Fall 11-29-2016

Identifying and Preventing Insider Threats

Matthew D. Waters
Eastern Kentucky University, matthew_waters3@mymail.eku.edu

Eastern Kentucky University

Identifying and Preventing Insider threats

Honors Thesis

Submitted

In Partial Fulfillment

Of The

Requirements of HON 420

Fall 2016

By

Matthew David Waters

Faculty Mentor

Dr. Ryan Baggett

Department of Safety, Security and Emergency Management

Identifying and Preventing Insider Threats

Matthew David Waters

Dr. Ryan Baggett: School of Safety, Security and Emergency Management

Abstract

Insider threats, or attacks against a company from within, are a pressing issue both domestically and internationally. Frequencies of these threats increase each year adding to the overall importance of further research analysis. In fact, many case studies have been conducted which state that these employees who participate in insider attacks tend to exhibit certain personality and characteristic traits, as well as certain observable behaviors, that would indicate to other employees that an attack is imminent. It is hypothesized that companies will be able to take a more preventative stance of security as opposed to a reactive stance by identifying these characteristics and behaviors, as well as the motivations that drive them. In order to accomplish this task, companies must implement multiple layers of technological means of security, as well as take a more hands-on, holistic approach with company-wide involvement.

Keywords: Honors Thesis; Insider; Threat; Characteristics; Behaviors; Holistic Approach; Technology; Risk.

TABLE OF CONTENTS

CHAPTER PAGE

Introduction

Every year, companies spend a significant amount of money on security means to protect their assets against outsider attackers, such as hackers. However, there is a more serious and pressing issue that companies around the world face, against which few are well protected: the issue of insider threats. Even though few companies understand and prepare for insider threats, insider attacks appear to be growing in frequency each year (Butavicius et al., 2012). In 2004, it was "estimated that over 80% of information security incidents for the past four years are the result of insiders" (Andrews et al., 2004, p. 14). This statistic is staggering given that it is estimated that the frequency of attacks has been growing ever since (Carter et al., 2012). Given the financial damage that insiders inflict on companies, it is arguable that they are worse than outsider attacks. In fact, "A recent FBI survey reported that the average cost of a successful attack by a malicious insider is nearly 50 times greater than the cost of an external attack" (Andrews et al., 2004, p. 14). Not only can insiders cause damage to the information assets of the company, but physical damage and damage to the company's reputation as well, all of which cause financial damage (Liang et al., 2012). What is even more concerning is the thought of adversarial insiders working within "government facilities dealing with materials that can cause such unacceptable catastrophic impact" (Hershkowitz, 2007, p. 106). However, arguably the biggest issue regarding insider threats is the fact that most companies are unprepared for an insider attack; they lack proper understanding of insiders, and thus are unable to identify the problem before it occurs. It is hypothesized that, by identifying certain characteristics and behaviors of insiders, as well as their motivations, companies can take a more preventative stance against insider threats by implementing layers of technological means of security as well as a holistic, companywide approach in order to identify and reduce the insider threat. In order to do this, it is necessary to develop a definition of an insider threat; then, the characteristics, behaviors and motivations of insider threats will be identified; once these have been identified, a few technological means of preventative security will be discussed; finally, the holistic approach that companies must take to ensure optimal protection will be discussed. First, a working definition of an insider threat must be developed.

Literature Review

There are three main sources that merit discussion for this paper: Butavicius et al.'s "Preventing and Profiling Malicious Insider Attacks"; Colwill's "Human Factors in Information Security: The Insider Threat – Who Can You Trust These Days"; and The National Infrastructure Protection Plan 2013. Butavicius et al. and Colwill's articles discuss insider threats more in-depth, such as their personality traits as well as other studies that have been conducted regarding the insider threat issue. The NIPP, however, discusses protection against threats in general. All three of these documents provide some of the most beneficial information used in this paper.

The aim of Butavicius et al.'s (2012) article is to identify and discuss specific information regarding the individuals that commit insider threats, including personality traits and observable behaviors, as well as personnel, policy and technical responses companies can take for a holistic response to insider threats. What is very beneficial about this article is the fact that the authors list and briefly explain a few previous research studies conducted regarding insider threat identification and prevention. The authors also implement the research and statistics obtained from these studies their own study as a means of backing up their claims. After listing and discussing the different means of identifying and preventing insider threats, they end their article by discussing in what ways future research could be conducted in order to be more completely prepared for insider threats.

There are few limitations and biases within this article that must be discussed. The first limitation is the fact that this article was produced for the Australian Government with research collected from insider attacks in Australia. The reason this is a limitation is because not all insider threats will be the same among different countries; that is, just because the number of insider attacks is rising in Australia does not mean that it is a growing problem in the United States as well. This is why it is important that a foreign report was included within this paper to show that the insider threat problem is growing not only in the United States, but in other countries as well. Another limitation presented in this article is the limited amount of research conducted up to this point regarding the insider threat problem in Australia. The authors themselves state that “it is strongly recommended that further research be undertaken” (2012, p. 3). It is for this reason that this paper analyzed a large number of research studies and other articles regarding insider threats in order to have a more accurate representation of the issue. The final limitation of this article is the fact that it cites only five studies conducted on insider threats for the entire report. Although limited research had been conducted on the issue up until 2012, it would have behooved the authors to use a larger amount of studies and research for a more accurate representation of the problem. Besides these few examples, and due to the fact that the authors discuss them, there appear to be very few limitations in this article. The authors themselves do not appear to have many biases as well given that they are all research scientists with disciplines focused in cognitive and social psychology. Butavicius also conducted research regarding protection and simulation training. The only bias that these authors may exhibit is the fact that they appear to have little experience regarding protection against insider threats.

The aim of Colwill's (2009) is to provide an explanation of the different characteristics exhibited by insider threats and the reactions taken by companies in order to prevent it them from attacking. In the article, he explains that mitigation is a key factor of risk management rather than simply reacting to an attack. In the end, he provides a number of solutions that can reduce the amount of insider threats a company faces, such as security policies, education and the maintenance of trustworthy relationships. In the article, Colwill cites both public and private sector organizations and individuals for his statistics regarding insider characteristics, different means of security and the effectiveness of different mitigation techniques.

There are few limitations within Colwill's article. As with the previous article, Colwill collected and analyzed statistics based on insider attacks within the United Kingdom. Thus, his statistics may differ significantly from those acquired by the United States or any other country. Another limitation is the fact that this article was published in 2009. Because of this, the statistics acquired by Colwill are a little dated and may not represent the problem as it is in 2016. Colwill's citations may also be in question depending on how much research he conducted on the individuals and institutions that published the information he utilized; however, this can be said essentially for any report. Colwill himself also does not appear to have any visible biases regarding insider threats or the steps necessary in preventing them. Having said that, the use of Colwill's article benefits this paper significantly given the information it provides.

The National Infrastructure Protection Plan (NIPP) 2013 is essentially a guidebook established by the Department of Homeland Security (DHS) for protecting the nation's critical infrastructure. Within this plan, the DHS lays out its vision, mission and goals when protecting the nation's critical infrastructure. It defines a large number of concepts necessary for understanding risk management and critical infrastructure. The plan also establishes "seven core tenets, representing the values and assumptions the critical infrastructure community should consider (at the national, regional, SLTT, and owner and operator levels) when planning for critical infrastructure security and resilience" (2013, p. 13). It goes on to list and define a five step process of risk management which can be used at any level (local, national, etc.). It ends by discussing twelve "calls to action" in order to build partnerships, manage risks and focus on outcomes. The section primarily used for this paper is the five-step process of risk management. The reason this information is so vital to preventing insider threats is due to the fact that it can be used in any environment both in the public and private sector. No matter the size of the company, this process can be utilized in order to identify the company's assets and the threats to said assets. The use of the plan for this paper is also very efficient due to the fact that it combines risk, threat and vulnerability assessments into a single management process, all of which are useful when preventing insider threats.

