EXAMINATION OF INSIDER THREATS: A GROWING CONCERN

by

Cecil L. Hartline Jr.

A Capstone Project Submitted to the Faculty of

Utica College

December 2017

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity

Abstract

The National Infrastructure Advisory Council (NAIC) reports that "…preventing all insider threats is neither possible nor economically feasible…" because the threat is already behind perimeter defenses and often know exactly where vulnerabilities exist within organizations (Cline, 2016). The purpose of this research was to determine the prevalence of malicious and unintentional insider threats. Statistically, the numbers support the idea that insider threats are increasing and occurring more frequently. The true numbers, which only account for the incidents that were reported, may be higher than originally expected. The statistical numbers are likely to much higher because organizations fear reputational damage and client loss. Organizations give reasons such as not enough evidence for conviction or too hard to prove guilt. The result of the paper indicates that companies focus most of their resources on external threats and not the insider threat that is costlier to remediate and considered the most damaging of all threats. The research focuses on malicious and unintentional insider threats and how they are different. A 2018 Crowd Research Partners report found 90% of organizations believe they are vulnerable to insider attacks, while 53% of businesses confirmed they had experienced an insider threat in the past 12 months (Crowd Research Partners, 2017a). The insider threat is hard to manage because an organization not only need worry about their own employees they also must monitor and manage third-party vendors, partners, and contractors. However, with a combination of technical and nontechnical solutions, including an insider threat program, companies can detect, deter, prevent or at least reduce the impacts of insider threats. Keywords: Cybersecurity, Professor Christopher Riddell, Professor Duane Corbo, insider threat, malicious insider, unintentional insider, social engineering, phishing, business email compromise.

Acknowledgements

I would like to extend my sincerest gratitude and appreciation to all the patient individuals who helped me accomplish this capstone project. A very special thank you to my Capstone Chair Professor Christopher Riddell, Co-Chair Professor Duane Corbo, and my second reader, and friend, Jason Tuttle. Your time and constructive feedback was an integral part to my success and could not have happened without your involvement. I would also like to thank the Utica College Cybersecurity staff who I have had the pleasure of working with during this time. I would like to thank each of them for their time, passionate participation, and hard work striving to make each course better for the next set of graduate students. Special thanks go to my success coach Anna Robinson who was essential to my success and in keeping my eyes forward on the important things.

I would like to extend my deepest gratitude to my son Jonah Hartline for his patience with me over the last three years in my pursuit of this degree. I would like for him to know that despite lost time it was he who inspired me to complete my goal. I would also like to thank all family members for their support and encouragement along the way.

Table of Contents

Examination of Insider Threats: A Growing Concern

Technological advances, including the explosion of the Internet, has altered traditional methods of how people collect, store, process, and communicate sensitive information. These changes have increased the capability of an insider to successfully steal confidential information, while reducing the likelihood of being identified, therefore, creating a low-risk, high-reward opportunity. Moreover, a Threat Intelligence 2017 Predictions Report, conducted by Chief Research Intelligence Analyst Stephen Gates and Senior Intelligence Researcher Cody Mercer stated the most significant attack vector for any organization is the insider threat (Gates and Mercer, 2017).

The Computer Emergency Response Team (CERT) Insider Threat Center at Carnegie Mellon's Software Engineering Institute (SEI), in partnership with the Department of Defense (DoD), the Department of Homeland Security (DHS), the United States Secret Service (USSS), and other federal agencies, formerly acknowledges the significance of the insider threat (CERT, 2017a; Cole, 2017). For the last 17 years, CERT at Carnegie Mellon's University SEI conducted research and analysis resulting in the creation of a database currently containing over 1000 real-world insider threat cases (CERT, 2017a). CERT not only collected empirical insider threat cases, but they also followed up by examining them from a technological and behavioral perspective. The study evolved over the years resulting in the creation of controls, publishing best practices, identifying unique behavioral patterns, and furthered the development of models and simulators to create and test techniques which can be used to detect and possibly prevent an insider attack.

The purpose of this research was to examine the prevalence of insider threats, their types and subtypes, the risks they present to organizations, and what can be done to prevent or reduce

their impact. This study will answer three questions: What are insider threats to cybersecurity? What threats do insiders present to organizations? What mitigation strategies and options have been implemented or suggested to address the insider threat problem?

Statement of the Problem

This research begins by developing a combined working definition of malicious and unintentional insider threats. Additionally, it defines the types of insider threats, offers examples of insider threats, the threats they present, and evaluates possible mitigation strategies for detecting, deterring, preventing, or at least reducing the effects caused by insider threats.

A posting by Danial Costa, March 7, 2017, in a Software Engineering Institute blog for Carnegie Mellon University, states the current definition of an insider threat, malicious insider threat, and unintentional insider threat. The revised CERT definition states: "Insider Threat - the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization" (Costa, 2017). The revised definition combines both malicious and unintentional insiders replacing the original definitions that were separate and specific. The new definition is generalized and addresses insider threats as individuals who have or had privileged access and who act "either maliciously or unintentionally" in a way which could "negatively affect" organizations.

Upton and Creese (2014) stated in the Harvard Business Review described insider threats as the following;

> Insider threats come from people who exploit legitimate access to an organization's cyber assets for unauthorized and malicious purposes or who unwittingly create vulnerabilities. They may be direct employees (from cleaners up to the C-suite), contractors, or third-

party suppliers of data and computing services. (Edward Snowden, who famously stole sensitive information from the U.S. National Security Agency (NSA), worked for an NSA contractor. With this legitimate access they can steal, disrupt, or corrupt computer systems and data without detection by ordinary perimeter-based security solutions – controls that focus on points of entry rather than what or who is already inside.

Organizations face challenges presented by insider threats regardless if malicious, unintentional, negligent, or caused by infiltrators. While cybersecurity professionals are still concerned with outside threats, the primary focus has shifted to non-malicious and malicious insider attacks. For example, in 2014, IBM reported that 31.5% of cybersecurity incidents were associated with malicious insiders, and 23.5% associated with non-malicious insiders (Scott, & Spaniel, 2017).

Dtex Systems, a global threat protection company, has dedicated the past decade to studying and fighting insider threats, arming organizations around the world with revolutionary technology helping to protect against insider threats (2017). The 2017 Insider Threat Intelligence Report conducted by Dtex Systems, describes three additional subtypes in addition to the revised CERT definition. Dtex Systems defines three types of malicious and unintentional threats as malicious users, negligent users, and infiltrators. Malicious users are those who intentionally cause harm to organizations most often by stealing sensitive information, intellectual property, and trade secrets. Unintentional negligent users are unwitting insiders who, through inadvertent negligence, may unknowingly cause a security breach. Dtex Systems describes infiltrators as those individuals who penetrate organizations by taking advantage of human and technological weaknesses. Indirectly, infiltrators are associated with insider threats because they manipulate or

coerce unsuspecting insiders to create a security vulnerability using tools such as ransomware and credential stealing as attack vectors (2017).

According to Tripwire (2017), insider threats present themselves in many ways and may very well be the main security threat of 2017. A recent lawsuit reported by The Guardian involving Waymo, formerly Google's self-driving car division, accused Anthony Levandowski of stealing 14,000 files and taking them directly to his new employer Uber (Tripwire, 2017; Harris, 2017). The authors further explain that Levandowski quickly set up a company after stealing Waymo's Intellectual Property (IP) which was then acquired by Uber for 680 million dollars.

While Levandowski's actions were malicious, Tripwire explains all insider threats are not inherently malicious. Unintentional insider threats may involve negligent employees inadvertently causing data breaches and daily data leaks either accidentally or through outside manipulation. Tripwire further explains why insider threats are costly to remediate and tough to deal with (2017). Tripwire describes cost and difficulty as being directly related to the following reasons; insider threats may persist for years before being detected, challenging to distinguish harmful actions from regular work, natural for savvy users to cover their tracks, and hard to prove guilt.

A 2018 Crowd Research Partners report surveyed 472 cybersecurity professionals and found 90% of organizations believe they are vulnerable to insider attacks, while 53% of businesses confirmed they had experienced an insider threat in the past 12 months. The survey also points out 27% of the surveyed cybersecurity professionals feel insider threats have become more frequent (Crowd Research Partners, 2017a). Additionally, the study discussed the risk factors of these attacks and concluded 37% were due to excessive access privileges, 36% due to

the increasing number of devices having access to sensitive information, and 35% caused by the rising complexity of information technology (IT).

Levandowski is an example of a malicious insider threat because his actions were harmful and intentional. According to Dtex Systems (2017), a negligent user causes security breaches but does so accidentally, without intent. For example, a malicious actor sent an email to a financial services firm containing a long-time customer's name and email address. The investment manager had no reason to question the request to transfer $100,000 to an offshore account because it contained what appeared to be a legitimate request providing detailed personal information which the infiltrators obtained through the client's social media accounts. The email turned an experienced investment manager into an unwitting accomplice in a six-figure heist (AT&T, 2016).

Infiltrators are outside the organization, but they are considered insider threats because they take advantage of the human element and technological weaknesses within an organization. Email phishing attacks take advantage of an innate human weakness making an organization’s users the weakest link. According to Dtex Systems, a financial firm employee clicked on what appeared to be a Dropbox email notification which contained a link to an executable file disguised as a PDF file. The infiltrator fooled the user into clicking on the Dropbox link which downloaded a virus to the employee’s computer. Because the victim was a savvy user, the employee deleted the file after realizing it was suspicious, but not before it was able to replicate and spread. Furthermore, the virus was not detected by the organization's anti-virus system because it was an unknown variant. The infiltrator created a scenario where the employee unknowingly contributed to a cyber attack against their institution by using a sophisticated social engineering attack (2017).

To further develop an understanding of the insider threat problem Tripwire (2017) explains 53% of companies estimate remediation cost to be $100,000, while 12% estimate remediation costs to be more than 1 million dollars. Furthermore, 74% of companies feel they are vulnerable to insider threat attacks, with 12% reporting an extreme vulnerability to insider attacks. Moreover, a Ponemon 2016 Cost of Breach Study indicated healthcare, education, and finance as the top industries spending most on remediating data breaches (2016).

A Ponemon 2016 Cost of Data Breach Study (as cited in Tripwire, 2017) states, there were 874 incidents, where the employee or contractor's negligence caused 568 breaches. Of these 874 incidents, 85 were due to outsiders using stolen credentials and 191 by malicious insider employees. Cole (2016) stated in 2015, malicious insider threats accounted for the costliest attacks, at approximately $144,000 per incident. Additionally, the author states the more significant issue is the unintentional insider or instances where an external entity manipulates an unwitting accidental insider employee. Moreover, the author further describes the insider threat as the "silent killer" for most organizations.

Tripwire describes insider threat problems faced by organizations as costly to remediate and difficult to prevent. Insider threats are more expensive to remediate because they can persist for long periods of time before being detected (2017). The longer the attacks occur, the higher the cost to remediate. Another problem is when an employee already works with sensitive information making it difficult to distinguish if employees are acting maliciously or performing regular work. If the employee is technically savvy, it makes it difficult to detect while it is happening and even more challenging to discover after the attack has finished (Ponemon, 2016; Tripwire, 2017). A person with adequate computer skills will cover their tracks, for example, by deleting or modifying log files which can reveal malicious activity. Proving guilt is likely the

most challenging part of dealing with insider threats. For example, a guilty employee may say it was human error or just write it off as a mistake (Tripwire, 2017).

According to AT&T, there are several new and dangerous avenues of attack for malicious insiders. The Internet of Things (IoT) is growing at an alarming rate and is estimated to reach 50 billion "things" by 2020. Mobility and Bring Your Own Device (BYOD) privileges have gained widespread use in organizations because of their proven productivity benefits. Extended supply chains help optimize logistics by linking third-party agencies such as contractors, suppliers, and partners with internal business systems. The link places more data in the hand of insiders at multiple companies whose security practices and policies are beyond the IT departments control (2016). Business Email Compromise (BEC) relies on spear-phishing emails while ransomware campaigns are having a significant impact involving innocent insiders who become victims of the attack. According to FBI (2017), BEC and email account compromise (EAC) continues to grow targeting businesses of all sizes. In fact, between January 2015 and December 2016, there was a 2,370% increase in identified exposed losses with fraudulent transfers sent to 103 countries.

