, para. 1.2, 4.9, 4.10).

Once software builds demonstrate sufficient maturity through beta trials or testing to be deployable the SCM modules need to support verification that the build, as installed, consists of the correct versions of software modules and that these versions are authorized and contain no independently installed functions or log access modifications. Once deployed the software baseline stabilizes over time and must be maintained through implementation of version controlled changes and continual monitoring to ensure that installed versions have not been changed in an unauthorized manner. CERT has indicated its studies have revealed:

> Some insiders have attacked by modifying source code during the maintenance phase of the software development lifecycle. However, once the system is in production and development stabilizes, some organizations relax the controls, leaving a vulnerability open for exploitation by technical insiders (Silowash et al., 2012, p. 53).

In addition to procedural efforts to conduct peer reviews and vetting all changes through a Configuration Control Board (CCB), organizations need tools to assist with "review of CCB baselines against actual production systems and determination if any discrepancies exist" (Silowash et al., 2012, p. 55). Moreover, Payment Card Industry Data Security Standards (PCI-DSS) Requirement number 10.5.5 states that organizations must use file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts. PCI-DSS requirement number 11.5 states that organizations must deploy a change detection mechanism to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly (Mehta, 2014).

Open source software implementations like Ubuntu Linux use extensive peer review and package management systems like the Advanced Packaging Tool (APT) that enforce

configuration baseline control through the use of cryptologic hashes and digital signatures to ensure the baseline integrity of system builds including new applications that are developed as open source implementations. “A cryptologic hash function, checksum, or digest is a one-way function which depends on all bits of the file being sealed such that any change to the file, even a single bit, will alter the resulting computed checksum” (Pfleeger & Pfleeger, 2011, p. 79-80). Several commercially based products provide cryptologic hash based software versioning and configuration management with digital signatures. A digital signature is a mathematical technique used to validate the authenticity and integrity of the software. Many digital signatures employ public key encryption to create two keys, one private and one public that are mathematically linked. The private key is then used to encrypt the cryptologic hash used to secure the software file. The encrypted hash along with other information like the hashing algorithm used to secure the data constitutes the digital signature which is decrypted upon receipt using the public key. (Rouse, 2014)

Some commercially based SCM systems also provide File Integrity Management (FIM) capability. A FIM agent sits on a host and provides real time monitoring of files. The FIM agent has the capability to detect unauthorized changes and the capability to report what has been changed and who has changed it. For files expected to change rapidly during software execution, such as log files, the hash values of user access permissions are monitored since they are not expected to change often (Mehta, 2014).

An example of a commercial configuration management tool with FIM capability is Tripwire Enterprise 8.3 (“Tripwire Enterprise 8.3,” 2013). Some other Tripwire product competitors offering integrated SCM and FIM compliance are “Windows File Integrity, Symantec Data Loss Prevention, and LogRhythm” (Lepofsky, 2011, para. 6). To date “too many

organizations have failed to implement FIM for fear of the additional work load created by a system that flags every single unauthorized change" (Kedgley, 2014, para. 12) Mark Kedgley Chief Technology Officer (CTO) of New Net Technologies, an IT security solutions company, disagrees stating "Combining FIM with effective change management and a consistent build standard not only fundamentally reduces the security risk but it also minimizes the risk of downtime created by unauthorized or misguided system changes" (Kedgley, 2014, para. 13). However, Mr. Kedgley's own statement acknowledges that implementing organizations need to have mature software development and maintenance practices and discipline exhibiting effective change management and a consistent build standard. For some organizations tools predicated on a mature software culture may not be turnkey enough to make a difference.

Discussion of Findings

Research Problem Review

This study endeavored to focus attention upon how to address MI threats. These threats consist of employees, contractors, or business partners who either currently have authorized access, or have had authorized access to an organization's critical information and have intentionally misused that access in a manner that compromised the organization. Other studies by both government and commercial organizations have shown that both large and small organizations have demonstrated an insensitivity to the seriousness of information compromises such as unauthorized access to and disclosure of confidential data, execution of fraudulent transactions, and sabotage of systems and data until they suffer major financial loss as a result of these breaches of information security. Studies have also highlighted the shortage of information available about MI activity and the failure of organizations to report MI incidents. This study attempted to embrace understanding of how to deal with MI threats through: understanding of

who comprises the MI threat; MI motives for and methods of attack; determining if an MI profile can be defined or modeled to enable MI identification to support avoidance of attacks; examination of legal considerations associated with using insight obtained by profiling, modeling, and other methods to identify potential MI threats; and aggregating useful procedural and behavioral mitigation methods based upon the current best understanding of the MI threat.