Given that the plan is a United States Government prepared document, there are practically no limitations to its use. Having said that, there is the issue discussed with the previous articles of non-representativeness to other countries. However, a solution to this limitation for future research is to gather information and statistics from multiple countries. Another limitation when using this plan is the vocabulary it uses, i.e. infrastructure. Because this plan is prepared for a national scale as opposed to the private sector, companies and individuals may be confused on when and how to use this plan. However, once they have read and analyzed it, they will understand that it is a simple plan that can be used on all levels in both the public and private sector. The only other limitation or bias observable in this plan is that it can be taken as an answer to all risk and threat problems, which is not the case. This plan must be conducted carefully and thoroughly and must also be combined with other means of threat and vulnerability assessments in order to ensure optimal protection of a company's assets or infrastructure.

Research Design

This study utilizes qualitative analysis research in order to acquire and analyze data to support the theory that insider threats can be identified by certain characteristics, behaviors and motivators, and can be prevented through a combination of a technological and holistic approach. The sources researched for this paper are a combination of government and public sector case studies. There are three variables to consider when determining the consistency of the theory presented: the characteristics of insiders; the observable behaviors of insiders; and the motivators that drive insiders.

Operationalization of Variables

The first variable analyzed was the certain characteristics that employees exhibit which indicate that they are insiders or are more likely to turn insiders. These identified characteristics can be measured nominally to determine whether or not an individual is or is likely to become an insider. By reviewing past incidents regarding insider attacks, researchers may be able to indicate which characteristics employees exhibited that indicated a possible attack, which is what most of the researchers did in the case studies reviewed for this paper. The manner in which this variable was obtained and analyzed for this paper was by conducting research on studies that professionals and experts have performed on past insider attacks on public sector companies. The information gathered from this variable will be measured with logical argumentation and comparisons.

The second variable analyzed was the observable behaviors of insiders. After reviewing many professional articles regarding insider threats, it was found that insiders usually exhibit certain observable behaviors along with personality traits and characteristics. As with the first variable, this information can acquired by reviewing studies conducted in the past by experts regarding insider threats. These studies can be compared and contrasted to determine which behaviors employees exhibit indicate that they were in the process of attacking the company's assets or had already attacked. The information acquired for this variable will be measured with logical argumentation and comparisons as well.

The third variable measured in this study was the motivators that drive employees to turn insiders. These motivations can range from personal gain to revenge et al. As with the other variables, this information for this variable was acquired from scholarly articles and past research studies conducted on insider threat attacks. Another means by which this information can be acquired is by personally interviewing the insiders themselves and asking the motivators which caused them to act. However, due to time constraints, the sole means of acquiring information on insider motivators was by reviewing case studies conducted by professionals in the field of physical and national security. As with the other variables, the information gathered for this variable will be analyzed by means of logical argumentation and comparison.

Population

The population for this study includes security managers, government officials, professional researchers and university professors who have an extensive knowledge on the subject of insider threats in the public sector. This study would not be adequate if it were to use another type of population given that the individuals would lack the proper knowledge of insider threats, their characteristics, their behaviors and motivators, and means of preventing insider attacks. Due to time constraints, this population is adequate for this study.

Limitations

As mentioned previously in the literature review, there are obviously some limitations regarding the sources researched for this study and the information acquired from them. One of the main limitations is that some of the case studies date back at least ten years; this could result in an inaccurate representation of the insider threat today. Another possible limitation discussed is the fact that, where this study focuses mainly on insider threats in the United States, some of the articles used were conducted by other countries, such as the United Kingdom. Another limitation could be a lack of information regarding identifying and preventing insider threats in the United States. However, ample amounts of information are presented that answer the research question and support the theory presented.

Results

Defining Insider Threats

Before proceeding, a definition of "insider threats" must be established. Because little information has been developed concerning insider threats and the different types of insiders, there are multiple definitions used in order to describe them. Essentially, there are two basic categories of insiders: adversarial insiders, or those who purposefully commit malicious acts (usually for personal gain); and unintentional insiders, or those who commit malicious acts either by accident or due to negligence. Insiders can be anyone who has access to the company's information systems and networks, such as employees, contractors, consultants, etc. (Butavicius et al., 2012). Insiders may also include third-party business partners and their employees, temporary help (Schultz, 2002), and even supervisors and managers. Larry Knutsen, member of the Laconia National Security Consulting Group, states that "privileged users, those who have been granted exclusive access to data within a company, are a major concern for organizations. Those given that status should be monitored closely because they have exceptional access to the data" (Magnuson & Sicard, 2015, p. 10). Insiders do not have to currently work for the company; rather, insiders can also include previous employees who have had access to the network and systems (DHS, 2014). In essence, an insider can generally be defined as "anyone with knowledge of operation or security systems and who has unescorted access to facilities or security interests" (Biringer et al., 2007, p. 55). Having discussed this information and provided a very high level definition of an insider threat, it is necessary to discuss the two categories of insider threats, as well as the actions that the individuals in these categories commit in order to be labeled as an insider threat. Once that is complete, a more refined and formal definition of insider threats can be established. First, a discussion of adversarial insiders is necessary.

Adversarial Insiders

When gathering data on insider threats and the types of insiders, the United Kingdom's Centre for the Protection of National Infrastructure sums up the category of adversarial insiders with their definition of an insider: "a person who exploits, or has the intention to exploit, their legitimate access to an organization's assets for unauthorized purposes" (CPNI, 2013, p. 6). As mentioned previously, the "unauthorized purposes", or motives, can include a number of different reasons which will be discussed later. There is also a multitude of different types of adversarial insiders. In his book, “Risk Analysis and Security Countermeasure Selection”, Thomas Norman discusses six categories of adversarial insiders: Class 1 Terrorists; Class 5 Terrorists; Sophisticated Economic Criminals; Unsophisticated Criminals; Lone Criminals; Cause Oriented Subversives (2016). Norman discusses Hackers as a seventh category, but due to the definition of insider threats that will be used for this paper, these two categories would not be considered as an insider threat.

The first category Norman discusses is Class 1 Terrorists. Norman defines Class 1 Terrorists as government trained and supported professionals whose sole purpose is to infiltrate the intelligence communities of other countries (2016). He states that these individuals are usually recruited from the adversarial country’s intelligence community, military, secret service, etc. The second group Norman discusses is Class 5 Terrorists. These are amateur civilians with basic terrorist experience who attempt actions of theft and violence against industry information and assets. These individuals may work alone, or may form militia-like groups. The third group of insiders is Sophisticated Economic Criminals. These individuals have the knowledge and tools to accomplish their goals of acquiring information or destroying assets. These individuals can be the insiders themselves, or outsiders in collusion with insiders. The fourth group Norman discusses is Unsophisticated Criminals. These are individuals who have access to the systems and networks, but pose little threat to the organization due to their lack of skills or knowledge. Norman states that simple theft of information or assets can be included in this category of insiders. The fifth group Norman discusses is Lone Criminals, individuals who work alone in order to steal or destroy company information and assets. Norman states that Sophisticated and Unsophisticated Criminals can fall in this category as well. The sixth category in Norman’s list is Cause-Oriented Subversives, individuals and activist groups who commit acts of theft and destruction due to their opposition to the government, an industry, religion, etc. (2016).