Chief Executive Officer for Haystax Technologies Bryan Ware, reported organizational barriers are the primary reason preventing the development of a sound threat management program. The study included over 300,000 members of the Information Security Community (ISC) on LinkedIn and Crowd Research Partners (CRP). According to Ware (2017), the three top barriers for businesses are lack of training and expertise (60 percent), insufficient budgets (50 percent), and lack of collaboration between departments (48 percent).

K. Narayan (2017) reported that only 17% of IT security professionals were even aware of insider threats, although usage data from Skyhigh's latest Cloud Adoption and Risk Report Q4

2016 indicated 85% of the organizations studied had such threats. The question remains, why are insider threats so challenging for organizations? (Sagan, 2017; Trzeciak, 2017) argues that successful businesses have employees who are known and trusted by their organizational leaders and fellow employees. The trusted employees may have detailed information, knowledge of security systems and their weaknesses while taking months or years to plan their attacks. For these reasons, Sagan (2017) suggests insider threats will continue to escalate leaving future leaders of the U.S. struggling with the significant amount of work regarding the mitigation of insider threats involving highly sensitive information.

Verizon's 2017 Data Breach Investigations Report revealed the insider threat in the healthcare industry as a significant concern. The healthcare industry is the only industry where employees are the predominant threat actors in cyber breaches (Verizon, 2017). Within the healthcare industry, there are three patterns of abuse; privilege misuse, miscellaneous errors, and physical theft and loss. According to Verizon (2017), the three pattern types account for 80% of breaches within the healthcare industry. The report also states the healthcare sector suffered 458 incidents, with 296 data disclosures. Of the 458 incidents, 32% were external threats, 68% internal threats, and partner breaches accounted for 6%. The primary purpose of these attacks was to obtain Personally Identifiable Information (PII), primarily used to commit identity theft (Verizon, 2017).

According to Cole (2017), companies are worried about their reputation and the possibility of losing clients, and it stands to reason that the projected percentage of insider threats could be much higher than initially expected due to an organization's reluctance to report insider attacks. Based on a Cybersecurity Watch Survey presented by Padayachee (2016), the suspected 46% of insider threats are likely to be more damaging than those caused by outside attacks. The

survey also suggested the actual percentage could be higher than 50%. As to cost estimates, the Insider Threat Spotlight Report stated above, found over 75% of surveyed organizations estimated remediation costs for insider breaches could reach $500,000 per incident, with 25% believing financial losses will exceed this level, costing millions of dollars (Schulze, 2016).

There are growing concerns facing government agencies regarding their ability to protect sensitive information and the dangers posed by inside employees and outside contractors. According to Willemssen (2015), the U.S. Government Accountability Office (GAO) has identified deficiencies in federal agencies exposing threats the sensitive data and systems. For example, agencies including DHS have weaknesses with the design and implementation of security controls as seen with 19 of the 24 bodies covered in the Chief Financial Officers Act. Furthermore, the author states that most of the 24 agencies continue to have security weaknesses in critical controls such as those responsible for limiting, preventing, and detecting inappropriate access to resources, as well as, managing the configurations of software and hardware. An example would be the 2015 breach of the Office of Personnel Management (OPM). OPM reported there had been an attack on the systems containing personnel records of approximately 4.2 million current and former federal employees. The Director of OPM stated that they had also suffered from an incident that involved its background investigation systems resulting in the compromise of investigation files for 21.5 million individuals.

Research from Lieberman Software Corporation at Microsoft Ignite 2015, revealed that 35% of IT professionals view insider threats presenting a more considerable risk than external cyber attacks, justifying the increased concern surrounding the dangers of insider attacks (Stoneff, 2017). Founder and CEO of Insider Threat Defense, Jim Henderson, added two additional points which contribute to the growing concern surrounding insider threats and the

dangers of data loss and destruction. The Insider Threat Timeline constructed by Henderson included a Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) alert which reported an increase in computer network exploitations and disruptions cause by disgruntled and former employees. It also stated companies who were victims of disgruntled or former employees in 2014 incurred losses from thousands to $3 million while also pointing out that 93% of U.S. based organizations are vulnerable to insider threats (Henderson, 2015).

The National Infrastructure Advisory Council (NAIC) reports that "…preventing all insider threats is neither possible nor economically feasible…" because the threat is already behind perimeter defenses and often know exactly where vulnerabilities exist within organizations (Cline, 2016). A 2017 Dell End-User Security Survey addresses the growing concern of inadequate end-user training. Haber (2017) describes the Dell survey as solicited responses from 2,600 business professionals from eight countries who handle confidential information at companies with more than 250 employees.

Dangers exist because the insider threat is real, problematic, and difficult to combat regardless if an insider is malicious or unintentional. Cole (2017) stated in a SANS 2017 Insider Threat Survey, that “unknown” and “no value placed” losses were highest which indicates most organizations do not have proper monitoring and reporting mechanisms to determine the actual impact of insider attacks. However, more than 40% of respondents showed they were concerned with negative publicity, suggesting that organizations at least recognize the threat and the need to report breaches despite the risk to their reputation and the possibility of fines.

According to Scott and Spaniel (2017), traditional strategies focused on protecting endpoints and mobile devices are no longer sufficient and must evolve to more modern approaches that focus on securing data and monitoring users. The authors further explain that

"insider threats and outsider threats are not different. Protecting data solves both equally." However, combined strategies for protecting data include non-technical policies, procedures and guidelines, and technical solutions such as DLP.

Education and awareness training can inform end-users that committing a cybercrime against a company could result in severe punishment and even prison sentences. SANS (2017) describes time, resources, communication, employee engagement, money, and buy-in from upper management as reasons why organizations find it problematic to implement and maintain a successful cybersecurity program. Furthermore, organizational awareness of insider threats allows for a proactive position to prevent potentially significant damage resulting from insider threats. Increasing awareness of insider threats will allow for a proactive stance to avoid substantial losses as a result of such risks.

There are two models available for reference explaining what needs to be in place before an insider thinks of taking the risk. The first model was developed initially in 1953 and revisited in 2015 by Schuchter and Levi (2016). The Association of Certified Fraud Examiners (ACFE) found that sociologists and psychologists still use the three elements of Cressey's Fraud Triangle including pressure, opportunity, and rationalization when assessing the insider threat (ACFE, n.d.). Additionally, it uses Black's Law Dictionary to define fraud as:

> All multifarious means which human ingenuity can devise, and which are resorted to by one individual to get an advantage over another by false suggestions or suppression of the truth. It includes all surprise, trick, cunning, or dissembling, and any unfair way by which another is cheated.

Understanding why is the first step in detecting and deterring the increasing number of insider threats. For example, disgruntled employees may steal data and leak sensitive information

to damage an organization's reputation. Understanding indicators and psychological factors including pressure, opportunity, and rationalization found in Cressey's Fraud Triangle will help agencies determine who would likely become a threat. Despite being created in the 1950s, Schuchter et al. (2016) revisited the Fraud Triangle explanatory framework and noted its evolution to the Fraud Diamond, and how both methods are still relevant today.

Cline (2016) evaluated Cressey's Fraud Triangle and found that pressure, opportunity, and rationalization were the three factors necessary for an individual to consider committing fraud. Additionally, he states if any of these factors are not present, then the crime is less likely to occur. David Wolfe and Dana Hermanson modified Cressey's model and referred to it as the Fraud Diamond. David Wolfe and Dana Hermanson expanded Cressey's Fraud Triangle to include capability, an individual's traits and ability to commit fraud (ACFE, n.d.). Cline (2016) agrees that even though the other three factors may be present, the individual must also have the capability of intentionally committing the crime.

Eliminating all insider threats is unrealistic, but a good start is to recognize some of the patterns and trends seen in many insider attacks. One such mitigation strategy mentioned in the Common Sense Guide to Mitigating Insider threats, Fifth Edition, involves the appropriate combination of policies, procedures, and technical controls in an attempt to prevent or control the damage caused by insider threats (CERT, 2016).

Justification for Research

Organizations are either not prepared, or at the very least, underprepared to defend against insider threats. For example, Haber (2016) reported in a Dell survey that 65% of employees consider it their responsibility to protect confidential information, while only 36% believe they are confident in how to protect such information. SANS 2017 Insider Threat Survey

sponsored by Dtex, Haystax Technology, and Rapid7 found that 18% of companies have provisions for insider threats, with 49% indicating they are developing such programs. Additionally, the survey found that 40% rate malicious insiders as the most dangerous threat, with 36% rating the accidental or negligent insider as the most damaging. Both are higher than the 23% of those surveyed who considered external threats to be the most damaging (Cole, 2017).

In a majority of cases, insider attacks are unreported leading to the misconception that insider threats are not common and seemingly unappreciated. The CERT Insider Threat blog reported in a post that 72% on average of insider incidents are found to be handled internally without legal action or assistance of law enforcement. A Cybersecurity Watch Survey presented by Padayachee (2016) indicated 46% of insider threats are likely to be more damaging than those caused by outside attacks. The 2013 Cyber Watch Survey also suggested the actual percentage could be higher than 50% since many insider incidents are handled internally and not reported.

Audience

This research examines the increasing concern regarding insider threats to corporate and governmental agencies by recognizing their types, presenting examples, and recommending mitigation strategies that will help prevent, deter, or reduce the effects of this emerging threat. As a result, it will benefit government and corporate leaders, threat awareness trainers, human resource employees, recruiters, and regular employees. It will help to understand the significance of the problem and allow organizational leaders and trainers to develop training programs to aid in preventing or reducing the impacts caused by insider threats.

Literature Review

The Computer Emergency Response Team (CERT) Insider Threat Center at Carnegie Mellon's Software Engineering Institute (SEI), in partnership with the Department of Defense (DoD), the Department of Homeland Security (DHS), the United States Secret Service (USSS), and other federal agencies formerly acknowledges the significance of the insider threat (CERT, 2017a; Cole, 2017)). For the last 17 years, CERT has conducted research and analysis resulting in the creation of a database currently containing over 1000 real-world insider threat cases (CERT, 2017a).

A posting by Danial Costa, March 7, 2017, in a Software Engineering Institute blog for Carnegie Mellon University, states the current definition of an insider threat, malicious insider threat, and unintentional insider threat. The revised CERT definition states: "Insider Threat - the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization" (Costa, 2017).

Insider Threats to Cybersecurity

Regarding insider threats, cybersecurity professionals traditionally focus most of their efforts toward combating outside threats. However, the primary focus has shifted to more challenging non-malicious and malicious insider attacks. For example, in 2014 IBM reported that 31.5% of cybersecurity incidents are malicious insiders, and 23.5% related to non-malicious insiders (Scott, & Spaniel, 2017). In a 2017 Crowd Research Partner Report, only 30% of organizations were extremely confident about their insider threat security posture. The report explains why insider attacks are on the rise beginning with an increase in the number of devices with access to sensitive information accounting for 55%. Mobile devices and web access

accounting for 51% of data leaving the network perimeter, while lack of employee awareness training and insufficient data protection strategies are equally responsible at 50%. Furthermore, the groups of employees who are of highest risk to organizations are regular employees at 50%, privileged information technology (IT) users and admins at 47%, and contractors, service providers, and temporary workers accounting for 47% (2017b).

There are some misconceptions concerning malicious and unintentional insiders. A recent Cyberark report states that a significant amount of companies realizes the "threat from within" but still focus their attention primarily on malicious insiders. The problem is the news highlights high-profile data breaches such as the massive data breach perpetrated by former U.S. National Security Agency (NSA) contractor Edward Snowden. Unintentional threats are less conspicuous, will not make headlines, and are a result of inside employees accidentally creating security weaknesses within the current security posture. While not the costliest insider threat, the unintentional insider is considered the most dangerous threat because they can damage or even cripple an organization (2016). A recent survey (as cited in Cyberark, 2016) consisting of Information Security Forum (ISF) members explains that the vast majority of insider breaches are caused by inadvertent employee behavior and not by nefarious malicious users.

Malicious users are the "insider threat" as most people would picture. They are users situated behind perimeter defenses which may intentionally steal data or attempt to harm an organization. Gelles (2016) describes motivators and indicators of malicious insiders as:

> Malicious insiders may be motivated by money, revenge, validation, or empowerment. They may possess an exaggerated sense of entitlement. Some may operate as spies for a foreign government or steal critical intellectual property (IP) for a competitive entity. Attacks by malicious insiders are seldom impulsive acts. A number of case studies have

> confirmed this by evaluating the precursors or indicators displayed by the insider before taking action (e.g., declining performance, undue access attempts, negative workplace interactions). Employees wishing to harm a current or former employer, business partner, or client – whether by stealing trade secrets, sabotaging information systems or by opening fire on colleagues – usually plan their actions.