Literature Review Efforts

The literature review presented available open source publications and media resources that could lend insight into the research questions re-articulated in the Research Problem Review section; namely, available information on the demographics, motivation and methods associated with MI activity, information associated with efforts to profile or model MI characteristics for purposes of identification, information on legal issues associated with the use of MI identification information, and information on procedural and technical mitigation methods. The information available on MI activity is vast and defies exhaustive review. However, initial review of information available implied that the key to understanding and mitigating the MI threat hinges around understanding the dynamic relationship between individual employees, the information processing systems they use to conduct everyday business, the organizational work environment created by employers, and the legal, economic, and ethical environment in which they coexist.

Little definitive open source information discussed the economic and ethical environment effects on MI activity other than to state that the trend was toward an increase in MI activity is usually associated with worsening economic conditions. However, in spite of a lack of reporting of MI incidents CERT and the FBI seem to have access to data from empirically derived case information. Of the two organizations CERT appears to have published more detailed

information regarding how their study results were derived from database information. However, overall conclusions regarding MI activity seem to be relatively consistent between CERT and the FBI. Information on technical MI monitoring and mitigation methods was available from a variety of government and commercial sources.

The sources used in this study were chosen to provide the most comprehensive insight into how technical methods can complement organizational policy and procedures to deal with currently known difficulties in dealing with the MI threat. These issues arise from the dynamic interaction between employers, employees, and the work environment that produce MI activity. The key insights derived from the literature review with respect to MI activity and methods of mitigation are:

- MI Motives and Methods are Highly Variable Requiring Tailored Solutions.
- MI Profiling and Modeling have not Made MI Identification Consistent and Repeatable.
- Legal Limitations Exist to Screening Employees for MI Tendencies.
- Active Management Participation is Essential for MI Mitigation.
- Selective, Precursor Initiated, Activity Monitoring and Peer Reporting are Essential.
- Minimizing Unknown Access Paths through Account Auditing is Essential.
- IDS and SIEM Tools Contribute Significantly to Effective Monitoring.
- RBAC, Two-factor Authentication, and Two Person Control Helps Eliminate Access Control Gaps.
- Software Baseline Control Using SCM and FIM Tools Helps Prevent Unauthorized Change.
- Mitigation Must Address the Power of the Insider Position.

Each of these insights is discussed below including an assessment of what was learned from the literature review, limitations encountered, and new perspectives synthesized.

MI Motives and Methods are Highly Variable Requiring Tailored Solutions

The results of this study with respect to motives and methods are predicated upon results of CERT, and FBI studies. The motives for MI activity are usually highly personnel and a function of personal predispositions, outside the workplace conditions, and the dynamic relationship between employees and the work environment created by organizational management. Results of CERT studies have pointed to the buildup of employee disgruntlement due to unmet or thwarted expectations while FBI studies have cited factors which are fundamental personal predispositions to MI activity such as inability to work with others (Cappelli et al., 2008; "5 Lessons from," 2013). In the IT&T sector and in cases of sabotage of CI the primary motive for MI activity was revenge (Keeney et al., 2005). In the B&F and government sectors the primary motive was financial gain (Kowalski et al., 2008).

Results from CERT and FBI studies have confirmed that the methods employed by MI differ markedly between technical sectors and B&F and government sectors. While the majority of the methods employed in all sectors are often not highly technical in nature, MI in the more technical sectors usually involves compromise of an organization's computing resources (Keeney et al., 2005). On the other hand, MI incidents in business and government sectors usually involve using corporate processing resources in authorized ways while taking advantage of weaknesses in an organization's business processes instead of compromising the organization's computing systems. (Kowalski et al., 2008) These studies also noted that managers in the financial sector were also able to alter business processes in order to profit financially and remain undetected longer (Cummings et al., 2012).

Therefore, methods of monitoring financial insider activity with respect to behavioral/offline or technical/online precursors of fraudulent activity are likely to be

significantly different and more process dependent than for technical occupations. These facts suggest that methods of dealing with MI activity must be tailored to the specific needs of an organization as dictated by its operating environment. As a result, solutions to the MI problem must be derived for each organization as a function of an insider security risk analysis (Silowash et al., 2012).

MI Profiling and Modeling have not Made MI Identification Consistent and Repeatable

The research conducted in this study indicates that despite the best efforts of the FBI and MITRE to produce either a profile or an analytical model that identifies MI activity and the efforts of CERT to employ systems dynamic modeling of the complex behavioral interaction between individuals, systems and organizations, definitive models capable of consistently predicting malicious insider activity are currently non-existent (Senator et al., 2013; "5 Lessons from," 2013; Caputo et al., 2009). As stated previously, the variability in MI motives for attack spans the gamut of human psychology. Attack triggering events and time until attack occurrence are dictated by the dynamic interaction between factors such as MI expectations and organizational sanctions imposed in response to behavioral precursors. MI demographics are distributed in the range of 17 to 60 years of age, and with the exception of cases of sabotage of CI, are evenly distributed between mem and women (Randazzo et al., 2005; Kowalski et al., 2008). Levels of access vary from highly privileged system administrators to low level users with only standard access, and methods of attack vary from sophisticated use of scripts and hacking tools to use of forgotten or overlooked shared accounts or unattended co-workers computers left unlocked (Moore et al., 2008; Cummings et al., 2012).