As mentioned above, Norman includes Hackers as a seventh category. A hacker can be generally defined as "a malicious or criminally minded outsider who seeks to cause damage to organizations or individuals for financial gain or personal notoriety" (Steele & Wargo, 2007, p. 24). Hackers "circumvent security and break into a network, computer, file, etc., usually with malicious intent" (www.dictionary.com). In their article "Intrusion Detection: Perspectives on the Insider threat", Andrews et al. state that "All insider attacks must use local resources (operating system components, installed applications, network appliances and so forth) in order to carry out their purpose" (2004, p. 14). Because insiders have access to the organization's networks, systems and other technology, they are not required to breach or break into the organization's systems. Therefore, Hackers would not be considered an insider threat. Having briefly defined and discussed the different types of adversarial insiders, it is important to discuss some of the many methods utilized in order to accomplish their goals of information and asset theft and destruction.

Adversarial Insider Activity

In their study, the United Kingdom's CPNI defines five main types of insider activity that it identified in its experiment: "unauthorized disclosure of sensitive information; process corruption; facilitation of third party access to an organization's assets; physical sabotage; and electronic or IT sabotage" (2013, p. 4). Of these five, the two most frequent acts committed by adversarial insiders were the unauthorized disclosure of sensitive information and process corruption. Ironically, electronic sabotage was found to be committed the least frequently. Also, the CPNI found that the vast majority of individuals were self-initiated, meaning they saw an opportunity for personal gain (or other motives) and initiated the attack themselves without any outside influence. As previously mentioned, hackers are not considered insiders for the sake of this paper. However, insiders may still utilize hacker tools on the Internet (such as automated tools) in order to commit malicious acts from within (Jeong et al., 2012). Insiders may also utilize coercion tactics to acquire Internet Protocol credentials from a coworker with access (Agrafiotis et al., 2015). Other tactics include the installation of backdoors into information systems, overloading the network or systems, and even utilizing social network sites to recruit other individuals as insiders (Jeong et al., 2012). Finally, it is important to note employees taking advantage of telework, or working from outside the workplace. According to Jeong et al., in order to increase productivity, more companies are providing employees with mobile access to their networks and information systems. This remote access, Jeong et al. argue, opens up more vulnerabilities for adversarial insiders to attack. They state that "a previous study on insider threat also concluded that 56% of the insider threat attacks were launched via remote access whereas 35% occurred inside the organization and 8% of attacks used a combination of the workplace and remote access" (2012, p. 185). As will be discussed in the holistic approach to preventing insider threats section, companies and organizations need to ensure that all means of security are being implemented when allowing such freedom to the employees.   Having discussed the tactics, tools, and methods of adversarial insider attacks, it is necessary to define and discuss the unintentional insider threat, as well as the means by which unintentional insider attacks are performed.

Unintentional Insiders

The CERT Insider Threat Team of the Software Engineering Institute at Carnegie Mellon University conducted a foundational study on unintentional insider threats in 2013 which was produced for the U.S. Department of Homeland Security (DHS). In this study, the team creates a definition of an unintentional insider comprised of four main parts. The first part states that an unintentional insider is “a current or former employee, contractor, or business partner” (2013, p. 1). This part of the definition does not differ from the adversarial insider, or insider threats in general. The second part states that an unintentional insider “has or had authorized access to an organization’s network, system, or data” (2013, p. 1). This part also discussed adversarial insiders, stating that individuals can only be insiders if they have access to and utilize the organization’s network, systems, or technology. The third part states that unintentional insiders create threats “through action or inaction without malicious intent” (2013, p. 1). It is this part which differentiates unintentional insiders from adversarial insiders. The final part states that, through this inaction or action without malicious intent, the unintentional insider “causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization’s information or information systems” (2013, p. 1). As with the first two parts of this definition, the final part of the definition of an unintentional insider does not differ from an adversarial insider if the outcome is the same whether the act was unintentional or meant to be malicious. Having defined unintentional insiders, it is necessary to explain the means by which they cause damage to an organization’s assets.

Unintentional Insider Activity

When it comes to unintentional insider threats, human error essentially plays the main role in causing substantial amounts of damage to an organization’s assets. The CERT Insider Threat Team provides a multitude of ways that human error affects employees and causes insider threats. One of the main examples the team provides is fatigue and situational awareness. According to the team, “If employees within a computing environment are sleepy . . .they may exhibit decreased attentiveness and increased inappropriate responses to critical network security information" (2013, p. 8). Essentially, if IT employees, or any employees within the organization for that matter, are plagued by fatigue, their situational awareness drops significantly which may result in the theft of important information or the destruction of essential means of cybersecurity and the assets they protect. Another example the team discusses is deviations from the company's policies and procedures. Lack of knowledge of company procedures or carelessness/negligence of standard practices can lead to breaches in the system and the destruction or theft of assets. The team states that lapses in judgement regarding these procedures and practices can be categorized in four ways: unintentional acts ('I didn't mean to do that.'); unintentional failures to act ('I forgot to do that.'); intentional but incorrect acts ('I thought that's what I was supposed to do.'); intentional but incorrect failures to act ('I didn't think I was supposed to do that.')" (2013, p. 18). Finally, in their foundational study, the team lists acts committed by unintentional insiders that can lead to serious negative consequences, including the accidental disclosure of information, unintentionally aiding an outsider by falling for phishing and other online scams, and even losing physical devices which may store important information such as a USB drive, phone, etc.

Having discussed the multiple types of insider threats as well as the many definitions of insider threats, it is now possible to create a working definition of insider threats that will be used for this paper:

> An insider threat is an employee or anyone (past or present) given permissible access to a company's assets, (whether physical or virtual) who unintentionally or with malicious intent causes significant damage to the company and its reputation

> through the release of essential, confidential information or the partial or complete destruction of its assets.

Having properly defined insider threats, the many identifiable personal, physical, and psychological traits of insiders, as well as the motivators that drive them must be discussed. By identifying these traits, an organization will be better prepared for a proactive response rather than a reactive response to insider threats.

Insider Threat Characteristics

Many studies conducted in the past regarding insider threats have shown that individuals who become insiders, whether adversarial or unintentional, tend to exhibit certain personality characteristics and personal predispositions that differ from other employees and identify them as insiders (Butavicius et al., 2012). Carter et al. states that if companies are able to statistically identify these characteristics, motivations and actions, then they will be able to properly establish different protection protocols that reduce the likelihood of an insider attack (2012). However, it is possible that other employees may exhibit some of these same characteristics without the predisposition of committing an insider attack (Butavicius et al., 2012). It is essential that the company identifies the individuals who exhibit these characteristics and traits, monitor them closely, and distinguish between the two. It is also essential that the company ensures its employees understand that these types of behaviors and actions can be a conduit through which insiders can gain information from others (Department of Homeland Security National Cybersecurity and Communications Integration Center, 2014). The purpose of this section is to list and describe these identifiable characteristics, behaviors and motivations of insider threats.

There are a number of different characteristics and personality traits that can distinguish insider threats from normal employees. In their article, Butavicius et al. cite a study conducted by Kowalski, Cappelli & Moore at Carnegie Mellon which focused on the characteristics, motives, and behaviors of insiders, more specifically in the IT department of the organization (2012). In this study, Kowalski et al. state that there was no single profile that could be used to describe an insider. The race, age, and ethnic backgrounds of the insiders varied considerably. However, they do present a few noticeable characteristics and personality traits of the identified insiders. They state that the insiders were predominately single males who had not been previously married; almost half of the insiders had prior arrest records; approximately half of the insiders were current employees and half were past employees of the company; and that the majority were employed in IT positions (Butavicius et al., 2012).

Another study cited by Butavicius et al. regarding insider threat characteristics and behaviors was conducted by Coldwell in 1993. In this study, Coldwell places significant emphasis on the feelings of frustration exhibited by insider threats. Coldwell discusses how these feelings of frustration are usually the result of negative social interactions either at home or in the workplace. He states that these feelings of frustration can lead to computer dependency and isolation which, in turn, leads to a decrease in social skills.