According to Cyberark (2016), malicious insiders account for 26% of internal breaches and are the costliest. For example, disgruntled employees or those in need of financial resources usually know and have access to, sensitive information while possessing the skills to bypass organizational security strategies. Dtex Systems in their 2017 Insider Threat Intelligence report concluded that security bypass and high-risk applications, theft via personal email, leavers and joiners, inappropriate Internet use, and pirated software and media are all signs of malicious intent (2017).

In a Breach Barometer Report: Mid-Year Review conducted by Protenus, Inc. in collaboration with DataBreaches.net found the healthcare sector is on track to exceed the "One Health Data Breach Per Day" (Davis, 2017). According to Protenus (2017), the report states insiders are increasingly responsible for a large number of data breaches and surpass hacking and ransomware by 28 percent. The report also stated that while hacking has accounted for a significant portion of data breaches in the healthcare sector, insiders caused 28 percent more breach incidents than hackers. The same report stated 41 percent of health data breaches in 2017 were due to insider threats. A Protenus, Inc. report characterized insider incidents as either insider-error or insider wrong-doing. Insider-error included accidents and anything else that was without malicious intent while insider wrong-doing included theft, snooping in patient files, and

any other incident where the insider knowingly violated the law or patient privacy (Protenus, 2017).

Recent news has highlighted government malicious insider threats such as former U.S. Army Private First Class, Chelsea Manning, who was found guilty of violating the Espionage Act. Manning leaked three-quarters of a million classified and unclassified but sensitive documents to WikiLeaks. Manning is one of many insider threats who struck fear into the government resulting in an executive order establishing a National Insider Threat Task Force. The National Insider Threat Task Force required federal agencies who handle classified materials to implement programs to detect individuals suspected of leaking sensitive information. This case also resulted in the Pentagon's Defense Security Service requiring contractors to implement methods to detect, deter, and mitigate insider threats. (Davenport, 2016).

Davenport (2016) also stated the global consulting firm, Booz Allen Hamilton's contractor, Edward Snowden's disclosure of the National Security Agency (NSA) bulk data collection of Americans' phone usage had increased concern within the federal government while decreasing Booz Allen's share price. The growing concerns are related to an employee's ability to abuse their position and privileges to ex-filtrate sensitive information. More recently and after Snowden an NSA contractor and six-year Air Force veteran Ms. Reality Winner faces charges under the Espionage Act. Winner allegedly shared documents revealing Russian involvement in hacking U.S. voting systems in the weeks immediately before the 2016 presidential election (Holpuch, 2017).

Former NSA contractor Harold Thomas Martin III was indicted on 20 counts of stealing materials from the Central Intelligence Agency (CIA), NSA, U.S. Cyber Command, the Defense Department, and the National Reconnaissance Office (NRO), which is an Intelligence Agency

(IA) responsible for, among other national security activities, the development and operations of America's intelligence satellites (Goldman, 2017). According to Shane and Becker (2016), Mr. Martin managed to get and kept a top-secret security clearance despite having insider threat behavior indicators such as drinking problems, a drunken-driving arrest, two divorces, unpaid taxes, and computer harassment. Kopan, Perez, and Jarrett (2017) stated Martin's indictment alleges he removed classified documents from 1996 to 2016 indicating he managed to evade detection as an insider threat for 20 years. These cases have two things in common; they were trusted employees or contractors who had access to sensitive information and used their privileged positions and organizational trust to intentionally ex-filtrate confidential information.

The majority of unintentional insider threats are simply employees doing their jobs on a daily basis, but in some instances, their actions put the organization at risk (Cyberark, 2016). While malicious insiders are the costliest and hardest to detect, it is the unintentional insider who can cause unintentional harm to organizations. In a SANS survey presented by Cole (2017) and sponsored by Dtex, Haystax Technology, and Rapid7 describes unintentional insider involvement as a higher risk than malicious insiders by allowing infiltrators to break into a network undetected. The survey also indicates that an unintentional insider is tricked or manipulated into causing harm. For example, the insider fell victim to a sophisticated phishing attack resulting in stolen credentials allowing the infiltrator to access sensitive information in a way that would appear legitimate.

Companies and organizations need to understand that threats posed by employees, often referred to as "unintentional" manifest themselves in employee actions that may be intentional. Scott and Spaniel (2017) present employee actions as deliberately circumventing company security polices for the sake of convenience or deciding not to follow security procedures.

Employees may not intend or believe their actions will cause harm, but in some instances, it does.

According to Waters (2016), human error is the primary reason for causing a significant amount of damages to an organizations asset. The author further addresses factors which can contribute to human error resulting in an unintentional threat. Fatigue can be a contributing factor because users will be less attentive, therefore, increasing inappropriate actions concerning network security decisions. Additionally, the author adds lack of knowledge of an organization's policies and procedures resulting in unintentional negligence regarding standard security practices, therefore, leading to security breaches and possible damage to organizational assets. Waters (2016) describes acts which occur in accidental disclosure and information and unintentionally aiding an external threat through carelessness. The actions include but are not limited to falling victim to phishing attacks, online scams, and losing physical devices such as portable drives, phones, and USB sticks.

Cole (2016) describes an unintentional insider scenario involving a phishing email where the insider's email becomes the insider threat. A user received an email requesting additional information concerning their company products. The email sent by the infiltrator stated the details for the request were located in the attachment. The user opens the attachment and realizes the details are regarding the company's new gateway solution product. After copying a pre-written response into the email, the user clicks the send button and resumes his previous activity. The user did not realize his system had been compromised by opening the attachment. This act is considered unintentional because the user has unknowingly allowed an outside threat, the infiltrator, to compromise his system and possibly pivot from their machine to other systems seeking sensitive information. According to Filkins (2017), a 2017 Data Breach Investigations

Report indicates that 66% of all malware were installed by end-users clicking on malicious email attachments.

Dtex Systems defines two types of malicious and unintentional threats as malicious users and negligent users. Malicious users are those who intentionally cause harm to organizations most often by stealing sensitive information, intellectual property, and trade secrets. Negligent users are unwitting insiders who through inadvertent negligence may unknowingly cause a security breach. Infiltrators are those individuals who penetrate organizations by taking advantage of human and technological weaknesses from inside employees (2017).

As stated above, malicious insiders are those who willfully harm an organization and frequently includes motivating factors. However, negligent insiders are those unintentional insiders who cause a security risk unintentionally. Inattentive users are not considered malicious but often become security risks because they ignore policy and security protocols according to Schulze (2016). Dtex Systems explains negligence accounts for 68% of insider security incidents, but most organizations focus their efforts on preventing intentional data theft. The author emphasizes that cloud sharing, remote communication, and portable workstations further complicate the employee negligence issue because these tools make it easier for unwitting employees to expose data accidentally (2017).

Insider threats can be malicious; however, Tripwire explains all insider threats are not committed intentionally and not all incidents are malicious. For example, an unintentional insider threat may involve a negligent employee who inadvertently causes data breaches and data leaks either accidentally or through external attacker manipulation (2017). For example, Paganini (2017) explained how an accidental insider at the aerospace giant Boeing inadvertently leaked a spreadsheet containing Personally Identifiable Information (PII) of 36,000 of his co-workers.

The spreadsheet contained information such as places of birth, employee IDs, accounting department codes, hidden columns containing both social security numbers and dates of birth.

Chief Research Intelligence Analyst Stephen Gates and Senior Threat Intelligence Research Analyst Cody Mercer agree the insider threat problem is widely accepted throughout the cyber-security community and considered the most significant attack vector to any IT entity (Gates & Mercer, 2017). Furthermore, the authors report ransomware campaigns as having a considerable impact and involve innocent insiders who unintentionally fall victim to these exploits. For example, tech support scams and extortion-ware have become incredibly advanced and even more dangerous over the last few years. The 2017 Internet Security Threat Report by Symantec indicates "the number of new ransomware families uncovered during 2016 more than tripled to 101 and Symantec logged a 36% increase in ransomware infections." Furthermore, the report stated the U.S. is the most significant and softest target worldwide. In fact, 63% of Americans are willing to pay the ransom demand, which was a 266% increase, while criminals demanded an average of $1077 ransom demand per victim (Symantec, 2017a).

Dtex Systems in their 2017 Insider Threat Intelligence report concluded that security bypass and high-risk applications, theft via personal email, leavers and joiners, inappropriate Internet use, and pirated software and media are all signs of malicious intent. The report stated, security bypass is considered the first step toward data theft which included using vulnerability testing and hacking tools such as Metasploit Framework, anonymous web browsers, and anonymous VPN tools. The Global Web Index as cited in Dtex Systems (2017) estimates that 24% of Internet users are currently running anonymous VPN services. The report indicated 87% of organizations surveyed found employees using personal email services on company endpoints even though those companies had implemented measures to block those cloud-based providers.

Personal email services can be used to exfiltrate data to outside malicious actors successfully without leaving a trail.

Dtex Systems (2017) indicates 56% of organizations had potential data theft by leaving or joining employees. The Dtex Systems 2017 Insider Threat Intelligence report distinguishes the difference between leavers and joiners. Leavers tend to show unusual file aggregation in the last two weeks of employment while joiners tend to import large amounts of data in the first two weeks of work (2017). In an Intermedia Insider Risk Report surveying more than 2000 office workers based on age, role, and industry found that 97% have some form of confidential or sensitive information while 93% admitted to engaging in at least one type of inadequate data security (2015).

The Internet allows users to get things done faster, better, and without much difficulty. Dtex Systems produced a risk assessment of those users who engage in inappropriate workplace activity such as online gambling and pornography. The risk assessment characterized activities such as gambling, lottery, sports, and betting as precursors or variables associated with employees who may circumvent security protocol. Furthermore, the users typically would need to bypass some form of security measures to access such sites and do not realize they are weakening the overall security posture of the organization (2017).

Two crucial points concerning pirated software and media as stated by Dtex Systems (2017) is that 76% of the assessments found employees using illegally obtained software and media. The author further explains there are legal ramifications which organizations face when users download or install pirated software and media. According to Dtex Systems (2017), damages for each illegally obtained software or media can be as much as $150,000 per copy.

Organizations remain trusting toward their employees, as well as others who are responsible for keeping sensitive information safe. NTTSecurity (2017) found that 42% of the presumed employees believed it was their responsibility to keep this information secure. The research shows that negligence can severely impact an organization's bottom line where the average cost due to negligence approached $207,000. The same analysis also states carelessness among negligent employees and contractors account for 68% of insider threats.

Insider Threats to Organizations

"One of the most challenging problems in managing large networks is the complexity of security administration" (NIST, 2017). Organizations can be directly involved in creating an environment that facilitates insider threat activities. Organizational problems consist of users having more privileges than necessary in order to perform their job, BYOD policies, mismanaged vendors and third-party contractors, BEC, detection time, easy for insiders to cover their tracks, differentiation between legitimate work and harmful actions, difficulty of proving guilt, sophisticated social engineering, cloud-based computing, and insufficient budgets. It is essential that specific groups are more responsible for the problems than others.

According to Worrall (2014), privileged access allows employees to move freely across the network without being detected. Worrall states "the problem is not where an attack starts or if an individual works for the company - it's about an attack that's already behind the traditional security perimeter." Additionally, the author adds that privileged credentials can turn an external threat into insider threats that can move freely inside the network while evading detection. Furthermore, privileged access becomes the true threat allowing malicious users to harm an organization, or provide the means for an outside attacker to use the credentials in the same way

as an insider (2104). Carson (2017) considered privileged accounts as being the most sensitive accounts within the organization and referred to them as "the keys to the kingdom."