The results of this study are predicated upon review of information from CERT, DOD, MITRE and FBI studies. The results of DOD modeling under the PRODIGAL program indicated

that significant signal to noise issues exist with the use of predictive analytics to identify MI activity (Senator et al., 2013). Those findings were corroborated by the MITRE study (Caputo, et al, 2009). CERT efforts expended on systems dynamic modeling produced insights into behavioral aspects of MI activity and resulted in lessons learned that can be applied by organizations to better monitor for and prevent MI activity, but were not designed to predict MI activity, or identify insiders (Moore et al., 2008). The CERT MERIT modeling effort was necessarily limited to information relative to insider sabotage of CI and subsequently correlated to espionage operations in order to accommodate DOD information needs. The database used by CERT as the definitive basis for its modeling and simulation efforts is limited by the lack of reporting on MI activity discussed in the Justification for Research section and consists of only 700 cases. (Cummings et al, 2012). Therefore, the empirical data available for modeling may not be statistically relevant. Both FBI and MITRE findings have indicated that modeling and analysis efforts to date have failed to employ rigorous scientific methods such as double-blind experiments and control groups to minimize the potential for bias. (Caputo, et al, 2009; "5 Lessons from," 2013). Nevertheless, modeling and analysis efforts to date have provided valuable insight into the dynamic interaction between employees, the processing systems they employ, and the organizations within which they function (Moore et al., 2008).

Legal Considerations Exist when Screening Employees for MI Tendencies

Even if definitive models did exist for MI identification, the ability of employers to pre-screen applicants for employment based upon questioning of employment applicants relative to traits identified by the model is legally limited by the American with Disabilities Act. Even after an offer of employment is tendered employers must be careful that questions asked during post hiring medical examinations are job-related and consistent with business necessity (Equal

Employment Opportunity, n.d.). The EEOC reviews cases referred to its attention under either the disparate treatment or disparate impact frameworks of Consideration of Arrest and Conviction guidelines to ensure that any rejection of employment is based upon qualification for the position in question and is consistent with business necessity (Equal Employment Opportunity, 2012). The EEOC has sued major U.S. corporations for violations under both the disparate treatment and disparate impact frameworks for violations of Article VII of the American Civil Rights Act. As a result, organizations must take these legal considerations under advisement when employing the results of background checks or the existence of personal predispositions to MI activity into their employee screening processes (Silowash et al., 2012).

Active Management Participation is Essential for MI Mitigation

Process and procedural methods of MI mitigation depend upon definition of, follow through, and consistent application of corporate policy as well as management ability to anticipate and deal with adverse events indigenous to the business environment. Failure of organizations to effectively deal with the MI threat risk leaves MI threat mitigation to the MI. Mitigating the threat begins with analysis and identification of the critical information to be protected. Implementation of the principles of least privilege, separation of duties as well as effective management of system access require continuing vigilance and ongoing effort from managers, IT professionals and the employees themselves. The process and procedural methods for mitigation of MI activity identified in this study are predicated upon lessons learned from CERT modeling activity, and lessons learned from analysis of ITS reports developed from cases resident in the CERT Threat Data Center. The environmental contexts in which these lessons apply are highly variable and as a result each organization must tailor these lessons to its own operational environment, resources, and risk appetite. The general principles of cyber risk

analysis apply. The upshot is that mitigation of MI activity is directly related to the corporate policies, procedures and culture created by management. Unless the created corporate culture emphasizes the importance of and invests continual vigilance toward management of the MI threat the threat of MI activity will remain high (Silowash et al., 2012).

Selective, Precursor Initiated, Activity Monitoring and Peer Reporting are Essential

Continuous monitoring of all employees for evidence of MI activity is a practical impossibility for the vast majority of organizations. Therefore, the existence of behavior or technical precursors should be taken as a queue to begin behavioral and technical monitoring of employees on a selective basis (Silowash et al., 2012). Information derived through this study indicates that CERT ITS reporting and GAO reporting on the health of the DOD nuclear weapons PRP have suggested the increased use of peer reporting as a means of early MI identification (Crow, 2004). ITS reporting notes that in almost all cases other employees knew of and did not report MI activity. The GAO found that in the U.S. Navy PRP people were reluctant to engage in peer reporting based upon a natural reluctance to inform upon their friends and associates. The GAO also cited fatal results for some Navy co-workers when peers failed to report behavioral precursors (Crow, 2004). The potential high payoff associated with peer reporting suggests that the psychosocial aspects of and organizational cultural issues associated with peer reporting need to be studied further in an effort to overcome employee aversion to this practice while maintaining high organizational morale.