Butavicius et al. discuss many other personal characteristics and traits (or vulnerabilities as they call them) inherent in insider threats. These characteristics and traits include "introversion, social and personal frustrations, ethical flexibility, reduced loyalty, entitlement and lack of empathy" (2012). They explain that insiders tend to exhibit a combination of these characteristics and traits, thus making it easier for managers and other employees to identify them. One final thing discussed by Butavicius et al. is a study conducted by Fischer in 2008.

Fischer states that insider threats tend to exhibit the same types of characteristics, traits and behaviors as spies who commit espionage. He states that by understanding the types of characteristics, traits and behaviors that these individuals exhibit, companies can easily identify potential insiders. Although this paper is focused around insider threats and not individuals committing espionage, its' still an interesting concept that could merit future research.

The Center for the Protection of National Infrastructure (CPNI) researchers provide their own statistics regarding insider characteristics and traits in their 2013 data collection study. When conducting research on insider threat cases, they state 82% were male; 49% were between the ages of 31 and 45; 88% were permanent staff; and 60% were individuals who had worked there for less than five years (2013). The researchers proceed to list and explain a multitude of different personality traits. These include immaturity; low self-esteem; amoral/unethical; superficial; prone to fantasizing; impulsive; manipulative; lacks conscientiousness; emotionally unstable; and even present evidence of having some form of psychological or mental disease (2013). Other traits that the researchers discuss include drinking/drug/gambling problems, a recent negative life event, such as a death in the family, and showing signs of stress, such as having a bad temper and a poor work attitude (2013). Because of these characteristics and traits, insiders usually exhibit observable behaviors that other employees should be watching for.

Insider Threat Behaviors

Insiders appear to exhibit different observable traits in the workplace. When discussing insider behaviors, Butavicius et al. cite three different studies based around this topic: one conducted by Kowalski et al. in 2008; one conducted by Shaw et al. in 1998; and one conducted by Moore et al. in 2008. In their study, Kowalski et al. state that in 52% of the insider threat cases they studied, there were noticeable online activities that these individuals were conducting.

These activities included sabotaging data backups, creating false accounts, and downloading malware (Butavicius et al., 2012). Shaw et al. discuss a behavior mentioned previously: computer dependency. They explain that computer dependency is when an individual spends such a significant amount of time on the computer that it begins to have negative effects on that individual's daily life. They state that this type of observable behavior should alert companies about a potential problem (2012). Moore et al. discus many types of insider threat behaviors. These behaviors include inappropriate social interactions, such as bullying and poor hygiene, and violating company rules and policies (2012). Another pattern of behavior that Moore et al. emphasize is the creation of digital access pathways into company databases and other sources of information. Once terminated, insiders would be able to access these pathways (or backdoors) from outside of the company's network/system (2012).

The CPNI also provides a list of observable behaviors in their study, which include actions such as irregular copying and IT activity. Essentially, this means that the insider reproduces sensitive material when unnecessary or unauthorized. The audit of the insider's system would also show irregular activity such as conducting key word searches in databases that the individual has no need to know (2013). Other behaviors include the unauthorized handling of sensitive information, as well as the complete violation of security protocols (2013).

The U.S. Secret Service and Carnegie Mellon University's Software Engineering Institute CERT Program conducted a study centered on identifying and managing insider threats. In this study, they emphasize the fact that the insiders who turned adversarial exhibited many observable behaviors prior to their attacks. In their case study, they found that eighty percent of employees exhibited warning signs, such as "tardiness, truancy, arguments with coworkers, and poor job performance. Insiders who committed IT sabotage held technical positions" (Cappelli et al., 2007, p. 5-6). They also found in their study, as stated with other cited case studies, that a majority of these individuals had set up backdoor access pathways prior to termination in order to gain access post termination.

Another critical, observable behavior is verbal behavior. Limited research has been conducted on the use of language as a warning sign of an insider attack, but those who have discussed it have done so extensively. In his case study, Schultz explains that aggressive verbal behavior, either written or spoken, can be an indicator of an imminent attack. An example he gives is an email containing aggressive or hostile language directed at a boss or a fellow employee (2002). In their case study, Ball et al. focus on detecting insiders through language exclusively. The verbal behavior they focus on mainly is the excessive use of first-person personal pronouns. They state that "the use of first-person plural pronouns, or we words, is negatively related to distancing and positively related to having a strong sense of community" (2013, p. 268). Essentially, the use of first-person personal pronouns tends to show that the individual is beginning to distance him/herself from the rest of the community, which can lead to that person becoming self-focused and disgruntled, which can result in an attack.

In their article, Ball et al. very briefly discuss the concept they call the "insider threat scenario" (2013). There are five main stages of this threat scenario: exploration; experimentation; exploitation; execution; and escape and evasion. In the exploration stage, the insider is beginning to be recruited by self-motivations, another company/organization, or is beginning to recruit others. In the experimentation stage, the insider begins to gather information regarding what profitable data can be stolen, as well as the weaknesses of the company's system and network. In the exploitation stage, the insider utilizes these weaknesses in order to gain access to the company's information. In the execution stage, the insider collects and extracts all data that is deemed profitable or essential. Finally, in the escape and evasion stage, the insider abandons the system, possibly leaving behind observable traces, access pathways or destructive programs. As mentioned, different behaviors manifest at different stages of the scenario. If companies are able to identify these behaviors, it is possible that they can link them to a specific stage of the scenario and understand how far the insider has progressed with the attack. In fact, the DHS briefly discusses five "behavior prediction theories" in their publication *Combating Insider Threat*: General Deterrence Theory (individuals commit the crime if they believe the benefits outweigh the costs); Social Bond Theory (individuals commit the crime if their social connections are weak); Social Learning Theory (individuals will commit the crime if they associate with delinquents); Theory of Planned Behavior (individuals' intentions are a key factor in predicting behavior); and Situational Crime Prevention (if a motive and an opportunity exist, the crime will be committed) (2014). Knowing and identifying the behaviors of insiders is essential, but it is also imperative that companies understand the motives behind their actions as well.

Insider Threat Motivators

There are multiple motivators that drive employees to become insiders. There may be a single motivating factor driving an insider, or a combination of factors. Butavicius et al. cite Kowalski et al.'s (2008) case study, which stated that revenge was the strongest motivating factor, followed by financial gain, dissatisfaction with company policies, and the desire to bring information to a new company (2012). Butavicius et al. list a number of other motivating factors, such as a feeling of entitlement to certain information or other means of personal gain; disgruntlement from a negative event, such as unmet expectations, a demotion, a negative interaction with another employee, and even a lack of acknowledgement for an accomplishment.;

and also a lack of loyalty presented to the company. According to Ball et al., “in their analysis of espionage cases in the 1990s, Herbig and Wiskoff (2002) found that divided loyalty was the most common reason for insider activity” (2013, p. 268). Other motivations may include ideology, psychosis, or recruitment (Biringer et al., 2007). In his journal publication, Colwill explains how economic and cultural changes can lead to fear and uncertainty, which can lead employees to turn insider (2009). Finally, an interesting motivator discussed by Steele and Wargo is laziness. They state that employees may turn unintentional insider by cutting corners and circumventing certain policies due to laziness. By doing this, these employees open the company’s systems up to serious security breaches (2007).

In a majority of the cases reviewed for this project, the researchers have stated that these behaviors were present and identified, but nothing was done to prevent the attack. The private (and even public) sector needs to understand that “no one is immune” and that “anyone can be a victim” (Magnuson, 2013). Because of this, it is imperative that companies have different preventative means of security implemented, both technological and human, in order to be optimally prepared for when an attack occurs. Some of these technological means will be discussed in the next section.