The reality is the most dangerous threat is one from trusted employees having privileged accounts. Gogan (2016) states that privileged accounts allow access to restricted information and full control over critical systems placing them in a position to act maliciously. Moreover, organizations tend not to spend the necessary money and hiring of specialists that allows for a proactive approach to network security. However, monitoring and controlling privileged access is a necessity and should be part of any security policy. Carson (2017) suggests that many IT users lack understanding of how privileged accounts work. The author further explains that privileged accounts are protected with a password just as user accounts are. Additionally, the problem is that there are plenty of tools to assist hackers in cracking passwords for privileged accounts. After cracking the privileged account password, the attacker can access and view an organization's most sensitive data, create backdoors, bypass existing security controls, and erase audit trails.

Padayachee (2016) concludes outsiders have limited opportunity for attack unless they can exploit vulnerabilities in the system while insiders have a more significant chance because they have privileged access. However, despite having the necessary privileged access, the insiders have policies, procedures, and agreements that they must adhere to, or choose to ignore, which may result in the user becoming an insider threat. For example, encryption can be cracked by an insider because of their privileged access

BYOD privileges are growing more popular among companies and users to increase efficiency and productivity. In a Crowd Research Partners 2016 Spotlight Report (as cited in Becker, 2016) consisting of 800 security professionals worldwide presented by LinkedIn and

sponsored by Bitglass, Blancco Technology Group, Check Point Software Technologies, Skycure, SnoopWall, Zimperium, and Tenable Security states the top reasons for enabling BYOD privileges includes improved user mobility accounting for 61%, higher employee satisfaction at 56%, increased employee productivity at 55%, and reduce costs accounting for 47%. However, the report also mentions the top obstacle for BYOD adoption was security concerns at 39%. The results of the study indicate respondents were overwhelmingly permitting BYOD in their organizations. Additionally, the survey found that BYOD was available to all employees at 40% of the companies while select employees are accounting for 32%. Moreover, the report stated some organizations were allowing BYOD for contractors at 23%, partners at 16%, customers at 16%, and suppliers accounting for 9%.

BYOD has increased security and privacy concerns because organizations are adopting such privileges. Crowd Research Partners (2016) indicated 12.1 billion mobile devices would be in use by 2018 and half of the world organizations will require BYOD by 2017. Additionally, 67% of CIOs and IT professionals remain convinced that mobility will impact their organizations as much, or more, that the Internet did the 1990s. According to Juniper (as cited in Crowd Research Partners, 2016), Wi-Fi networks will carry approximately 60% of all mobile traffic by 2019 while reaching over 115,000 Petabytes (PB). As a result, the report mentions one out of five organizations, or 21%, have experienced a security breach through the use of BYOD or corporate-owned devices. Furthermore, 39% of surveyed organizations reported that BYOD or corporate-owned devices had downloaded malware. Agudelo, Bosua, Ahmad, and Maynard (2015) argue that the technical capabilities of mobile devices, combined with employee access to online social networks, significantly increase the threat posed by insiders.

BEC schemes have caused at least $5.3 billion in total losses to approximately 24,000 organizations around the world according to the FBI (as cited in Trend Micro, 2016). FBI (2017) defines BEC as;

> Business E-mail Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The E-mail Account Compromise (EAC) component of BEC targets individuals that perform wire transfer payments.

Trend Micro (2016) argues very few BEC schemes rely on malware and most rely on highly successful social engineering techniques. For example, "The Bogus Invoice Scheme", "Supplier Swindle", or "Invoice Modification Scheme" are different versions of the same scam. The author states these attacks most often involve organizations working with a foreign supplier. For example, the customer is asked to wire funds for an invoice payment to a fraudulent account

Altman, a middle market Pennsylvania Regional Executive for Huntington Bank explains that BEC fraud has been successful and has become more pervasive (2016). The FBI reported recently (as cited in Altman, 2016) that there has been a 270% increase in victims reporting losses from BEC compromises. The FBI in a public service announcement, based on IC3 complaints, defines five different scenarios related to BEC. According to FBI (2017), the five scenario types are as follows:

- Business Working with a Foreign Supplier. The situation typically involves a company with a long-standing relationship with a supplier and is requested to wire funds for an invoice payment to an alternate and fraudulent account.
- Business Executive Receiving or Initiating a request for a Wire Transfer. Initially, the email accounts for high-level executives (Chief Financial Officer (CIO), Chief

Technology Officer (CTO), etc.) becoming compromised. "CEO Fraud", "Business Executive Scam", "Masquerading", and "Financial Industry Wire Frauds" represent other names for this attack.

- Business Contacts Receiving Fraudulent Correspondence through Compromised Email. The Scenario begins with an employee having their personal email hacked. Intermingling personal email with business communications, the attacker will request invoice payments to a fraudulent bank account sent from the employee's compromised personal email account and sent to multiple vendors found in the employee's contact list.
- Business Executive and Attorney Impersonation. Victims of this scenario report being contacted by a lawyer or a representative of a law firm and claim to handle sensitive information or time-sensitive information and may be conducted via phone or through email. This scenario typically occurs at the end of the day or work week and timed to coincide with the close of business of international financial institutions.
- Data Theft. This scam usually involves fraudulent requests sent via a business executive's compromised email account. Typical targets include departments responsible for W-2s or maintain Personally Identifiable Information (PII), such as the human resources department, bookkeeping, or auditing groups. This data theft scenario of the BEC scam began just before the 2016 tax season.

The BEC scam is growing significantly and evolving at the same time. The FBI (2017) states the scam targets small, medium, and large businesses. Furthermore, there was a 2,370% increase in identified exposed losses. Additionally, BEC has been reported in all 50 states and 131 countries.

The threats posed from third party vendors must be appreciated and understood by major companies. To better insure their own security, such companies must also examine and assess third party vendor security, in some instances, this may involve thousands of such vendors.

Due to the ever-changing informational processes of such vendors, it is a monumental task. The lack of understanding and appreciation of third party threats, Gorman asserts, results in numerous misconceptions and creation of a several myths surrounding cybersecurity threats.

Third-party contractors, vendors, and partners have the potential to become insider threats to organizations. For example, Cheng and Yao (2017) mention a third-party contractor, Fazio Mechanical Services is responsible for Target's data breach by using a phishing email attack in September 2013. Fazio had access rights to Target's network for remotely monitoring energy consumption and temperatures of the stores. Through a phishing email, the attackers gained access to Target's network and access to vulnerable machines. The attackers then compromised the Point of Sales (POS) systems and deployed data-stealing malware called BlackPOS on the POS terminals that were capable of scanning the memory of POS devices looking for sensitive information. The stolen data was then encrypted and move from POS devices to drop sites outside of Target's data network. Additionally, Cheng and Yao (2017, June 9) describe the Target Corporation breach in 2013 consisting of 40 million credit card information and 70 million customer's PII while incurring $248 million in losses. Megatrend data breaches, like Target Corporation, have prompted class action lawsuits seeking damages for those experiencing stolen personal information. According to Hewes (2016), There were 70 class action lawsuits against Target Corporation for the 110 million customer accounts that were compromised alleging that businesses fail to adequately safeguard customer information and do not give sufficient notice of the breach.

In a Crowd Research Partners Insider Threat Spotlight Report (as cited in Veriato, 2016), the groups posing the most considerable security risk to organizations are privileged IT users/admins accounting for 60%, while contractors/consultants and temporary workers at a close 57%, and regular employees accounting for 51%. Third-party technology networks can represent a significant security risk to any extensive data network. Kansteiner (2016) states that history has proven attacks on well-protected systems can be a result third-party vulnerabilities. For example, Target Corporation, Home Depot, Barclay's, sever large hotel chains, AT&T, and Goodwill were all compromised via third-party weaknesses. The author notes that one-third of all network attacks are linked to current or former third-parties including vendors, sub-contractors, service providers, and only 44% of network administrators have a formalized process for assessing the risk posed by third-party networks. For example, a large oil firm was attacked using a Chinese restaurant network as the attack vector because the attackers knew the oil firm's employees routinely visited their website to view the online menu (Kansteiner 2016).

Social engineering and phishing attacks create problems because they are highly successful and have become the best way to gain unauthorized access since perimeters are well-protected. Clark (2017) stated

> Social engineering may be defined as obtaining information or resources from victims using coercion or deceit. During a social engineering attack, attackers do not scan networks, crack passwords using brute force methods, or exploit software vulnerabilities. Rather, social engineers operate in the social world by manipulating the trust or gullibility of human beings.

In a case study, attackers used compromised Twitter accounts to send an erroneous Tweet warning of two explosions in a government building. Staff, despite being warned after previous incidents, still fell for the scam.

Detection of insider threats is difficult because it is hard to differentiate between who is doing their job and who is performing harmful actions. In a Crowd Research Partner Insider Threat Spotlight Report, 61% of the respondents have a more difficult time detecting and preventing an insider attack versus external attack (2017b). The report further explains the reason for such difficulty beginning with 66% of the respondents who believe the reason is insiders already have credentialed access to the network and services, 53% of the respondents believe that the number of increased applications such as email, DropBox, and social media can leak data, and 46% of the respondents think the increased amount of data leaving the network perimeter introduces a problem (Veriato, 2016). According to Keanini (2015), most organizations have no strategies in place to deal with insider threats. The author further explains that in a survey of 355 IT professionals found the 61% said they couldn't deter insider attacks, and 59% admitted they couldn't even detect one.

Thales 2017 Data Threat Report found that 73% of security respondents anticipate security spending increases over the next year, up from 58% in 2016. Security spending doubled from 12% to 23% last year (Thales, 2017). According to Filkins (2016), Financial Services is projected to spend 10-12% on security, while education is dropping from 4% -6% in 2015 to 1% -3% in 2016. A possible explanation for this is that education raised their IT budgets the previous year, so even though the percentage may appear lower, the amount of money being spent remains the same. Additionally, Technology/ IT services and healthcare projected numbers

remained the same from 2015 to 2016 while government industry increased from 4% - 6% in 2015 to 7% - 9% in 2016.

In a SANS whitepaper survey respondents stated, "we tackle the low-hanging fruit (patches, port restrictions, account management, etc.) first and then focus resources on the results of internal threat assessments. We pay attention to what we are trying to protect, where we are most vulnerable, and then decide what our tolerance is for compromise." The whitepaper also indicates that budget allocations concerning cybersecurity may be the effect of not tracking security spending, therefore, making it difficult to prove that cyber security spending is working. The whitepaper states, "those responsible for budgeting need the visibility, methods, and metrics to answer the critical questions of who, what, why, where, and how security spending supports the organizations business objectives in a consistent, continuous and repeatable manner (Filkins, 2016). Gartner (2017) explains that worldwide spending on cybersecurity products and services will reach $86.4 billion, an increase of 7% over 2016. Furthermore, cybersecurity spending is expected to reach $93 billion in 2018.

Organizations are moving to the cloud because of the benefits such as lower cost, faster time to market, and increased employee productivity. According to Coles (2017), IT departments are holding back cloud adoption primarily because of security concerns. The author further explains, based on a Ponemon Institute survey of 400 IT and IT security leaders, that employees are not waiting for IT. Furthermore, employees are bringing the cloud services to work as part of a movement called "bring your own cloud" or BYOC movement. The Ponemon survey indicates user-led cloud adoption must be understood and managed by organizations (Coles, 2017).

The National Institute of Standards and Technology (as cited in Singh, Jeong, and Park, 2016) defines cloud computing as, "cloud computing is a model for enabling convenient,

resource pooling, ubiquitous, on-demand access which can easily deliver with different types of service provider interaction." Souza (2016) introduced in a Cloud Security Alliance blog posted on October 27, 2016, the top threats in cloud computing by surveying over 100 respondents. The top threats are as follows:

- Employees leaking critical information and tradecraft on illicit sites
- Data type and formats being exfiltrated along with exfiltration mechanisms
- Why so many data threats go undetected
- What happens to the data after it has been exfiltrated
- Tools to disrupt and prevent the data exfiltration cycle
- Possibilities to delete traces of data once exfiltrated

Singh et al. (2016) mention security issues in the cloud environment are caused by its essential characteristics such as resource pooling, virtualization, elasticity, and some measured services. The authors also mention there was a 70% increase in Advanced Persistent Threats (APT) attacks, 68% suspicious activities, and 56% brute force attacks on cloud computing in 2015. According to Corbin (2014), the State Department Chief Information Security Officer is concerned with network operations being turned over to third-party providers possibly leaving the government IT workers without the appropriate access granted allowing them to conduct regular security audits. The author indicates the government may have to rely on the third-party who they have no control over to conduct such audits. Generally speaking, organizations remain concerned about security in the cloud and the primary reason why IT professionals are hesitant to make a move.