Minimizing Unknown Access Paths through Account Auditing is Essential

In accordance with CERT case studies many MI attacks occur after employee termination through the use of remote access and user access privileges that for one reason or another have become unknown to the organization. CERT ITS reports show that MI identity, and the access

paths used by MI, are usually discovered through review of system logs and auditing of user accounts (Moore et al., 2008). Unknown user accounts are not always created through MI technical, clandestine efforts. Many unknown access paths are actually created when system administrators grant legitimate access in support of increased effort or work scope, and then fail to remove personnel from access after their participation is no longer required. Corporate memory with regard to accesses granted is often erased through employee transfer or termination. Due diligence must be exercised through periodic audits conducted for the express purpose of reducing access privileges that are no longer required. Upon termination, transfer or retirement of employees organizations need to ensure that known access paths for the employees are terminated (Silowash et al., 2012).

IDS and SIEM Tools Contribute Significantly to Effective Monitoring

While CERT findings have shown that organizational policy and procedures should employ network monitoring and system log correlation to detect MI activity and associated unknown system access paths, the sheer volume of network traffic and system log information can combine to make effective monitoring difficult at best. System security professionals in both commercial and government organizations have recommended the use of IDS systems and SIEM software to assist in these efforts (Rouse, 2012). However, there are false positive downsides associated with the use of these tools if due diligence is not exercised in narrowing the scope of their employment to responding to specific MI behavioral and technical precursor activity. (Software Engineering Institute, 2012). Additionally, IDS and SIEM tools can be costly. Organizations should engage in careful risk mitigation trade-off analysis when deciding if the use of these tools provides sufficient return on investment with respect to the information they

are trying to protect. Consideration should be given to employment of open source tools to reduce cost. (Bashir, n.d.)

RBAC, Two-factor Authentication, and Two Person Control Mitigate Access Control Gaps

Studies have shown that access control systems employing RBAC access control polices can provide fine grained access control while retaining reasonable flexibility for system administrators in responding to changing access needs. They provide significantly greater flexibility than do label based MAC type systems, and do not allow users to grant access control as is the case with DAC type systems (Ferraiolo & Kuhn, 1992). However, they must be carefully integrated into an organization's computing environment because they often employ unique, non-standard interfaces resulting in difficulty in addressing heterogeneous system interfaces within the environment (SANS Institute, 2014).

Recent developments of ABAC type control systems show promise in providing even more flexibility in adapting to change than RBAC systems. However, lack of definitive requirements for ABAC system development has resulted in integration issues similar to the integration issues associated with RBAC systems. Additionally, information from ABAC system developers indicates that these systems have exhibited performance issues when implementing fine grained access control (StackExchange, 2014). In any event RBAC systems have helped improve the management of user access privileges, in spite of the need for careful system integration.

For the most sensitive administrator user accounts two factor authentication can be used in conjunction with separation of duties to minimize the possibility of unauthorized operations (Silowash et al., 2012). However, overuse of multiple authorization personnel and two factor authentication tools can result in poor organizational performance with respect to mission

requirements. In the end it is incumbent upon the implementing organization to integrate tools and processes in a cost effective and technically feasible fashion. If the use of access control and authentication tools is deemed not cost effective for the information to be protected, the organization must be prepared to prevent the creation of unknown access paths through manual audits.

Software Baseline Control Using SCM and FIM Tools Mitigate Unauthorized Change

CERT has indicated that defending against the most technically sophisticated MI attackers with privileged or administrator access to an organization's operating software requires strict management of the software baseline. The use of SCM tools and online executing FIM tools can provide detection and alerting to attempts to modify software or file access privileges without authorization (Silowash et al., 2012). For organizations processing credit card data PCI-DSS standards require the use of FIM capability (Mehta, 2014). Effective use of SCM and FIM tools requires strict software development discipline and effective integration to prevent false positives, and the tools can be costly. In non-compliance situations, employment of these tools, like many other countermeasures, is a risk analysis and mitigation decision requiring tradeoff of the risk of MI incidents against the value of the information to be protected (Kouns & Minoli, 2010). Nevertheless, employment of these tools can be effective in implementing CERT recommendations and PCI-DSS requirements for ongoing review of software baselines against actual production systems and determination of the existence of discrepancies.

Mitigation Must Address the Power of the Insider Position

While the use of technical monitoring tools is an essential element of a comprehensive MI mitigation strategy it must be remembered that the use of these tools is controlled by insiders. When misused by trusted insiders the output of these tools can be manipulated to cover up

malicious activities. Eventually, any organization has to rely upon the performance of some trusted cadre of personnel augmented by process and procedure. In a very real sense the power of the insider position cannot be over emphasized.