Technological Approach

Technology plays a key role when it comes to preventative security measures. With the use of technology, security personnel are able to identify possible attacks, trace the attack back to the attacker(s), and prevent the attack from happening. However, this can be difficult when it comes to insiders. It can be argued that “the greatest challenge to any security system is protecting against the insider threat” (Biringer et al., 2007). The reason for this is because, as discussed previously, insiders have complete access to the company’s network and systems.

Insiders are able to identify vulnerability points within the security system and gain access to restricted areas. Because of this, it is essential for companies to implement layers of technological security. By implementing multiple means of security, the number of accessible vulnerabilities is reduced, thus preventing insiders from attacking (Department of Defense, n.d.).

Intrusion Detection Systems

One of the primary examples of preventative technology is Intrusion Detection Systems (IDS). According to Liang et al., “Intrusion Detection Systems (IDSs) are deployed to detect live (in real-time) attacks on network and host systems by using a database of past attack signatures” (2012, p. 186). They state there are primarily two types of IDSs: anomaly based (this type of system identifies behavior that deviates from the norm); and signature based (this type of system compares the audit logs of the company to a list of well-known attack signatures and determines whether or not there is a threat) (Liang et al., 2012). Something to note is that the Defense Advanced Research Project Agency has begun testing a new anomaly based intrusion detection system known as Anomaly Detection at Multiple Scales; this system would allow the IDS to sift through massive quantities of data very quickly in order to identify strange behaviors almost as soon as they occur (Liang et al., 2012). This system could be efficient for companies to implement given that it normally takes extended periods of time to sift through vast amounts of data. As mentioned with the multiple layers of security, the Department of Defense (DOD) explains that there should be multiple layers of IDSs within a security system in order to ensure optimal protection (n.d.).

Honeypot Technologies

Another means of security based technology is the use of honeypot technology. According to Spitzner, “A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource. What this definition means is that honeypots derive their value from threats using them. If the enemy does not interact or use the honeypot, then it has little value” (2003, p. 1). Honeypots are digital objects or locations, such as Microsoft Word documents, databases, and others that are created for the sole purpose of catching adversaries (Liang et al., 2012). Honeypots can even be login credentials and credit card numbers (Spitzner, 2003). Honeypots have no production value whatsoever. Essentially, honeypots are digital bait traps for insider threats (in the past they have been solely used for detecting outsider attacks but are now being used more often for insider threats). There should be absolutely no interactions with these digital entities, and thus, as soon as contact is made with a honeypot, the individual should be considered an insider attempting to attack (Liang et al., 2012). A potential disadvantage of honeypot technologies is that they only collect data while they’re being interacted with; they do not collect vast amounts of data across the network or system. There are also many uses for honeypots. They can be used to track fraud or theft, capture intelligence on potential attacks, and even prevent automated attacks (Spitzner, 2003).

There are three main types of honeypot technologies: honeypots; honeytokens, and honeynets. Honeypots are the most basic of the technologies. These are the digital entities, such as documents and databases, that companies create in an attempt to catch adversarial insiders. Honeypots help reduce the amount of alerts received from possible threats, as well as the amount of false positives reported given that they only alert when they have been interacted with. This, along with the fact that they require minimal resources, makes honeypots efficient when it comes to digital security. What also makes honeypots an efficient means of security is the fact that they still capture and report activity even when it is encrypted (Spitzner, 2003).

The second type of honeypot technology is honeytokens. These are essentially the links that lead insiders to the actual honeypots. Honeytokens can range from simple created hyperlinks to false log in and password information. Interesting enough, honeytokens can essentially be honeypots themselves; that is, honeytokens can be false documents and databases that lead an insider to the actual honeypots. What makes honeytokens efficient is the fact that they are extremely flexible and easy to change. They can be easily customized to fit any environment necessary (Spitzner, 2003).

The third type of honeypot technology is honeynets. Honeynets are the most advanced and complex type of honeypot technology. Rather than a single computer or a specific document, honeynets are a large network of computers. Essentially, honeynets are massive networks that contain multiple honeypots and honeytokens. According to Spitzner, honeynets are used to gather more information than simple honeypots, such as who the insider is, possible motives, and whether or not the individual accessing it has malicious intent. Security managers are able to put any information they deem appealing to insiders within these networks, much like a honeypot or honeytoken, making them very flexible and customizable (Spitzner, 2003).

Although the use of honeypot technologies can be an efficient means of security, there are some disadvantages to using them. One of these disadvantages is the fact that security managers must make honeypots enticing enough for insiders to interact. As mentioned, honeypot technologies have no use if the insider does not interact with them. Thus, it is up to security personnel to make sure that honeypot documents, netowrks, etc. are as enticing to insiders as possible (Spitzner, 2003). Another potential disadvantage is if the insiders discover that the documents or networks they are interacting with are honeypots. If this occurs, the insiders would be able to implement bogus information which could lead security personnel in the wrong direction. That is why it is essential that the least amount of people know of the honeypot's existence (Spitzner, 2003). Panda and Yaseen (2012) state that using honeypots to catch insider threats is ineffective given their knowledge of the network and systems and the fact that they utilize their access privileges to make use of pathways that are very difficult to identify by security mechanisms. A proper response to this argument is that honeypot technologies are created for the sole purpose of enticing insiders without their knowledge. No matter what pathways insiders choose to make use of to gain access to certain documents, databases, etc., if there is strategic placement of incognito honeypots all throughout the system, then the insider will be more likely to interact with these honeypots and less likely to evade detection.

Another beneficial use of technology is the use of auditing, authorizing and logging users' activity within the network. Security personnel may be more likely to identify insider threats by auditing their network activity and comparing it to known patterns of adversarial insider activity (Ball et al., 2013). Auditing may also include the identification of common behavior of certain users, making it easier to identify irregular activities or behaviors (Slocombe, 2014). Not only must employees be audited and monitored, but the properties of individual documents (such as the information they contain and even how many times and for how long they were accessed) must also be examined and taken into consideration in order to determine whether or not they are playing a role in an insider attack (Andrews et al., 2004). Companies must also ensure that certain employees are authorized to gain access to certain systems, documents, etc. through authorized devices. According to Slocombe, this is one of the primary means of cyberattack prevention (2014).

Other Technological Approaches

Other basic forms of technology that can aid in the prevention of insider threats worth mentioning include firewalls and virus scanners (DOD, n.d.). Steele and Wargo discuss the importance of a secure, encoded communication software as well. The U.S. Department of Homeland Security also provides an extensive list of security technologies for preventing insider threat attacks in their advisory report "Combatting the Insider Threat" (2014), such as data access monitoring and control, data loss prevention, crowd-source security, etc.

Many companies rely solely on technology as a means of protection against insider threats. Because of their advanced knowledge of the company's network, systems and means of security, technology alone cannot prevent insiders from attacking. Although technology plays a major role in the prevention of insider threats, it takes a more holistic approach from the entire company in order to prevent insider threats more efficiently, as well as be better prepared for when they do occur. One way in which companies can do this is through the implementation of effective security management by using risk management documents, such as the Department of Homeland Security's National Infrastructure Protection Plan 2013, as well as conducting risk, threat and vulnerability assessments.