Insider Threat Mitigation Strategies

The National Infrastructure Advisory Council (NAIC) reports that "…preventing all insider threats is neither possible nor economically feasible…" because the threat is already behind perimeter defenses and often know exactly where the vulnerabilities exist (Cline, 2016). A 2016 Cyber Security Intelligence Report mentions that in 2015 the insider threat continues to pose the most significant threat to organizations. The same report indicated that 60% of all attacks were carried out by those who had insider access to an organization's systems (IBM, 2016). Ware (2017) explains in a Haystax survey conducted in partnership with Crowd Research Partners and including 300,000+ respondents from the Information Security Community reported the most significant barriers to better insider threat management are lack of training and expertise accounting for 60%, decrease of budget at 50%, lack of collaboration between separate departments at 48%, and 43% of the respondents say it's just not a priority.

Modern insider threat mitigation strategies include both protecting data and monitoring users. These current approaches are made up of non-technical policies, technical methods, procedures, and associated guidelines. Organizations should try to conceive a plan which attempts to understand the aspects that motivate "trusted" employees to violate this trust and should be considered by employers during the hiring process (Greitzer, Imran, Purl, Axelrad, Leong, Becker, and Sticha, 2016). The authors also express their concerns surrounding the current methodologies that focus on detection of unauthorized user access, malicious anonymized user activity, and detecting data leakage. The authors further define the use of typical approaches such as firewalls, passwords, and encryption to prevent unauthorized access, but often these tools are only valid for detecting and preventing external attacks.

There are two models available for explaining what needs to be in place before an insider thinks of taking the risk. The first model was developed initially in 1953 and revisited in 2015 by

Schuchter et al., (2016). The Association of Certified Fraud Examiners (ACFE) found that sociologists and psychologists still use the three elements of Cressey's Fraud Triangle including pressure, opportunity, and rationalization when assessing the insider threat (ACFE, n.d.).

Cline (2016) evaluated Cressey's Fraud Triangle and found that pressure, opportunity, and rationalization were the three factors necessary for an individual to consider committing fraud. Additionally, he states if any of these factors are not present, then the crime is less likely to occur. David Wolfe and Dana Hermanson modified Cressey's model and referred to it as the Fraud Diamond. They expanded Cressey's Fraud Triangle to include capability, an individual's traits and ability to commit fraud (ACFE, n.d.). Cline (2016) agrees that even though the other three factors may be present, the individual must also have the capability of intentionally committing the crime.

Each inside attacker will have their reason for conducting an insider attack. Costis (2017) focuses on the most common motivating factors seen with insider threats. The author suggests financial gain, business gain, revenge, and ideology are four of the most common motivating factors among insider threats. Furthermore, the financial benefit has traditionally proven to be the leading motivating factor regarding insider threats while ideology is the least significant motivating factor. Tripwire (2017) presents the same motivating factors such as acting on an opportunity, taking revenge for a perceived injustice, making a statement, doing competitors bidding, seeing themselves as a future competition. Additionally, Blankenship and O'Malley (2017) would suggest adding disgruntled employee, entitlement, fear of layoff, work conflicts, and outside influence as motivating factors.

Behavior indicators are essential to understanding how to recognize the signs of employees who may become, or already have become insider threats. It is vital that organizations

also understand the behavior indicators so they can be included in training to help aid the employees in recognizing the possibility of an insider threat. Blankenship et al. (2017) offer several sample indicators to watch for with insider threats. The authors explain that poor performance appraisals, voicing disagreement with policies, conflicts with co-workers, financial distress, unexplained financial gain, odd working hours, unusual overseas travels, and leaving the company as indicators to be aware of to build an effective insider threat program.

Forrester Research is one of the most influential research and advisory firms in the world and suggests that organizations must recognize two important points before trying to implement a successful insider threat program. As stated in a recent Forrester report, organizations first need to understand and accept that insiders are responsible for more than half of their data breaches. They also must realize that insider threats are not a technology problem, and if treated as such, ignores the human aspects such as motivation and behavior (Blankenship et al., 2017). Waters (2016) suggests organizations should also recognize the fact that there is no "one size fits all" stance to adequate policies and procedures while Dtex Systems (2017) suggests there is no single bulletproof solution to preventing insider threats.

According to Tripwire (2017), businesses should include the insider types in a formal insider threat program. Privileged users are those who are trusted most and usually have higher privileges than regular users. Higher privileges mean more opportunity to misuse data regardless if intentionally or unintentionally. Third-parties would include remote users, subcontractors, third-party vendors, and partners. Terminated employees are those who either take data with them when they leave or may be able to access information after termination using malware, backdoors, or because no one thought to disable their access.

According to Lord (2017b), the best method to control who has access to what is to apply the principle of least privilege at each level of a system. The author suggests including end users, systems, processes, networks, databases, applications, and just about any other facet in an IT environment. Furthermore, the benefits are better security, minimizing the attack surface, limiting malware propagation, better stability and reduced scope of an audit. The Common Sense Guide to Mitigating Insider Threats, Fifth Edition, states that all organizations should legally and contractually require accountability and full disclosure for all third-party vendors, partners, subcontractors, etc. The third-party vendors should be responsible for backup services including any offsite backups. Those third-parties should include encryption into their backup solution for greater protection. The Common Sense Guide to Mitigating Insider Threats, Fifth Edition, suggest that each department within organizations should have a termination checklist. A checklist for the IT department would include removing all user access (CERT, 2016).

Waters (2016) argues technology alone cannot completely mitigate the insider threat and must be attacked from a holistic point-of-view that incorporates both technical and non-technical behaviors. To create a successful insider threat program, organizations must think holistically and not depend entirely on technology as a solution. However, technology does have a role to play and should be combined with other non-technical solutions. Forcepoint feels the essential ingredients to a successful insider threat program includes policies, processes, technology controls, risk management, and auditing and monitoring. For accountability purposes, policies should establish rules for BYOD, social media, Web surfing, and transferring data to a personal device. The procedures should be given to each employee and signed so they can be held accountable for their actions. Processes involve training that covers insider threat best practices and should be part of every new hire's orientation and reinforced often. Technology controls

enforce access to systems based on assigned roles, and project-based access is cut off once the project is complete. Risk management defines the organization's mission-critical data and critical assets. Consider all things that are necessary for conducting business and develop a risk management plan for each. The before mentioned items are preventative measures while auditing and monitoring log files provide evidence of events which have already occurred while supporting a comprehensive insider threat program (2017).

Forcepoint believes that building an insider threat program that gives complete user visibility and behavior context involves five "pillars." The first pillar is user activity monitoring and provides a solution that will establish a baseline that is typical of a user's activities. The reality is that most users spend most of their time doing routine tasks. For example, logging on to a known device, checking emails, opening up files, and surfing the Web may be normal indicators of user's routine tasks. The second pillar is indicators of risk which will distinguish between what is normal routines and not-so-routine user actions and is accomplished through a behavior audit and will determine harmful effects such as loss or destruction of proprietary data, exposure of personally identifiable information (PII), and theft of sensitive data through unauthorized access. Pillar three is risk scoring and requires machine-based analytics to process large amounts of data coming in while making the most of behavior audits by already including risk indicators. Machine-based analytics will remove the analyst bias while automatically producing a score for a user's behavior. Derived scores from an algorithm treat users equally by using weights based on least essential and most significant behaviors. To reduce risk surrounding user behavior over time risk scores just aren't enough. The solution to minimize risk begins at pillar four by addressing forensic context that allows an organization to go beyond risk scores and produce forensic data which provides an accurate view that connects all the dots. Pillar five

consists of remediation and mitigation and dependent on all other pillars. Organizations can take action once unusual activities have been flagged. Behavior audits performed by machine-based analytics distinguish between normal and abnormal behavior and then suggest what forensic context is needed. Once the organization has the forensic information, it can then take action (2017).

CERT's Common Sense Guide to Mitigating Insider Threats, Fifth Edition has emerged as an industry standard for insider threat program implementation according to Forcepoint (2017). CERT produced an Insider Threat Best Practices for organizations to implement to mitigate IT theft, IT sabotage, and fraud. The best practices were based on the idea that insider threats are influenced by technical, behavioral, and organizational issues. Insider threats are best addressed using policies, procedures, and technologies which would also include an organization's employees. For example, agencies should implement strict password and account management policies and practices, enforce separation of duties and least privilege, define security agreements for cloud-based services, and institutionalize change control (2017b).

Another source for building an insider threat program came out of the massive release of classified information through WikiLeaks. Through an executive order, the National Insider Threat Task Force was established with the mission to develop a government-wide insider threat program that can prevent, deter, detect, and mitigate compromise to classified information. Senior leaders found that there was no "easy button" for solving the insider threat issue but the National Institute of Standards and Technology (NIST) provided a solution, the Cybersecurity Framework (CSF). CSF can be used as a baseline for an insider threat program and provide the end-to-end capability. Stakeholders can develop a strategy that will safeguard the safety and reputation of organizations. Organizations using the CSF tool will discover sensitive data

regardless where it resides, identify endpoints at risk, flag abnormal behavior, and do so in an unobtrusive manner (Symantec, 2017).

Government agencies seem to get most of the spotlight when it comes to data breaches. This is likely due to the type of data which is stolen which usually includes PII such as names, addresses, birthdates, and social security numbers. There is a technology which can help in preventing government breaches regardless if it's an external attack, malicious insider, or unintentional insider. One such example is Data Loss Prevention (DLP). DLP is a strategy that protects sensitive data from theft, loss or misuse (Lord, 2017a). Furthermore, DLP effectively classifies confidential information to prevent the information from being accidentally or maliciously shared and a good option for monitoring and controlling endpoint activities.

Cybersecurity budgets for many organizations focus on perimeter defenses. As the perimeter gets stronger, the adversary will concentrate on unintentional insiders as the entry point of choice. Cole (2017) states in the September 2016 SANS Threat Landscape Survey showed that 80% of respondents experienced a phishing attack; that 75% of identified impactful threats entered by email; and that 46% of attacks were launched by users clicking web links in an email. Phishing is a form of social engineering that takes advantage of a human weakness. According to (Lord, 2017c; Filkins, 2017), phishing attacks through email are the most common security challenges and continues to be a significant source of compromise. Phishing attacks are attempts to get sensitive information such as passwords, credit cards, etc. by using email, social media, phone calls and any other form of communication. There are, however, a few ways to mitigate the threat that plagues unwitting insiders. The author suggests training session with mock phishing scenarios, SPAM filters, antivirus, keep systems up-to-date, password expiration

policy, block malicious sites using a web filter, encrypt sensitive information, convert HTML emails to text only, and secure remote users with encryption (Lord, 2017c).

Insider threats to cloud security can be unintentional or intentional. Since insider threats are those who sit on the inside, then it is someone who likely works for the cloud services provider. Souza (2016) has indicated that data exfiltration seems to be the dominant concern for organizations. Google Cloud Platform (2017) outlines several methods to reduce, deter, or possibly eliminate some cloud computing security concerns. The author defines six different categories of data exfiltration and possible mitigation strategies.

Outbound mail. Organizations should monitor volumes of data their user sends, source email addresses, recipient email addresses and what devices emails are sent from.

Downloads from insecure devices. This category should prohibit downloads of sensitive information, use Cloud Access Security Broker (CASB) which will allow only authorized devices, wrap files in Digital Rights Management (DRM) to apply permissions and enforce encryption, and consider using dynamic watermarking which can be used to track users who take screenshots or photographs of computer displays.

Uploads to external services category. Organizations should prevent data from being downloaded by keeping it in the cloud and all computation in the cloud. Prevent the installation of third-party applications such as social media or unauthorized browser plug-ins. Regulate traffic and enforce encryption using CASB.

Insecure cloud behavior. Virtual machines (VM) in the cloud can be mitigated by prohibiting outgoing connections to unknown Internet Protocol (IP) addresses, avoid assigning public IP addresses, disable remote management, limit direct SSH access to the VMs, monitor and limit the amount of data that can be read from cloud storage, and perform regular audits.

Rogue administrator. Enable logging, make all administrator access temporary, and require multiple employees to approve administrative actions.

Employee termination. Consider connecting logging and monitoring systems to Human Resources (HR) software that records an upcoming termination and adjusts the alerting thresholds appropriately.