An example of that power is provided by the espionage case of FBI agent Robert Phillip Hanssen. In several incremental activity periods from 1978 through 1999 Hanssen became an increasingly important player in the FBI counterintelligence program. During an increment from 1985 through 1987 he set up the FBI Intelligence Investigative System giving him access to the true names of every FBI intelligence source in New York. He sold these names along with many highly classified FBI documents to the Soviet KGB resulting in the deaths of at least two double agents. His insider position made him responsible for participating in sensitive FBI counterintelligence operations giving him access to information that enabled him to remain undetected as the second mole sought by the FBI after uncovering of Aldrich Ames in 1992. He managed to remain below the FBI detection threshold until he was betrayed by KGB agents who turned over information compiled by him in 1999 even though the KGB agents were unaware of his identity. The detailed information was eventually internally correlated by the FBI and led to his detection and conviction of espionage. Review of the Hanssen case revealed weaknesses in FBI organizational processes and procedures that enabled Hanssen to use his insider position to avoid detection. (McGeary, 2001)

Recommendations

Improve the Accessibility of a Reference Body of Knowledge

Several studies have addressed the limited body of knowledge with respect to insider threat incidents and the associated problem of reluctance on the part of organizations experiencing insider problems to provide detailed reporting information. Detailed information is

essential to deriving practical lessons learned for practitioners. The slow pace of incident reporting suggests that an opportunity exists to build upon the good work already accomplished through creation of the CERT Insider Threat Center database. Adding to the core set of 700 cases that currently exist in the database should be accomplished in a standardized fashion. A logical first step is the development of a standard question template for conducting interviews with principal parties involved in investigating an incident. The reporting organization, any forensic or legal investigators employed by that organization and as necessary, employees involved and law enforcement are all excellent sources for template development. Leveraging CERT experience in developing standardized questions may prove effective based upon their experience with the existing database.

Next a standardized approach to case coding is essential. Once again leveraging existing CERT case codebooks currently used to codify information in the CERT Insider Threat Center database may provide the standardized templates needed to achieve consistency for each new case entered. Finally, a standardized interface for technical access to the database should be provided along with appropriate user documentation. Any standardized, commercial access method such as Structured Query Language (SQL) or de facto commercial products such as Microsoft Access will probably prove acceptable. As new incidents are reported the use of the standardized templates and interfaces can be leveraged to produce accessible data for future studies to all interested organizations.

Future Structured Experiments are Needed

While the extensive case study and modeling research conducted over the last decade has provided key insights into MI motivations, methods of attack, and potential mitigation techniques, there is a finite danger that biases exist in the results derived because standard

scientific methods such as the use of control groups have not been employed. Both the FBI and MITRE have suggested significant errors can occur when experimentation focuses on the MI exclusively without comparison against a model for "normal" behavior. Although it is expensive, consideration should be given to creating a set of structured experiments for insider activity for the sabotage of CI, IT&T, B&F, and government sectors as a minimum. The results of these experiments could be used to verify the validity of previous results obtained from previous experimentation and eliminate biases if necessary.

Future Research is Needed to Promote Effective Peer Reporting

Multiple studies have shown that in almost every case other people, both inside and outside the organization, knew of MI activity during both planning and execution stages. Programs such as the DOD PRP have in the past successfully made use of peer reporting as a means of identifying the potential for MI activity. Based on the literature review, there is no denying that in today's current social and ethical environment the effectiveness of peer reporting methods have decreased. However, the potential high pay off in terms of minimization of both organization and employee damage suggests the need to investigate the psychosocial issues associated with overcoming employee reluctance to report on their friends and co-workers. Development of effective leadership techniques for employing peer reporting while maintaining organizational morale can potentially provide a more effective means of detecting the potential for MI activity and mitigating its adverse effects.

Documentation of Access Control and Behavioral Monitoring Tools is Necessary

Studies have established the general effectiveness, expense, and integration issues associated with the use of IDS and SIEM software. The same is true of SCM and FIM tools. However, organizations seeking to employ these tools need detailed information with which to

trade off capabilities against the integration and maintenance efforts required to maintain effective monitoring. The current state of practice requires each organization to investigate all aspects of a tool's functionality, effectiveness, integration issues, and interoperability with other tools for each tool it may consider using for access control, log and network monitoring, software configuration management, and file integrity management. The currently available source for this type of data is marketing information from individual tool vendors.

Organizational cybersecurity staffs would benefit significantly from a website similar to the Computer Forensics Tool Catalog maintained by NIST where functional capability, integration and effectiveness information could be maintained about available IDS, SIEM, SCM, FIM, and access control tools. Establishment of such a website would require effort to develop a taxonomy of functions and technical parameters similar to the one developed by NIST for forensics tools as well as a search feature to find tools and description pages for vendors to input information about their tools. Research is required to establish an acceptable functional taxonomy for the various tool categories as well as a comprehensive, standardized way for vendors to describe their tools. Additional research could provide a set of functional standards against which tools could eventually be tested. At additional expense and effort a website similar to the Department of Homeland Security's CyberFETCH website would provide a forum for the exchange of documents, blogs, questions and answers, product reviews, and test results for these monitoring tools. The resulting repository of information would provide a codified body of knowledge upon which security organizations can draw when making tradeoff decisions.