Risk Management

NIPP 2013 Risk Management Framework

The National Infrastructure Protection Plan (NIPP) is a document produced by the Department of Homeland Security in an effort to "Identify, deter, detect, disrupt, and prepare for threats and hazards to the Nation's critical infrastructure" (something to note is that the NIPP discusses the protection of critical infrastructure; for the sake of this paper, critical infrastructure will be substituted with companies' information, technology and human assets) (2013, p.1). In order to do this, the NIPP emphasizes the importance of effective risk management. The risk management framework is designed to be flexible, meaning it can be used throughout the public sector (government agencies) as well as the private sector (privately owned companies). It is also intended to be used in changing security environments given that risks, threats and hazards are constantly changing (2013). This is important given that insider threat pathways within a company's system are also constantly changing. The NIPP lists and explains five steps of its risk management framework: set infrastructure goals and objectives; identify infrastructure; assess and analyze risk; implement risk management activities; and measure effectiveness.

In step one of the risk management framework, the company identifies and sets infrastructure goals and objectives. Essentially, these are the end goals that the security managers desire for their company (2013). In this case, the end goal would be the protection of company assets from insider threats.

In step two, security managers identify those assets they wish to protect. These assets must be essential to the continued operation of the company; that is, if these assets were stolen or destroyed, the company would shut down. The NIPP states that not only should security managers identify those assets which ensure the continued operations of the company, but also the operations regarding the delivery of products and services to its customers (2013). Once identified, risk managers label the criticality of the assets to the company. In this case, the assets would focus on information vital to the company's mission.

The third step of the risk management process is assessing and analyzing risk (this process will be explained more thoroughly in the next section regarding THIRA). The DHS's Risk Lexicon defines risk as "the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences" (2010, p. 27). The NIPP explains that a risk assessment is a tool used by security managers in order to inform their own decision making regarding protective and responsive means of security. Essentially, risk managers identify all possible risks to their companies and assets and label these risks either quantitatively (number scales that the company has determined) or qualitatively (usually low, medium, and high) based on their criticality and likeliness to occur. In order to do this, however, companies constantly obtain new and reliable information regarding their vulnerabilities, the risks that threaten them and the consequences that may result in an attack. In this case, the security managers would identify who is at risk for turning adversarial insider on the company, how likely is it for these individuals to cause damage, and what the results would be if they did.

The fourth step is to implement risk management activities. Once security managers have identified and labeled their assets and the risks that threaten them, they implement risk management activities to "Identify, Deter, Detect, Disrupt, and Prepare for Threats and Hazards . . . reduce vulnerabilities . . . [and] mitigate consequences" (2013, p. 1) based upon the criticality scores of their identified assets and risks. In this case, security managers may implement certain policies regarding the use of or access to certain technologies and information systems in an attempt to prevent insider threats. Something security managers must take into consideration at this step is the cost of these risk management activities.

The final step in the risk management process is to measure the effectiveness of the risk management activities. Essentially, security managers whether or not the means of risk management aid in the accomplishment of their objectives and goals identified in the first step. If they do, then the risk managers have accomplished their goal of risk management. If they do not, the risk managers must identify flaws in the process. One final note regarding the NIPP's risk management process is that it is a continuous process; that is, due to the constant changing nature of risks and threats, as well as their possible vulnerabilities, companies must constantly identify, analyze and updating their information regarding their assets, vulnerabilities, risks, threats and management activities to ensure optimal protection.

Risk Assessment

Another means of protection against insider threats is the Threat and Hazard Identification and Risk Assessment process (THIRA). The DHS Risk Lexicon defines a risk assessment as a "product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making" (2010, p. 28). The NIPP compliments the THIRA process regarding risk identification and prevention given that the THIRA process utilizes the five core capabilities described in the NIPP: prevention; protection; mitigation; response; and recovery (DHS, 2013). Essentially, the THIRA process is a tool used by communities (or in this case companies) in order to identify their capability targets and resource requirements for possible risks (DHS, 2013). Like the NIPP, the THIRA process is very flexible and can be used in a multitude of different environments. In the DHS's Threat and Hazard Identification and Risk Assessment Guide, it states that in order for the process to be efficient, the entire community (company) must be actively involved (2013). There are four steps in the THIRA process: identify the threats and hazards of concern; give the threats and hazards context; establish capability targets; and apply the results.

The first step of the THIRA process is to identify the threats and hazards of concern. In this step, the company would develop a list of site-specific threats and hazards that could cause damage to the company and its assets. This list defines different types of threats and hazards to identify, as well as different factors to consider when defining the list (DHS, 2013). Companies should utilize a number of different sources to ensure that all possible threats and hazards have been identified. Once that is complete, they should only include those threats and hazards that have been identified to be the most likely to occur and to cause significant damage to the company and its assets (DHS, 2013). Regarding insider threats, the company would focus solely on "Human-caused incidents, which result from the intentional actions of an adversary, such as a threatened or actual chemical attack, biological attack, or cyber incident" (DHS, 2013, p. 6). The company would identify different threats that the adversarial or unintentional insider would pose to the company, how likely these actions are to occur, and the significance of an attack. These threats could include the different pathways that insiders would take in order to infiltrate and steal information from systems.

Step two of the THIRA process is giving the threats and hazards context. In this step, the company is simply adding context to the identified threats and hazards from the first step. According to the DHS's THIRA guidebook, "context descriptions outline the conditions, including time and location, under which a threat or hazard might occur" (2013, p. 9). It states that, because the conditions will differ, companies should develop more than one context description for each threat (2013). Regarding insider threats, context may include who could possibly conduct an attack, when they may attack and under what circumstances i.e. their pathways.

The third step of the THIRA process is to establish capability targets. According to the guidebook, "capability targets define success for each core capability based on the threat and hazard contexts developed in Step 2" (2013, p. 23). Core capabilities refers to the five core capabilities described earlier (prevention, protection, etc.). Capability targets define both the impacts and desired outcomes of the threats and hazards identified in the previous steps. The impact defines how a threat or hazard will affect a company's core capabilities, whereas the desired outcome defines the timeframe and level of effort necessary to successfully deliver the five core capabilities (2013). Because it defines the success of the core capabilities, the guidebook states that the capability targets should be measurable, whether quantitatively or qualitatively depending on the company's preference (2013). Regarding insider threats, the company would identify the impact of an insider attack on its network and systems as well as the timeframe it would take in order to successfully deploy the five core capabilities in order to properly prepare for, prevent and respond to insider threats.

The final step of the THIRA process is applying the results. In this step, the company identifies the resources required to meet the capability targets (DHS, 2013). Each company should identify exactly what combination of resources provides optimal protection from insider threats, as well as response to insider threats should they occur. These can include certain technological means of security such as intrusion detection systems and firewalls, updated policies and procedures, and even different means of copying information and data.

Threat Assessment

Another means of identifying and preventing insider threats is conducting a threat assessment. A threat can be defined as any natural, man-made or technical action, individual, occurrence, etc. that has the potential to harm life or other assets (DHS, 2010). The DHS Risk Lexicon defines a threat assessment as a "product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property" (2010, p. 37). A threat assessment is essentially a simplified version of the THIRA process; that is, where the THIRA process focuses on identifying potential threats and hazards, the conditions of the threat and hazards and the response and resources of the company, a threat assessment simply identifies the threats and undesired events that may occur. According to Biringer et al., "estimating the threat potential for the insider threat is probably the most daunting task of security risk managers. The task is socially, politically, and legally sensitive, and it is technically challenging to protect against the trusted insider" (2007, p. 69). Biringer et al. state that the insider threat spectrum (that is, who has the possibility of being an insider threat and the possible actions they will undertake) must be defined in order to establish an efficient security protection system (2007). As with the NIPP 2013 risk management process and the THIRA process, an insider threat assessment should quantitatively or qualitatively define the levels of risks and threats for possible insiders, qualitatively being the preferred (levels of low, medium and high). Once the possible insiders have been identified and their actions (undesired outcomes) analyzed, the company will have essentially defined which categories of employees are more likely to turn insider. Something important to note that Biringer et al. discuss is that "all employment positions at a facility should be included in the threat analysis. Any employee may pose a potential insider threat, even trusted managers and security personnel" (2007, p. 334).