Eliminating all insider threats is unrealistic, but a good start is to recognize some of the patterns and trends seen in many insider attacks. One such mitigation strategy mentioned in the Common Sense Guide to Mitigating Insider threats, Fifth Edition, involves the appropriate combination of policies, procedures, and technical controls in an attempt reduce or control the damage caused by insider threats as early as possible (CERT, 2016).

Discussion of the Findings

The purpose of this research was to examine the prevalence of insider threats, their types and subtypes, the risks they present to organizations, and what can be done to prevent or reduce their impact. This study will answer three questions: What are insider threats to cybersecurity? What threats do insiders present to organizations? What mitigation strategies and options have been implemented or suggested to address the insider threat problem?

The problem statement was applicable because the insider threat is growing at a phenomenal rate and needs to be understood and recognized by organizations so they might prevent or reduce the impact associated with insider threats. Not only is it growing rapidly it is getting broader and has taken on new meaning. According to Costa (2017), CERT at Carnegie Mellon's SEI updated their definition by combining the definition of a malicious insider threat and unintentional insider threat. The author describes the new definition as: "Insider Threat - the potential for an individual who has or had authorized access to an organization's assets to use

their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization." This makes the definition workable again by removing obsolete and separate definitions. The working definition was needed for some readers to help clarify the meaning, to avoid misunderstandings, and by indicating what the author thinks the meaning should be. The current definition for an insider threat is provided by the CERT at Carnegie Mellon's SEI because they have been conducting research and development specifically on this issue since 2000 by examining real-world insider threats and are considered the industry standard for implementation of an insider threat program.

We have seen in the recent past the impact insiders can have on organizations such as Edward Snowden, Reality Winner, and Harold Thomas Martin III. These are malicious insiders with privileged access who likely already have access to the sensitive or classified information they are seeking. They also are behind perimeter defenses equipped with various tools to exfiltrate data such as mobile devices, personal email, and portable storage devices. Fortunately, there are mitigation strategies which can help by preventing or reducing the impact that insider threats can have on organizations.

When we think of insider threats our thoughts almost automatically assume a malicious insider who is committing nefarious acts with the intent to do physical or reputational harm to their organization. We automatically assume a malicious insider threat because this is what we typically see in the news headlines and highlights such as the breaches perpetuated by the three names mentioned above. The malicious insider will typically have motivating factors, they are the costliest to remediate, and almost never act on impulse. Rather, they choose to take months or even years to meticulously plan their attacks (Sagan, 2017). This approach may not be noticed by mitigation strategies such as behavior analytics because it focuses on learning routine tasks of

regular employees. The profiles developed by behavior analytics may see the privileged insider as normal because they may already exfiltrate out large amounts of data and have sufficient privileges to access sensitive areas of the network. Gelles (2016) explains malicious insiders have motivating factors accompanied with behavioral indicators. The author explains that malicious insiders are motivated by money, revenge, and ideology, with financial gain at the top of the list. Furthermore, malicious actors typically will have precursors and indicators such as a decline in their performance, conflicts with co-workers, and unsuccessful access attempts. A meticulous and malicious insider likely have the knowledge and skills to evade detection.

Even though we see malicious insider threats in the news, for example, leaking sensitive information concerning government agencies they are not the real threat to organizations. The real problem is unintentional insiders and negligent employees who often expose a company to outside attacks but do so without malice. Their accidental actions can result in unintentional security weaknesses leading to an accidentally leak of sensitive information without knowledge of doing so. Most of these are not seen in the news, they are not reported or underreported, and are considered a more significant threat than malicious insiders (Waters, 2016)

Research indicates that malicious insiders have motivating factors and behavior indicators that suggest nefarious intent. According to Waters (2016) The unintentional insider has contributing factors such as fatigue which results in inattentive employees and inappropriate actions concerning security practices. Organizations can have a significant role to play in contributing factors for several reasons such as little or no training, working long shifts, and not covering appropriate policies associated with network and systems during the hiring process. Orientations should cover corporate policies, procedures, standard security practices, and all necessary training. They need to be informed and know what is expected of them and will be

held accountable for their actions resulting in disciplinary actions. For example, Haber (2017) reported in a Dell survey that 65% of employees consider it their responsibility to protect confidential information, while only 36% believe they are confident in how to protect such information. All employees should consider it their responsibility to protect sensitive data and it should be the company's responsibility to train them on how to do so.

To be clear, Tripwire (2017) explains that all insider threats are not committed intentionally and not all incidents are malicious. In fact, it is the unintentional negligent employee who unintentionally discloses sensitive information or by aiding an external threat by falling victim to phishing attacks, online scams, ransomware, or losing physical devices such as portable drives, phones, and USB sticks (Waters, 2016). Negligent users are not malicious but often cause security issues by ignoring policy and security protocols. They do so most often because they believe that security is slowing them down and decreases their productivity. Negligent users like to find easy ways to get their work completed so they do have good intentions but they do not think about and unaware of the security threats they create and responsible for. Negligent employees make up a significant number of unintentional threats. Dtex Systems (2017) explains that negligence accounts for 68% of the problem but organizations still insist on focusing attention on detecting and preventing external threats and malicious intentional data theft.

The research uncovered something that was interesting. There is a category of insider threats that I do not agree with as it was explained. The category of infiltrators are individuals who are not on the inside of the network but Dtex Systems (2017) classifies them to be insider threats because they exploit employee weaknesses by using social engineering and other malware. They may use social engineering over the phone, a phishing email, or track Internet

sites visited by the user so they can infect the website. When the employee revisits the site, it will download malicious code to their system and creating a security vulnerability allowing the external threat to gain access to critical resources. The justification for this classification is that they take advantage of innocent insiders who unknowingly contribute to security vulnerabilities by becoming a victim of social engineering, ransomware, or other malware threats. In my opinion infiltrators should not be considered an insider threat because they are outside external threats.

Organizations are not doing a good job at combating the insider threat issue. This is primarily because companies are only beginning to consider the possibility their trusted employee can cause intentional or unintentional harm. However, organizations are beginning to realize the real threat resides behind the perimeter and not hackers sitting outside the network which is protected by robust perimeter defenses. Despite the recognition, companies continue to focus their resources on protecting against external attacks. If they do focus effort protecting inside threats it is primarily the malicious insider who receives the attention and not the unintentional insiders who are the greater risk. For example, a recent survey (as cited in Cyberark, 2016) consisting of Information Security Forum (ISF) members explains that the vast majority of insider breaches are caused by inadvertent employee behavior and not by nefarious malicious users. Looking back at what was mentioned regarding training; if organizations continually experience multiple data breaches, data leakage, or theft of stolen information through social engineering and phishing attacks then it's time to consider providing cybersecurity training.

Training should be an integral piece to an overall insider threat program while considering both malicious and unintentional threats. According to Ware (2017), the three top

barriers for businesses are lack of training and expertise (60 percent), insufficient budgets (50 percent), and lack of collaboration between departments (48 percent). The numbers indicate more than half of employees have no training or inadequate training at best. Training and awareness are the best ways to combat insider threats. Technologies to combat insider threats are still maturing but are essential piece to an overall solution. Organizations who feel that installing technology-based solutions alone will resolve their issues are nothing short of naive. Waters (2016) would argue that technology alone cannot completely mitigate the insider threat and must be attacked from a holistic point-of-view incorporating both technical and non-technical solutions. Examples would be behavior analytics tied to HR systems. Training that includes insider threat awareness, explaining motivating factors and behavior indicators of malicious insiders, defining contributing factors for the unintentional or negligent insiders, and address how to report suspicious activity. Training and incidents are related, if an organization introduces training and implements an insider threat program, in time, there should be a decrease in the number of cybersecurity incidents.

Another issue concerning third-parties and companies connecting vendors, partners, and outside contractors and subcontractors to their internal business systems. Referred to as digital ecosystems, they can contribute to malicious and unintentional insider threats. Third-parties are connected directly to internal systems so it is as if they are sitting in the same building. The average fortune 500 company works with 20,000 different vendors, of which most have access to critical data and systems (Gorman, 2016). That is a significant number of vendors who may have access to the same data as regular employees. Access to the same data and the inability to monitor vendors, partners, subcontractors and contractors successfully can introduce cybersecurity issues. An organization who has connected various third-parties to many different

companies will now be forced to understand each and every businesses security posture and cybersecurity practices. Even if your perimeter defenses are incapable of being breached the hackers will simply look for other avenues of attack such as unwitting insider using social engineering. Third-parties are great attack vectors for companies who spend a lot of money to protect from external threats. Another interesting fact about third-parties, according to Gorman (2016), comes from a Deloitte survey of 170 large organizations. The survey found that 28% of the respondents were faced with significant business disruption while more than a quarter of the agencies suffered reputational damage due to third-parties. Furthermore, an unbelievable 87% of the organizations surveyed admitted to "disruptive incidents" with third-parties within the last two years. Moreover, third-parties have become one of the hardest-to-manage cyber risks for organizations across all industries.

Third-party employees can become insider threats just like employees who work for the company. It is likely they have some level of access in order to perform their jobs resulting in them becomes targets and potential malicious or unintentional insider threats. Much of this is because most organization either do not manage, or mismanage third-parties. Businesses need to hold third-parties responsible for adhering to security best practices as defined by the business. An example that many have heard about was the Target Corporation breach. Cheng and Yao (2017, June 9) states the incident was caused by a third-party contractor. Fazio Mechanical Services attack came in the form of a phishing email attack in September 2013. Fazio had access rights to Target's network for remotely monitoring energy consumption and temperatures of the stores. Through a phishing email, the attackers gained access to Target's network and access to vulnerable machines. The attackers then compromised the Point of Sales (POS) systems and deployed data-stealing malware called BlackPOS. BlackPOS was used on POS terminals and

capable of scanning the memory of POS devices searching for sensitive information. The stolen data was encrypted and moved from POS devices inside Target's network to drop sites outside of Target's data network. Moreover, the authors noted the Target Corporation breach happened in 2013 and resulted in the theft of 40 million credit cards and 70 million customer's PII, resulting in civil lawsuits and costing Target Corporation $248 million in losses to date.

Organizations are focused primarily on the mitigation of external cyber attacks leaving them vulnerable to attack on internal networks. Privileged users, BYOD, third-parties, BEC, the time it takes to detect a threat, easy to cover their tracks, difficult to distinguish between regular work from harmful actions, not enough proof for conviction, social engineering, inadequate or no budget for cybersecurity, security issues surrounding cloud computing, and even the new BYOC movement are issues faced by all organizations .

Companies who feel their employees would not become insider threats will still need to monitor them in order to comply with corporate security policies and securit audits. They could have serveral threats happenng at any given time especially when the attack has orginated form outside the network using malware or social engineering attacks. The same is true for deciding how much money to spend on cybersecurity. If you do not implement security then you have no way to have visibility into the network. With no visibility the organization will not know there is a issue until it too late. Without evidence of an insider attack you have no argument for why you need to monitor your own users.

Many organizations are in denial about insider threats, otherwise, more companies would be focused on security from the inside network to the outside network. A 2018 Crowd Research Partners report surveyed 472 cybersecurity professionals and found 53% of businesses confirmed they had experienced an insider threat in the past 12 months. The survey also points out that 27%

of the surveyed cybersecurity professionals feel insider threats have become more frequent (Crowd Research Partners, 2017a). Additionally, the study discussed the risk factors of these attacks and concluded 37% were due to excessive access privileges, 36% due to the increasing number of devices having access to sensitive information, and 35% caused by the rising complexity of IT.

Privileged access is necessary to perform many job-related duties. However, the problem is that companies seem to be giving select employees too much unnecessary access. The risk should be apparent, that privileged access can turn an external attack into an insider threat who can move through the network while evading detection. Carson (2017) considered privileged accounts as being the most sensitive accounts within the organization and referred to them as "the keys to the kingdom."

Privileged accounts can be used for malicious or unintentional purposes and compromised through social engineering attacks. IT administrators who are responsible for maintaining networks and systems can accidentally introduce misconfigurations within the network or networked systems providing opportunity for external attackers to gain access. More than any, privileged accounts need to be monitored closely and controlled. By following best practices malicious or unintentional privileged access can avoid or at least reduce the impact of an attack (Carson, 2017).