Continue Analytic and Behavioral Modeling Research

Analytic and behavioral modeling efforts to date have not produced consistent and repeatable indications of MI activity. Behavioral modeling conducted by CERT was not intended

to predict MI activity instead focusing on understanding the nature of interaction between potential MI employees, their predisposition to MI activity and the effect of organizational constraints and the business environment upon their behavioral tendencies. Additionally, executable computer models were developed only for IT&T and sabotage of critical infrastructure contexts. However, the behavioral insights gained through system dynamic modeling have indicated that focusing on employee monitoring in response to behavioral precursors has payoffs with respect to detecting and preventing MI incidents. Procedural and technical mitigation techniques have evolved from these modeling efforts.

Analytic modeling has suffered from signal to noise issues between malicious and non-malicious activity. However, limited success has been achieved when analytic techniques are used in conjunction with structured experiments employing control groups of benign users as well as malicious actors. Given the relatively few operational contexts examined using predictive analytics in conjunction with controlled experiments additional efforts are warranted to determine if these techniques can produce consistent indicators unique to MI activity that do not require re-development for each organization and operational environment examined. Additionally, analytic examination of data baselines collected in response to behavioral precursors may benefit from improved signal to noise ratios as opposed to normal standard volume collection of information. The ability to follow through on both behavioral and predictive analytic modeling in a structured experiment environment is "expensive and time consuming" (Caputo et al., 2009, p. 19).

Conclusion

This study endeavored to focus attention upon how to address MI threats. These threats consist of employees, contractors, or business partners who either have authorized access, or

have had authorized access to an organization's critical information and have intentionally misused that access in a manner that compromised the organization. The study attempted to embrace understanding of how to deal with MI threats through: understanding of MI demographics, motives for and methods of attack; determining if an MI profile can be defined or modeled to enable MI identification and avoid attacks; determination of legal considerations associated with using insight obtained by profiling and modeling to identify potential MI threats; and aggregating useful procedural and behavioral mitigation methods based upon the current best understanding of the MI threat. Review of available open source publications and media resources has revealed that indeed the insider threat is difficult to identify. MI demographics provide no effective identifying clues and models have failed to consistently predict their identities. Legal considerations must be addressed to effectively prescreen prospective employees for MI tendencies. Finally, detecting and mitigating MI activity requires MI oriented risk assessment, eternal vigilance and investment. In short, dealing with the MI threat requires easily as much, if not more, intensive effort than dealing with the external threats.

At this point it is beneficial to remember the admonition of G.K. Chesterton who stated "If a thing is worth doing, it is worth doing badly". That is to say even though dealing with the MI threat seems a daunting task the cybersecurity community has no choice but to put forth its best effort. Studies have shown that MI threats, even though few in number, cause a disproportionate degree of damage. The research conducted in this study has shown that techniques for detecting and mitigating the threat are available and can be effectively applied albeit with due diligence and effort. Some of these procedural and technical methods include definition of, follow through, and consistent application of corporate policy as well as anticipation of and dealing with adverse events indigenous to the business environment. Other

methods include conduct of a comprehensive MI risk assessment; selective monitoring of employees in response to behavioral precursors using tool such as IDS and SIEM software; minimizing unknown access paths through account auditing; effective management and control of the organization's production software baseline using SCM and FIM tools; and effective use of peer reporting. Additionally, this study identified recommendations for future research and expansion of the utility of the existing database of MI knowledge. In the final analysis addressing the MI problem is like many other cybersecurity issues. It requires continuing effort from dedicated and knowledgeable professionals to achieve success.

References

5 Lessons from the FBI insider threat program. (2013). Retrieved from http://www.darkreading.com/vulnerabilities---threats/5-lessons-from-the-fbi-insider-threat-program/d/d-id/1139281

65 million need not apply. (2014). Retrieved from http://www.nelp.org/site/issues/category/criminal_records_and_employment/65 Million "Need NotApply"

American Chesterton Society (2014). A thing worth doing. Retrieved from http://www.chesterton.org/a-thing-worth-doing/

Avatier (2014). Attributes Are Now "How We Role". Retrieved from http://www.avatier.com/products/identity-management/resources/gartner-iam-2020-predictions/

Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., & Shaw, E. D. (2006). *Comparing insider IT sabotage and espionage: A model-based analysis* (CMU? SEI-2006_TR_026). Retrieved from Software engineering Institute: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8163

Bashir, S. (n.d.). *Using an open source intrusion detection system to detect and protect from insider attacks* [Lecture notes]. Retrieved from http://academy.delmar.edu/Courses/ITSY2430/eBooks/Snort (anOpenSource-IDS).pdf.