Vulnerability Assessment

One final means of identifying and preventing insider threats is the conducting of vulnerability assessments. The DHS Risk Lexicon defines a vulnerability assessment as a "product or process of identifying physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards" (2010, p. 39). Companies may hire an outside assessment agency or use their own security manager(s) to identify and assess different vulnerabilities within the company that may pose a threat to its assets. Dr. Ryan Baggett, a Homeland Security professor at Eastern Kentucky University, states that "Protective Security Advisors are available in every state to assist with infrastructure security and resilience needs. Upon request, the PSA will conduct a site assistance visit at the critical infrastructure site" (personal communication, October 15, 2016). He goes on to state that the assessment tool that the PSAs (and possibly security managers) use evaluate "six components within the categories of information sharing, security management, security force, protective measures, physical security and dependencies" of the company (personal communication, October 15, 2016). Regarding insider threats, the company should focus on cybersecurity and possibly even physical security. Once all vulnerabilities have been identified and assessed, the company will be able address these issues and improve its security.

The use of government documents and guides such as the National Infrastructure Protection Plan, as well as the conducting of risk, threat and vulnerability assessments can be effective in identifying and preventing insider threats. However, in order to mitigate threats, companies must take a more holistic approach to the issue. By taking a holistic approach, companies will not only update policies and training, improve the work environment, and ensure the best employees possible are employee, they will also include every employee and department within the company to ensure that everyone is properly prepared for and protected against insider threats.

Holistic Approach

As discussed previously, identifying and preventing insider threats cannot be accomplished through the use of technology alone. In fact, Colwill states that "Experience shows that an overreliance on technology without consideration of other factors can have disastrous results for managing the insider threat" (2009, p. 186). In their report regarding the thwarting of insider attacks, Magnuson and Sicard state that the last step companies should take when attempting to protect information from insider threats is to implement more computer programs (2015). Additionally, they state that companies wishing to improve protection against insider threats cannot strengthen one means of protection (such as the use of technology) while sacrificing another (such as training) (2015). In a separate article, Magnuson quotes Douglas Thomas, head of corporate counterintelligence at Lockheed Martin Corp, and Dawn Cappelli, director of insider risk management at Rockwell Automation, stating that the solution for insider threats is not solely technical; rather, "an insider threat program needs to be holistic. It needs to look at the person. It needs to looks at technical behaviors as well as non-technical" (2013, p. 30). However, in order for this to occur, managers and security personnel need to recognize that there is a problem and that the proper steps must be taken in order to prevent it from happening. Magnuson and Sicard identify five reasons why executives tend to shy away from the insider threat problem: "denial, lack of guidance, complexity, funding and not knowing of the problem" (2015, p. 10). Steele and Wargo add ignoring the threats due to the technological complexity as well as the fact that managers may not want to accept that their "family" or employees would do such a thing (2007). Another possible reason could include the complex legal and political issues that come with observing employee behavior (Biringer et al., 2007). Whether it be through denial, a lack of knowledge or just ignoring the problem due to its complexity, nothing can be done about the insider threat problem until managers accept that it is a growing and prevalent issue and take a holistic approach to prevent it from occurring. One of the ways that managers can accomplish this is by updating and posting the company's security policies.

Policies and Procedures

Properly posting and explaining the company's policies and procedures is an excellent aid in preventing insider threats. Something to note is that there is no "one size fits all" stance when it comes to security policies and procedures (Steele and Wargo, 2007). Rather, companies must identify their assets and objectives in order to create a solid, efficient list of policies and procedures. Once companies have identified their security needs, it is essential that they clearly communicate these policies and procedures to all employees within the company. Magnuson quotes Douglas Thomas stating "there must be a companywide, robust communications strategy to let employees know about any counter-insider threat program" (2013, p. 31). He continues quoting Thomas, stating that everyone needs to be included in this "holistic solution" (2013). These policies and procedures can be used as a means of deterrence for possible insiders. In a report regarding employee characteristics and cybersecurity policies issued to the U.S. Department of Homeland Security, authors Carter et al. explain deterrence theory as it relates to policy violations: "deterrence theory suggests that individuals will be deterred from performing undesirable behavior (e.g. crime, computer abuse, policy violation) if they perceive that there will be punishments or sanctions which are certain, severe, and swift" (2012, p. 4). In essence, if employees perceive that they will be severely punished for violating the policies and procedures explained to them, then they are less likely to do so. However, in order for this to work efficiently, companies must follow through with punishments as swiftly as possible once the violation has been identified. Something important to note is that these policies not only pertain to physical and cyber violations; they include anything that they perceive may cause damage to the company and its assets, such as drug and alcohol use.

Ad/Marketing Campaigns

One specific policy that companies should instruct their employees on is the DHS's "If you See Something, Say Something" campaign. According Reeves, the campaign is "a renewed drive to redistribute surveillance responsibilities to the public" (2012, p. 235). In essence, this campaign was created by DHS in order to make it easier for civilians to report suspicious terroristic behavior, but it works just as well with employees reporting adversarial insiders. With the implementation of this campaign, employees should be informed on suspicious behavior to watch out for, as well as how to determine whether or not a fellow employee is attempting to manipulate them into aiding them commit an attack (Colwill, 2009). However, there are negative consequences that coincide with this campaign as well. Reeves explains that there may be legal issues regarding libel that could result in reporting coworkers for insider threat activity (2012). Also, as Magnuson puts it, "nobody likes a snitch", and therefore employees may be reluctant to report others employees, even if they suspect insider activity (2013). However, if employees are properly informed on company policies and procedures, this campaign should be a benefit rather than a hindrance in preventing insider threats.

Training

Along with the lack of policies and procedures is the lack of proper training for employees. According to Colwill, "education, training and awareness are perhaps the greatest non-technical measures available and a common theme for human factors and security" (2009, p. 193). Instructing employees on the policies and procedures of the company is one thing, but in order to be truly effective, old habits must be broken through proper training (Colwill, 2009). Martin Hershkowitz puts it perfectly in his report on minimizing insider threats when he states that:

> Training may be one of the most complex but necessary components of an anti-insider threat program. In addition to exposing the employees to the extent of the program they will be required to undergo in order to be a member of the HS/HD team, all employees and management should be trained to recognize those characteristics that imply that the individual displaying those characteristics may be a saboteur, terrorist, criminal or simply dangerous person for their mission(s) and how to handle the next steps. (2007, p. 110).

The DHS lists a number of different training programs that companies should utilize in their report on combating insider threats. These programs include identifying phishing and other online threats, maintaining proper skill and abilities levels, enhanced awareness of unintentional and adversarial insider threats, and even improved use of security tools (2014). Having said that, one of the most essential part of any training program is that the employees understand that the programs and their corresponding levels of security are essential for preventing insider threats (Colwill, 2009). If employees believe that the levels of security are overbearing, it could lead to reduced loyalty and a greater potential for insider threats. Thus, the training programs would be counterproductive.

Human Resources

Not only must companies implement proper training programs, but proper investigation and examination programs as well. According to Steele and Wargo, "organizations must realize that HR is the first line of defense against malicious insiders. HR must do a better job of screening prospective employees. This includes thorough background checks on employment, criminal, and credit history" (2007, p. 30). The Department of Defense explains that companies should establish a psychological baseline for employees in order to identify those who may be more likely to turn insider. Once this baseline has been set, it states that all employees in high-stress positions should undergo a complete psychiatric examination to determine if they are fit to hold their position without turning insider. It explains that this process should continue every two or three years depending on the company's resources. The DOD also states that companies should be continuously testing for illegal drug and alcohol use as well. Finally, it discusses the importance of conducting thorough background investigations on all employees, including any local, state or federal criminal charges and financial information (n.d.). As mentioned previously, these could be possibly motivations as to why employees turn insider.