BYOD is becoming more accepted but some IT departments are not ready for BYOD, therefore, slowing its adoption while inpatient end-users are becoming frustrated. BYOD can be beneficial for organizations specifically for efficiency, productivity, and financial benefits. A recent Crowd Research Partners survey found that BYOD privileges were being overwhelmingly accepted at 40% of the companies surveyed. The survey also revealed that select employees at

32% of the companies were given BYOD privileges. The same survey predicts there will be 12.1 billion mobile devices in 2018 and approximately half the organizations around the world will need BYOD by 2017. The study mentioned that one out of five, or 21%, of companies have experienced a data breach because of BYOD and corporate owned devices. Related to BYOD, BYOC is considered a movement that consists of employees bringing the cloud to work. This is direct result of IT within organizations hesitating to adopt BYOD primarily for security reasons. Companies will be forced to allow BYOD privileges while struggling to find ways to manage BYOC endpoints (Crowd Research Partners, 2016).

BEC has five different scenarios by which BEC is conducted. The business working with a foreign supplier, business executive initiating or requesting a wire transfer, business contacts receiving fraudulent correspondence from compromised email accounts, business exective or attorney inpersonation, and data theft are all ways being used to conduct BEC. FBI (2017) states that BEC is growing significantly and at a fast pace. The author further indicates that BEC has caused a 2,370% increase in identified exposed losses while being seen in all 50 states and 131 countries world-wide. Furthermore, the FBI reported recently that there has been a 270% increase in victims reporting losses from BEC. BEC is usually associated with some form of social engineering because users are the weakest link. Some BEC scams may rely on malware for exploitation but this is rare.

Insufficient budgets are largely responsible for insider threats. The problems aren't that organizations are not allocating budgetary funds to IT. The problem seems to be about deciding where to spend the money. The statistics indicate that cybersecurity spending will continue to rise. A Vormetric Insider Threat Report stated in 2014 cybersecurity budgets increased by 10 % and believed there would be another double-digit increase for 2015. The budgetary amounts

related to IT ranged from 500,000 thousand to 1 million for 2014, 2015, 2016. The amount allocated to remediate breaches and protect a company's reputation should be considered carefully. The report stated that only 4%-6 % of the overall IT budget was allocated to security for 2014 and 2015. However, for 2016 the overall budget amount remained the same but there was a slight increase of 7%-9% allocated for security (Vormetrc, 2016). While the increased budget amounts allocated to security are small, it is promising because an increase of any kind indicates that companies are beginning to recognize the importance of cybersecurity.

Cloud computing can be beneficial for both employer and employee making them more productive, efficient, and reduced costs. A survey of 400 IT and IT security leaders (as cited in Coles, 2017), are holding back on cloud adoption primarily for security concerns. Singh et al. (2016), mentions security threats within the cloud are inherent in its design. Resource pooling, virtualization, and elasticity are all avenues for compromise. The authors further explain there was a 70% increase of Advanced Persistent Threat attacks, 68% reported as suspicious activities, and 56% reported brute force attacks within the cloud environment in 2015. There is also the concern that malicious and unintentional insiders who work for the cloud provider may either maliciously commit an attack or an inexperienced insider may accidently misconfigure a system leaving a company's data exposed because of the unintentional vulnerability introduced into the environment. Souza (2016) shares a few additional concerns surrounding cloud computing. The author explains that leaking of critical information and tradecraft, data exfiltration mechanisms, unable to detect compromised systems, how data is used once exfiltrated, and deleting traces of data once exfiltrated remain the top concerns.

It is impossible to find every vulnerability and prevent all threats behind perimeter defenses. Cline (2016; IBM, 2016) states that preventing all insider threats are not possible nor

economically feasible. The author explains in a 2016 Cyber Security Intelligence report that the insider threat continues to be the most significant threat to businesses. Furthermore, the same report indicated that 60% of all attacks were carried out by those who had insider access to an organization's systems which could be malicious or unintentional insiders, negligent employees, or third-party contractors.

Companies can implement formal insider threat programs to mitigate the insider threat to the business. However, in a joint survey conducted by Haystax and Crowd Research Partners reported the most significant barriers preventing the implementation of an insider threat program were lack of training and experience accounting for 60%, insufficient budgets at 50%, collaborations between departments at 48%, while an amazing 43% said it just isn't a priority. That is almost half of the respondents of the survey who claim an insider threat program as not a priority.

The CERT at Carnegie Mellon SEI is a great place to start if interested in developing an insider threat program. They have been studying extensively insider threats since 2000. Training is essential because your employees are often your best weapons when combating insider threats. They are the troops on the ground on the front-line. They need to be trained and trained often so they can develop the skills to help understand what motivated the insider, and if motivated, be able to recognize the behavior indicators.

Companies may not realize that insider threats are not technology problems. In fact, Blankenship et al. (2017) agrees that the threat is not a technology problem and if treated as a technology problem the human aspects such as motivation and behavior indicators will be ignored. It takes both technical and non-technical approaches to completely address the issue. It is also important to understand that organizations are not identical and there is not "one size fits

all" approach. Each program should be customized to meet the needs of the intended organization based on their vision.

There are some strategies which can be used to possibly prevent or deter and insider attack. Privileged access needs to be limited to just the function that needs it and then go back to regular privileges. Privileged use and third-parties needs to be monitor and controlled on a regular schedule. Third-parties should have a mandatory full disclosure including accountability. Each department should have a set of guidelines, a termination checklist, for what needs to be done when an employee is terminated. This would include removing all user access including remote access. Forcepoint (2017) mentions the essential ingredients to a successful insider threat program includes a combination of policies, processes, technology controls, risk management, and auditing and monitoring. Additionally, an insider threat program should include separation of duties and the principle of least privilege, create security agreements for cloud-based providers, an implement change control.

Building a program thinking it will stop all possibilities of an insider threat is unrealistic. Companies will need to determine what are critical assets and how can they be prioritized and protected. Social engineering will always be a problem because humans are the greatest threat to any organization. Mock social engineering and phishing scenarios will educate user on how to recognize these threats. Google Cloud Platform has several suggestions about mitigating threats in the cloud but they seem to be very technical and IT administrators might have a hard time implementing those suggestion, or worse, misconfigure and create a vulnerability. CERT at Carnegie Mellon SEI suggest a combination of policies, procedures, and technical controls can reduce insider threats.

Future Research and Recommendations

While researching insider threats I found the statistics and impact of insider threats staggering. The number of threats grow each year, and most companies would agree, they are becoming more frequent. The impacts to businesses who experience an insider attack are far more damaging than external attacks. The cost of remediation could possibly have been put into an insider threat program and prevented the attack. From a business perspective, ransomware victims usually pay the ransom because the information stored is vital and irreplaceable. Ransomware has been highlighted in the news recently but insider threats are more common. The insider threat is far more reaching than sabotage or fraud. It can have a negative impact such as reputational damage and loss of clients. I think to get the attention of businesses we need to see more high-profile breaches such as the one with Ms. Reality Winner and another involving Edward Snowden. These cases likely inspired organizations to at least think about insider threats and the impacts they have.

One of the most powerful tools to prevent or reduce the impact of insider threats is an organization's employees. Every business can implement a comprehensive cybersecurity policy and provide in-depth training to each employee every year or earlier if needed. The first step to formulate an insider threat strategy includes technical and nontechnical approaches to mitigate insider threats. Technology can help solve the issue by controlling access to sensitive data. According to CERT (2016), businesses should know and protect their critical assets then begin to put together a formal insider threat program. HR should cover organizational polices and have employees sign showing they understand. HR can start looking during the hiring process and determine if there are any behavior indicators or contributing factors which may turn a good employee into a malicious one. Make sure to include insiders and third-parties in risk

assessments. Monitor users for inappropriate actions such as social media, browsing pornography, or researching exploit tools. Security policies should include strict password practices and include stringent access controls and monitoring for privileged accounts. Behavior analytics is a form of technology that can be implemented to flag users when they are out of their routine threshold. DLP is a technology-based strategy for controlling leakage of sensitive information and could help monitor when this information leaves the network. Behavior analytics will create a baseline for all users and flag the user if they deviate too far outside their regular routine. Control processes by enforcing separation of duties and implement the principle of least privilege that will only give users the access they need to complete their job. Consider security agreements for cloud providers that implicitly covers access restriction and monitoring. Policies should include system change controls and backup, recovery, and remediation processes. Enforce physical security around critical assets and areas having access to sensitive information. Each department should have a termination checklist so nothing is missed when the employee leaves such as have remote access to the network and leaving user accounts active. This strategy will cover many scenarios but the insider threat program, policies, and technology-based solutions should be flexible enough to accept modifications in weak areas.

Future research should address how to balance insider threats and external attacks from a budgetary standpoint. It should focus on what is needed to prove to management that security budgets need to support mitigation of insider threats. Other than historical research many companies do not have technology, security practices, monitoring capabilities in place that can provide evidence needed to get management's attention. It needs to be addressed in a way that management understands. That is, having monetary value placed on the cost of reputational damage, loss of clients, and the cost to remediate and insider incident. Another area of research

would be to find a way to have organizations report when they have had a breach. At this time, the number of insider threats are largely unknown due to many incidents not being reported. The threat intelligence that can be taken from unreported threats could be vital to our knowledge and essential to other organizations.

New Research Question 1

How can data exfiltration be controlled when insiders use encryption?

CERT at Carnegie Mellon SEI would be a great place to begin researching how traffic inspections could be utilized to detect data exfiltration by insiders and insiders who have been compromised by external threats.

New Research Question 2

How would an increase in insider threat training reduce cyber risk?

You could start by researching general articles initially and then move toward scholarly articles, reports conducted by well-known cybersecurity companies, or surveys by the same groups such as Crowd Research Partners, Forcepoint Powered by Raytheon, and Dtex Systems. A simple Google search for "insider threat training reduces risk" produced an article from Harvard Business Review titled *More Training Won't Reduce Your Cyber Risk.* You could choose to prove this or debunk it.

New Research Question 3

How effective are current technology-based solutions for detecting insider threats?

There are a few companies who focus on technology-based solutions to solve insider threat problems and claim to be effective, in some cases 80% effective. For example, Forcepoint Powered by Raytheon, Varonis, and Observeit offer technology-based solutions to insider threats. Another good place to look would be reports generated by industry leaders such as

Verizon's Data Breach Investigations Report 2016 and Ponemon Institute's 2017 Cost of Data Breach Survey: Global Overview.

References

ACFE. (n.d.). Fighting fraud in the government. Retrieved from https://www.acfe.com/uploadedFiles/Shared_Content/Products/Self-Study_CPE/Fighting Fraud_Chapter.pdf

Altman, J. (2016, August). Business email compromise know the signs of bec or risk losing money that can never be recovered.

AT&T. (2016). Insider threats. Retrieved from https://www.business.att.com/cybersecurity/archives/v1/insider-threats.html

Agudelo, C. A., Bosua, R., Ahmad, A., & Maynard, S. B. (2015). Understanding knowledge leakage & byod (bring your own device): A Mobile Worker Perspective. Retrieved from https://arxiv.org/pdf/1606.01450.pdf

Bekker, S. (2016, March 30). Study: byod usage widespread but security is a question mark. Retrieved from https://rcpmag.com/Blogs/Scott-Bekker/2016/03/Security-a-Question-in-BYOD.aspx

Blankenship, J., & O'Malley, C. (2017). Best practices: mitigating insider threats. Retrieved from https://pages.observeit.com/rs/248-SYG-803/images/Forrester_Report_Best_Practices_Mitigating_Insider_Threats.pdf

Carson, J. (2017, August). The evolution of the digital insider trader.

CERT. (2016). Common sense guide to mitigating insider threats, fifth edition. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

CERT. (2017a). Insider threat research. Retrieved from https://www.cert.org/insider-threat/research/index.cfm

CERT. (2017b). Insider threat best practices. Retrieved from https://www.cert.org/insider-threat/best-practices/

Cheng, L., & Yao, D. (2017, June 9). Enterprise data breach: causes, challenges, prevention, and future directions.

Clark, J. W. (2017). Trends in social engineering: securing the weakest link. Retrieved from https://www.nsi.org/Impact17Presentations/J.Clark.pdf

Cline, H. G. (2016). Understanding the insider threat. Available from Dissertations & Theses Europe Full Text: Business.