Beal, V. (2014). Predictive analytics. Retrieved from http://www.webopedia.com/TERM/P/predictive_analytics.html

CBS news (2014). Navy kicks out 34 on nuclear training test. Retrieved from http://www.cbsnews.com/news/navy-kicks-out-34-for-cheating-on-nuclear-training-tests/

Cappelli, D., Desai, A. G., Moore, A. P., Shimeall, T. J., Weaver, E. A., & Wilke, B. J. (2008). Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System. Retrieved from http://resources.sei.cmu.edu/asset_files/WhitePaper/2008_019_001_52338.pdf.

Caputo, D., Maloof, M., & Stephens, G. (2009). Detecting insider theft of trade secrets. *IEEE Computer Society Journal*, *7*, 14-21. http://dx.doi.org/10.1109/MSP.2009.110

Carnegie Mellon University (2014). 2014 US state of cybercrime survey. Retrieved from http://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_298322.pdf.

Computer Economics (2010). Malicious insider threats greater than most IT executives think. Retrieved from http://www.computereconomics.com/article.cfm?id=1537

Crow, R. (2004). Personnel reliability programs. Retrieved from http://www.ppc.com/assets/pdf/white-papers/Personnel-Reliability-Programs.pdf.

Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., & Trzeciak, R. (2012). *Insider threat study: Illicit cyber activity involving fraud in the US financial services sector* (CMU/SEI-2012-SR-004). Retrieved from Software Engineering Institute: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=27971

Demarco, C. (2014). BYOD policies could facilitate corporate espionage. Retrieved from http://www.insidecounsel.com/2014/06/19/byod-policies-could-facilitate-corporate-espionage?ref=nav

Equal Employment Opportunity Commission (2000). ADA enforcement guidance: pre-employment disability related questions and medical examinations. Retrieved from http://www.eeoc.gov/policy/docs/guidance-inquiries.html#2

Equal Employment Opportunity Commission (2012). Consideration of arrest and conviction records in employment decisions under Title VII of the Civil Rights Act of 1964. Retrieved from http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm#IIIB

Federal Bureau of Investigation (2012). The insider threat: An introduction to detecting and deterring an insider spy. Retrieved from http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat

Ferraiolo, D. F., & Kuhn, R. (1992). *Role based access controls* [15th National Computer Security Conference paper]. Retrieved from NIST Computer security resource center: http://csrc.nist.gov/rbac/rbacSTD-ACM.pdf

Hu, V., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., & Scarfone, K. (2014). *Guide to attribute-based access control (ABAC) definition and considerations* [NIST Special Publication 800-162]. Retrieved from Computer Security Resource Center: http://csrc.nist.gov/projects/abac/july2013_workshop/july2013_abac_workshop_abac-sp.pdf

Jansen, C. (n.d.). Mandatory Access Control (MAC). Retrieved from http://www.techopedia.com/definition/4017/mandatory-access-control-mac

Jansen, C. (n.d.). Security Incident and Event Management (SIEM). Retrieved from http://www.techopedia.com/definition/4097/security-incident-and-event-management-siem

Janssen, C. (n.d.). Authentication. Retrieved from http://www.techopedia.com/definition/342/authentication

Kedgley, M. (2014). File integrity monitoring software. Retrieved from http://www.newnettechnologies.com/file-integrity-monitoring-software.html?gclid=CLTSv_eDvsECFWcF7AodsU0ADA

Keeney, M., Kowalski, E., Cappelli, D., Shimeall, T., & Rogers, S. (2005). *Insider threat study: Computer system sabotage in critical infrastructure sectors*. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51934

Kouns, J., & Minoli, D. (2010). *Information technology risk management in enterprise environments: a review of industry practices in a practical guide to risk management teams*. Retrieved from http://www.amazon.com/s/ref=nb_sb_noss_1?url=search-alias%3Daps&field-keywords=Information+technology+risk+management+in+enterprise+environments+in+enterprise+environments

Kowalski, E., Cappelli, D., & Moore, A. (2008). *Insider threat study: Illicit cyber activity in the IT&T sector*. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52257

Kowalski, E., Conway, T., Williams, M., Cappelli, D., Willke, B., & Moore, A. (2008). *Insider threat study: Illicit cyber activity in the government sector.* Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52227

Lane, D. C. (1995). On a resurgence of management simulations and games. *Journal of the Operational Research Society*, *46*(5), 604-625. http://dx.doi.org/doi:10.1057

Lepofsky, R. (2011). Phase II: Why I have not yet implemented file integrity management. Retrieved from http://www.networkworld.com/article/2228830/security/phase-ii---why-have-I-not-yet-implemented-file-integrity-management--fim--.html