It has been argued by many authors cited in this paper that the holistic approach is the key to preventing insider threats. By taking a holistic approach to the problem of insider threats as opposed to relying on technology, all employees become more involved with the mission and objectives of the company. As discussed previously, this feeling of importance and belonging can lead to increased loyalty to the company, and thus reduce the total number of employees turning insider.

Conclusion

The purpose of this research paper was to discuss the growing issue of insider threat to companies and to explain the importance of using preventative measures of security rather than reactive measures. It was hypothesized that there are certain characteristics and behaviors that insider threats exhibit that make them stand out from the rest of the company's employees. It was then hypothesized that once companies identify these characteristics and behaviors in their employees, they would be able to prevent them from comprising the companies' assets. The third hypothesis was that, once these characteristics have been identified, companies would be more successful at preventing insider threats by using a hands-on holistic approach to the preventative means of security along with layers of technological means of security. Before testing these hypotheses, a working definition of insider threat had to be established. Once that was completed, research was conducted on the different characteristics and behaviors that insider threats exhibit in the workplace. The motivations of those who had turned insiders were also analyzed as a means of attempting to prevent others from turning insider as well. There were many characteristics, behaviors and motivations identified that separate insider threats from the rest of the company's employees, thus proving the first hypothesis to be correct. The next step was to identify technological means of security that aid in preventing insider threats. A few of these were identified and briefly discussed. The final step was to identify the means by which companies can take a holistic approach to preventing insider threats. Along with this, research was conducted on the effectiveness of these preventative means, showing them to be efficient in preventing insider threats from occurring, although not completely. Because of this, both the second and third hypotheses were shown to be correct.

The information presented in this study could be reexamined and reused in the future in order to determine whether or not these preventative means of security are effective against insider threats. In order to do this, researchers would have to analyze the different preventative means of companies and determine how many insider attacks have been prevented and how many have succeeded. This would include not only identifying the detection, prevention and auditing capabilities of the technology implemented at the company, but also the security policies, training programs and other holistic approaches to the problem. Researchers must work closely with security managers at these companies to analyze and determine the effectiveness of preventative means of security.

The reason this research topic is important is due to the amount of physical and financial damage that insider threats can cause to a company as discussed in the introduction. As stated, the average insider attack can cost up to fifty times that of an outsider attack, which can be within the millions range. Not only can an attack cause physical and financial damage to the company, but to the public and the economy as well. It is also important given that the insider threat issue has been steadily growing since 2004. Because of this, it is vital that companies utilize preventative means of security in order to protect their information (and others) assets from attack.

References

Andrews, M., Thompson, H. H., & Whittaker, J. A. (2004). Intrusion detection: Perspectives on the insider threat. *Computer Fraud & Security*, *2004*(1), 13. doi:10.1016/S1361-3723(04)00018-1

Agrafiotis, I., Buckley, O., Creese, S., Goldsmith, M., Legg, P., & Nurse, J.R.C. (2015). *Identifying attack patterns for insider threat detection*. Oxford, England: University of Oxford.

Ball, L. J., Dando, C. J., Jenkins, M. C., Menacere, T., Ormerod, T. C., Sandham, A., & Taylor, P. J. (2013). Detecting Insider Threats Through Language Change. *Law & Human Behavior (American Psychological Association)*, *37*(4), 267-275. doi:10.1037/lhb0000032.

Biringer, B. E., Matalucci, R. V., & O'Connor, S. L. (2007). *Security risk assessment and management: A professional practice guide for protecting buildings and infrastructures*. Hoboken, NJ: John & Wiley Sons Inc.

Butavicius, M., McCormac, A., & Parsons, K. (2012). *Preventing and profiling malicious insider attacks*. Edinburgh, South Australia: Command, Control, Communications and Intelligence Division.

Cappelli, D. M., Desai, A. G., Moore, A. P., Shimeall, T. J., Weaver, E. A., & Willke, B. J. (2007). *Management and education of the risk of insider threat: System dynamics modeling of computer system sabotage*. Pittsburgh, PA: Carnegie Mellon University.

Carter, L., McBride, M., & Warkentin, M. (2012). *Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies*. Retrieved from https://www-hsdl-org.libproxy.eku.edu/?abstract&did=728046.

Center for the Protection of National Infrastructure. (2013). *CPNI insider data collection study report of main findings*. Retrieved from http://www.cpni.gov.uk/Documents/Publications/2013/2013003-insider_data_collection_study.pdf.

CERT Insider Threat Team. (2013). *Unintentional insider threats: a foundational study*. Retrieved from https://www-hsdl-org.libproxy.eku.edu/?abstract&did=741559

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days?. *Information Security Technical Report*, *14*(4), 186-196. doi:10.1016/j.istr.2010.04.004

Dictionary.com. (2016). Hacker. Retrieved from http://www.dictionary.com/browse/hacker?s=t

Hershkowitz, M. (2007). The “Insider” Threat: How to Minimize It. *Journal of Police Crisis Negotiations*, 7(1), 103-111.doi: 10.1300/J173v07n01_06

Jeong, D. H., Liang, L., Yu, B., & Zeadally, S. (2012). Detecting Insider Threats: Solutions and Trends. *Information Security Journal: A Global Perspective*, *21*(4), 183-192. doi: 10.1080/19393555.2011.654318

Liang, L., Jeong, D. H., Yu, B., & Zeadally, S. (2012). Detecting Insider Threats: Solutions and Trends. *Information Security Journal: A Global Perspective*, *21*(4), 183-192. doi:10.1080/19393555.2011.654318

Magnuson, S. (2013). Companies Ill-Prepared to Fend off Insider Threats. *National Defense, 98*(720), 30-31.

Magnuson, S., & Sicard, S. (2015). Experts: Thwarting Insider Threats Takes a Holistic Approach. *National Defense, 99*(735), 10-11.

Norman, T. L. (2016). *Risk analysis and security countermeasure section*. Boca Raton, FL: CRC Press.

Panda, B. & Yaseen, Q. (2012). Insider threat mitigation: preventing unauthorized knowledge acquisition. *International Journal of Information Security, 11*(4), 269-280. doi: 10.1007/s10207-012-0165-6.

Reeves, J. (2012). *If you see something, say something: Lateral surveillance and the uses of responsibility*. Raleigh, NC: North Carolina State University.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security, 21*(6), 526-531.

Slocombe, G. (2014). Beware the insider attack. *Asia-Pacific Defense Reporter, 40*(8), 36-37.

Spitzner, L. (2003). *Honeypots: catching the insider threat*. Retrieved from http://craigchamberlain.com/library/insider/Honeypots%20-%20%20Catching%20the%20Insider%20Threat.pdf

Steele, S., & Wargo, C. (2007). An Introduction to Insider Threat Management. *Information Systems Security*, *16*(1), 23-33. doi:10.1080/10658980601051334

United States Department of Defense. (n.d.). *Insider threat mitigation: Final report of the insider threat integrated process team*. Ft. Bellvoir, VA: Defense Technical Information Center.

United States Department of Homeland Security. (2010). *DHS risk lexicon*. Washington, DC: Government Printing Office.

United States Department of Homeland Security. (2013). *National infrastructure protection plan 2013*. Washington, DC: Government Printing Office.

United States Department of Homeland Security. (2013). *Threat and hazard identification and risk assessment guide*. Washington, DC: Government Printing Office.

United States Department of Homeland Security National Cybersecurity and Communications Integration Center. (2014). *Combating the insider threat*. Washington, DC: Government Printing Office.