Cole, E. (2016, October). Taking action against the insider threat. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/action-insider-threat-37322

Cole, E. (2017, August). Defending against the wrong enemy: 2017 SANS Insider Threat Survey. Retrieved from https://www.sans.org/reading-room/whitepapers/awareness/defending-wrong-enemy-2017-insider-threat-survey-37890

Coles, C. (2017b, December 01). 9 cloud security risks every company faces. Retrieved from https://www.skyhighnetworks.com/cloud-security-blog/9-cloud-computing-security-risks-every-company-faces/

Corbin, K. (2014, September 25). Virtualization, cloud complicate insider threats for federal cios. Retrieved from https://www.cio.com/article/2687816/government-use-of-it/virtualization-cloud-complicate-insider-threats-for-federal-cios.html

Costa, D. (2017, March 07). CERT definition of 'insider threat' - updated. Retrieved from https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html

Crowd Research Partners. (2016). Byod & mobile security. Retrieved from http://crowdresearchpartners.com/wp-content/uploads/2017/07/BYOD-and-Mobile-Security-Report-2016.pdf

Crowd Research Partners. (2017a). Insider threat 2018 report. Retrieved from http://crowdresearchpartners.com/portfolio/insider-threat-report/

Crowd Research Partners. (2017b). Threat monitoring, detection and response report. Retrieved from http://crowdresearchpartners.com/portfolio/threat-monitoring-detection-response-report/

Cyberark. (2016). The dangers within: unmasking insider threats. Retrieved from http://lp.cyberark.com/rs/316-CZP-275/images/ebook-The Danger Within-Unmasking Insider Threats-9.28.2016.pdf?mkt_tok=eyJpIjoiTVRJME1UVTJObU5pWkRJMSIsInQiOiJLalU3VUI3V3M3WUlBakFmTUpnZzZscjVXNU8yOUFmNTNUYjVPeTJCNUVDTkcyYklQMVwvb3lSNEs4ZXlOSW

Davenport, C. (2016, October 6). NSA case highlights growing concerns over insider threats; Officials say they can be every bit as dangerous as the outside hack. Retrieved from https://www.washingtonpost.com/business/economy/nsa-case-highlights-growing-concerns-over-insider-threats/2016/10/06/61b90a5e-8bc7-11e6-bf8a-3d26847eeed4_story.html?utm_term=.00f00fd4336a

Davis, J. (2017, October 26). Insiders, hackers causing bulk of 2017 healthcare data breaches. Retrieved from http://www.healthcareitnews.com/news/insiders-hackers-causing-bulk-2017-healthcare-data-breaches

Dtex Systems. (2017). 2017 insider threat intelligence report. Retrieved from https://dtexsystems.com/2017-insider-threat-intelligence-report-ad/?utm_source=google&utm_medium=cpc&utm_campaign=na_search_brand&utm_ad_group=dtex_systems&utm_keyword=dtex systems&gclid=EAIaIQobChMIutyM0oK91wIVRSWBCh2RVgpQEAAYASAAEgI9GfD_BwE

FBI. (2017, May 4). Business e-mail compromise e-mail account compromise the 5 billion dollar scam. Retrieved from https://www.ic3.gov/media/2017/170504.aspx

Filkins, B. (2016, February). It security spending trends. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

Filkins, B. (2017, September). Sensitive data at risk: the SANSs 2017 data protection survey. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/sensitive-data-risk-2017-data-protection-survey-37950

Forcepoint. (2017). 9 Steps to building an insider threat defense program. Retrieved from https://www.forcepoint.com/resources/whitepapers/9-steps-building-insider-threat-defense-program

Gartner. (2017, August 16). Gartner says worldwide information security spending will grow 7 percent to reach $86.4 billion in 2017. Retrieved from https://www.gartner.com/newsroom/id/3784965

Gates, S., & Mercer, C. (2017). Nsfocus threat intelligence 2017 predictions report. NSFOCUS., retrieved from https://nsfocusglobal.com/wp-content/uploads/2015/10/TI-2017_Predictions_Report__v4.pdf

Gelles, M. G. (2016). Insider threat: prevention, detection, mitigation, and deterrence. Amsterdam: Butterworth-Heinemann.

Gogan, M. (2016, November 18). The threat of privileged user access - monitoring and controlling privilege users. Retrieved from https://www.scmagazineuk.com/the-threat-of-privileged-user-access--monitoring-and-controlling-privilege-users/article/568624/

Goldman, A. (2017, February 08). Government contractor indicted in theft of top-secret documents. Retrieved from https://www.nytimes.com/2017/02/08/us/politics/harold-martin-nsa.html?_r=0

Google Cloud Platform. (2017, June 22). Preventing data exfiltration | documentation | Google Cloud Platform. Retrieved from https://cloud.google.com/security/data-loss-prevention/preventing-data-exfiltration

Gorman, P. (2016, November). Five third-party cybersecurity myths.

Greitzer, F. L., Imran, M., Purl, J., Axelrad, E. T., Leong, Y. M., Becker, D. E., Laskey, K. B., Sticha, P. J. (2016). Developing an ontology for individual and organizational sociotechnical indicators of insider threat risk. Retrieved from http://ceur-ws.org/Vol-1788/STIDS_2016_T03_Greitzer_etal.pdf

Haber, L. (2017, April 20). Dell end-user security survey highlights security concern vs. productivity. Retrieved from http://www.channelpartnersonline.com/news/2017/04/dell-end-user-security-survey-highlights-security.aspx

Harris, M. (2017, February 23). Who is Anthony Levandowski, and why is Google suing him? Retrieved from https://www.theguardian.com/technology/2017/feb/23/anthony-levandowski-google-uber-self-driving-cars-lawsuit

Henderson, J. (2015). The insider threat timeline. Retrieved from http://www.insiderthreatdefense.com/pdfs/ITD Insider Threat Timeline 2-21-14.pdf

Hewes, A. C., Jr. (2016). Threat and challenges of cyber-crime and the response.

Holpuch, A. (2017, June 06). Reality Winner faces 10-year sentence in first espionage act charge under Trump. Retrieved from https://www.theguardian.com/us-news/2017/jun/06/reality-winner-espionage-act-leak-russian-hacking

IBM. (2016). 2016 Cyber security intelligence index. Retrieved from https://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03133usen/SEW03133USEN.PDF

Imternedia. (2015). Meet the business world's riskiest user. Retrieved from https://www.intermedia.net/report/riskiestusers

Kansteiner, M. J. (2016, June). Mitigating risk to DOD information networks by improving network security in third-party information networks. Retrieved from https://calhoun.nps.edu/bitstream/handle/10945/49502/16Jun_Kansteiner_Michael.pdf?sequence=1&isAllowed=y

Keanini, T. (2015, May 28). Why are insider threats so difficult to detect? Retrieved from https://www.itproportal.com/2015/05/28/why-insider-threats-difficult-detect

Kopan, T., Perez, E., & Jarrett, L. (2017, February 08). Former NSA contractor indicted in stolen data case. Retrieved from http://www.cnn.com/2017/02/08/politics/nsa-contractor-alleged-classified-theft-harold-martin-indictment/index.html

Lord, N. (2017a, January 26). What is data loss prevention (dlp)? A definition of data loss prevention. Retrieved from https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

Lord, N. (2017b, July 26). What is the principle of least privilege (polp)? a best practice for information security and compliance. Retrieved from https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance

Lord, N. (2017c, August 31). Phishing attack prevention: how to identify & avoid phishing scams. Retrieved from https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams

Narayan, K. (2017, May 18). 5 Devious instances of insider threat in the cloud. Retrieved from https://www.skyhighnetworks.com/cloud-security-blog/5-devious-instances-insider-threat-cloud/

NIST. (2017, September 26). Role based access control | crsc. Retrieved from https://csrc.nist.gov/projects/role-based-access-control

NTTSecurity. (2017). Global threat intelligence center (gtic) quarterly threat intelligence report. Retrieved from https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/ntt-security-GTIC-2017-q3-threat-intelligence-report.pdf

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: an insider threat perspective. Decision Support Systems, 92, 47-56. doi:10.1016/j.dss.2016.09.012

Paganini, P. (2017, February 28). Boeing notified 36,000 employees following an accidental data leak. Retrieved from http://securityaffairs.co/wordpress/56736/data-breach/boeing-data-leak.html

Ponemom. (2016). Closing security gaps to protect corporate data: a study of US and European organizations. Ponemon Institute LLC. Retrieved from

https://info.varonis.com/hubfs/docs/research_reports/Varonis_Ponemon_2016_Report.pdf

Protenus (2017). 2017 on track to exceed 2016 trend of 'one health data breach per day'. Retrieved from https://www.protenus.com/hubfs/Breach_Barometer/2017/Mid Year Review/2017 Protenus Breach Barometer Mid Year Review.pdf?utm_campaign=Breach+Barometer&utm_medium=email&_hsenc=p2ANqtz-_ih8kwB15UPZBdGlha4KFl9963vuXgyt9ufyzVIDT98z1Da1L

Sagan, S. D. (2017, Feb 20). How governments and companies can prevent the next insider attack. University Wire Retrieved from https://search.proquest.com/docview/1870121719?accountid=28902

SANS. (2017). 2017 Security awareness report. Retrieved from https://securingthehuman.sans.org/media/resources/STH-SecurityAwarenessReport-2017.pdf

Schuchter, A., & Levi, M. (2016). The fraud triangle revisited. Security Journal, 29(2), 107-121. doi:10.1057/sj.2013.

Schulze, H. (2016). Insider threat spotlight report. INSIDER THREAT. Retrieved from http://crowdresearchpartners.com/wp-content/uploads/2016/09/Insider-Threat-Report-2016.pdf

Scott, J., & Spaniel, D. (2017). Deception and the insider threat. managing the insider threat, 1-52. doi:10.1201/b12063-10

Shane, S., & Becker, J. (2016, October 29). N.S.A. appears to have missed 'big red flags' in suspect's behavior. *New York Times.* Retrieved from https://www.nytimes.com/2016/10/30/us/harold-martin-nsa.html

Singh, S., Jeong, Y., & Park, J. H. (2016, November). A survey on cloud computing security: Issues, threats, and solutions.

Souza, E. (2016, October 26). Defeating insider threats in the cloud. Retrieved from https://blog.cloudsecurityalliance.org/2016/10/27/defeating-insider-threats-cloud/

Stoneff, C. (2017, April 25). Insider threats or external cyber attacks: which is worse? Retrieved from https://www.identityweek.com/insider-threats-or-external-cyber-attacks/

Symantec. (2017a, April). Internet threat security report. Retrieved from https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_

Symantec. (2017b). Implementing an effective insider threat program. Retrieved from https://www.symantec.com/content/dam/symantec/docs/white-papers/implementing-an-effective-insider-threat-program-en.pdf

Thales. (2017). 2017 Thales data threat report. Retrieved December 10, 2017, from https://www.thalesgroup.com/sites/default/files/asset/document/thales_2017_data_threat_report-global_edition.pdf

Trend Micro. (2016, June 9). Billion-dollar scams: the numbers behind business email compromise. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise

Tripwire. (2017, April 11). Insider threats as the main security threat in 2017. Retrieved from https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/

Trzeciak, R. (2017, November 06). 5 best practices to prevent insider threat. Retrieved from https://insights.sei.cmu.edu/sei_blog/2017/11/5-best-practices-to-prevent-insider-threat.html

Upton, D. M., & Creese, S. (2014, September). The danger from within. Retrieved from https://hbr.org/2014/09/the-danger-from-within

Veriato. (2016). Insider threat spotlight report. Retrieved from https://www.veriato.com/docs/default-source/whitepapers/insider-threat-report-2016.pdf

Verizon. (2017, May 02). 2017 dbir: understand your cybersecurity threats. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Vormetric Data Security. (2015). Trends and future directions in data security. Retrieved from http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf

Ware, B. (2017). Insider attacks industry survey. Retrieved from https://haystax.com/blog/ebook/insider-attacks-industry-survey/

Waters, M. D. (2016, November 29). Identifying and preventing insider threats.

Willemssen, J. C. (2015). Federal agencies need to better protect sensitive data. Retrieved from http://www.gao.gov/assets/680/673678.pdf

Worrall, J. (2014, October 14). The 'insider threat' is privileged access, not a person. Retrieved from https://www.cyberark.com/blog/insider-threat-privileged-access-person/