McCaughan, T. (2014). Air Force nuke officers caught up in big cheating scandal. Retrieved from http://www.cnn.com/2014/01/15/politics/air-force-nuclear-scandal/

McGeary, J. (2001). The FBI Spy It took 15 years to discover. Retrieved from http://content.time.com/time/world/article/0,8599,2047748,00.html

Mehta, L. (2014). File Integrity Monitoring (FIM) and PCI-DSS. Retrieved from

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). *The "big picture" of insider IT sabotage across US critical infrastructures* (CMU/SEI-2008-TR-009). Retrieved from Software engineering Institute: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8703

NIST Computer security resource center (2013). Attribute Based Access Control (ABAC) - overview. Retrieved from http://csrc.nist.gov/projects/abac/

National Employment Law Project (2014). Criminal records and employment. Retrieved from http://www.nelp.org/site/issues/category/criminal_records_and_employment/

Owen, D. (n.d.). What is a false positive and why are false positives a problem? Retrieved from http://www.sans.org/security-resources/idfaq/false_positive.php

Pfleeger, C. P., & Pfleeger, S. L. (2011). *Security in computing* (4th ed.). New York, Boston, San Francisco, Toronto, Montreal, London, Munich, Cape Town, Sydney, Tokyo, Singapore, Mexico City: Prentice-Hall.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector* (CMU/SEI-2004-TR-021). Retrieved from Software Engineering Institute: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7227

Raytheon (n.d.). Best practices for mitigating and investigating insider threats. Retrieved from http://www.raytheon.com/capabilities/rtnwcm/groups/iis/documents/content/rtn_iis_whitepaper-investigati.pdf.

Rosenblatt, S. (2013). Two-factor authentication: What you need to know (FAQ). Retrieved from http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/

Rouse, M. (2012). Security Information and Event Management (SIEM). Retrieved from http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

Rouse, M. (2014). Digital signature. Retrieved from http://searchsecurity.techtarget.com/definition/digital-signature

Ruppert, B. (2009). *Protecting against insider attacks*. Retrieved from SANS InfoSec Reading Room: .

Ryan, A. (2012). Can you refuse to hire a felon? Retrieved from http://www.laborlawyers.com/can-you-refuse-to-hire-a-felon

SANS Institute (2014). Extending role based access control. Retrieved from http://www.sans.org/search/results/Extending Role Based Access Control

Sawyer, J. H. (2011). Basic baselining for quick situational awareness. Retrieved from http://www.darkreading.com/risk/basic-baselining-for-quick-situational-awareness/d/d-id/1136572?

Schneirer, B. (2009). Insiders. Retrieved from https://www.schneier.com/blog/archives/2009/02/insiders.html

Security models strengths and weaknesses. (n.d.). Retrieved from https://sites.google.com/site/jamestwigger/Home/research/security-models-strengths-and-weaknesses

Senator, T. E., Bader, D. A., Dietterich, T. G., Lee, J., Corkill, D., Goldberg, H. G., & Chow, E. (2013). Detecting insider threats in a real corporate database of computer usage activity. Retrieved from http://www.cc.gatech.edu/~bader/papers/PRODIGAL-KDD2013.pdf

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. J., & Flynn, L. (2012). *Commonsense guide to mitigating insider threats: 4th Edition* (CMU/SEI-2012-TR-012). Retrieved from Software engineering Institute: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34017

Software Engineering Institute (2012). Insider threat control: Using a SIEM signature to detect potential precursors to IT Sabotage. Retrieved from http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=85

Software Engineering Institute (2014). Insider threat. Retrieved from http://www.cert.org/insider-threat/

StackExchange (2014). Looking for approach to implement attribute based access control (ABAC). Retrieved from http://security.stackexchange.com/questions/54379/looking-for-approach-to-implement-attribute-based-access-control-abac

Sterman, J. D. (2006). Learning from evidence in a complex world. *American Journal of Public Health*, *96*(3), 505-514. http://dx.doi.org/doi: 10.2105

Tripwire Enterprise 8.3 Connect. Protect. Detect. (2013). Retrieved from http://ca.westcon.com/documents/40952/tripwire_enterprise_8.3_product_brief.pdf.

U.S. Department of Labor (2012). TRAINING AND EMPLOYMENT GUIDANCE LETTER NO. 31-11. Retrieved from http://wdr.doleta.gov/directives/attach/TEGL/TEGL_31_11.PDF

U.S. Government Accountability Office (1992). Nuclear Personnel Reliability Program. Retrieved from http://www.gao.gov/products/NSIAD-92-193R

Wheeler, D. A. (2005). Open source SCM/RCM systems. Retrieved from http://www.dwheeler.com/essays/scm.html

Workshop on Research for Insider Threat (WRIT). (2013). Retrieved from http://www.sei.cmu.edu/community/writ2013