2-15-2024

Strategies for Insider Threat Mitigation and Detection

Adam Clifton
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Adam Clifton

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Cynthia Phillips, Committee Chairperson, Information Technology Faculty
Dr. Alan Dawson, Committee Member, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2024

Abstract

Strategies for Insider Threat Mitigation and Detection

by

Adam Clifton

MS, Walden University, 2023

BS, Park University, 2013

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

February 2024

Abstract

Some information technology (IT) security professionals lack strategies to protect against insider threats. This lack of strategy is concerning because of the widespread organizational damages from insider threat incidents within global organizations, which often lead to financial penalties against organizations and a lack of public trust. Based upon the total quality management model, the goal of this qualitative multiple-case study was to explore strategies IT security managers used to secure their organizations against threats from trusted insiders. Data were collected by conducting semi-structured interviews with five high-level network security practitioners specializing in insider threat mitigation. Five themes emerged during data analysis: risk acceptance and tolerance, operating environment limitations, employee profiling, proactive measures, and measurement of success. A key recommendation is for IT security managers to implement a risk register for security gaps in their organizations to improve their insider threat mitigation strategies. The potential implications for positive social change include bolstering the public's confidence in the organizational safeguarding of personal information, leading to improved security relating to economic transactions.

Strategies for Insider Threat Mitigation and Detection

by

Adam Clifton

MS, Walden University, 2023

BS, Park University, 2013

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

February 2024

Acknowledgments

I wish to thank my committee chair and mentor, Dr. Phillips. I greatly appreciate your guidance throughout this rigorous doctoral process. I would also like to extend my gratitude to Dr. Dawson and Dr. Miles. This has been an arduous, yet fun journey, and I appreciate everything I have learned from you all.

Special thanks to Dr. Kunath, for helping me begin this journey. And especially, Jim Jantz, for showing me a shining example of what exemplary leadership is. This journey took a toll on me, on many occasions. And, if it was not for Jim's continuous support and encouragement, I would have not succeeded. Words cannot express how grateful I am for you, Jim, from the bottom of my heart. This would have not been possible without your unwavering support. Thank you for teaching me what it truly means to support your people.

Table of Contents

List of Tables

Section 1: Foundation of the Study

The focus of this study was the problem of insider threat in the information technology (IT) landscape and methods to further understand and mitigate the problem. An insider threat can be defined as a person with malicious intent who has legitimate access to organizational systems (Gunasekhar et al., 2015). This topic has gained extensive media attention in the past few years, not only in the government space but also in the private sector. This threat can cause serious monetary and reputational damages to an organization (Sanders et al., 2019). In a 2018 IT industry survey, over a third of organizations that responded had experienced multiple (five or fewer) attacks from a trusted insider, indicating that insider attacks had become more frequent (Alsowail & Al-Shehari, 2020). This increase is especially alarming when compared to surveys from 10 years earlier, where a quarter of survey respondents identified experiencing insider threat attacks (Gupta & Sharman, 2012). Research on standards and practices, lessons learned, and cutting-edge mitigation strategies may yield new insight that stakeholders can use to improve company defenses against insider threat. Improvements to insider threat mitigation response and prevention is important to numerous global organizations.

Background of the Problem

Annual industry surveys consistently showed that insiders pose the second greatest cybersecurity threat, exceeded only by hackers, and that insider attacks were costly for organizations to recover from (Greitzer, Purl, Becker, et al., 2019). Existing research on insider threat has primarily focused on network activity logs and metrics, as the majority of research papers identified during the literature review pertained to this

specific topic. Data sets were often segregated based on their source. Researchers often used the Carnegie Mellon University (CMU) open-source threat data set in their studies involving varying data science techniques (Hsu & Wu, 2023). With data sciences gaining momentum in the tech industry, current researchers often revisited the findings of studies conducted many years ago, applying trending data science methodologies to identify new vectors for potential research. Recent studies identified within the Walden Library resource had documented recently disclosed instances of insider threat activity. The literature indicated a gap in knowledge centered on actual prediction and mitigation strategies implemented within current IT organizations. Furthermore, there was an opportunity for further research with a larger participant pool that represented varying employment positions.

Problem Statement

Preventing insider threats is a challenging task for IT professionals. Industry standard practices center on the analysis of network activity logs that can quickly scale beyond the capabilities of a human analyst (Tuor et al., 2017). Therefore, it can be a challenge to detect and identify authentic malicious insider threats within a reasonable time frame without properly tuning analysis methods to promote predictability. Findings from a recent survey focused on targeted incidents of cybercrime showed that over 27% were perpetrated by a trusted insider and that overall damage was more severe than for attacks by external attackers (Trzeciak, 2017, as cited in Homoliak et al., 2019). The general IT problem was that current industry strategies to protect against insider threat are ineffective. The specific IT problem was that some IT security professionals lack

strategies to protect against insider threats. The focus of this study was real-world insider threat mitigation and prevention strategies within large scale commercial IT companies and U.S. government organizations.

Purpose Statement

The purpose of this qualitative multiple-case study was to identify the strategies used by IT security managers to protect their organizations against insider threats. The population for this study was IT security managers in the private sector and U.S. government facilities in the continental United States. I invited contacts made during the last 5 years of employment, who shared an interest in preventing insider threat, to participate in this study. The contribution to social change was the potential limiting of negative impacts to internal systems from an insider threat, to include unauthorized disclosure of classified data and loss of proprietary information. These acts can cause irreparable damage to an organization's public reputation, as well as the potential for the loss of life within classified information mission domains (BaMaung et al., 2018).

Nature of the Study

To address the research question in this qualitative study, I chose a multiple-case study design. This approach was appropriate for this study because of its wide range of data collection possibilities (Dieterle & Duchek, 2023). Possibilities included interviews, surveys, and interactive forums. I used participant interviews as the primary method for gathering information during this study. These formal and informal information exchanges are a key characteristic of the qualitative design (Croix et al., 2018). The open-ended nature of interviews is a key feature of a qualitative approach. When incorporated

into an interactive framework, data from interviews are a valuable contribution to the research process (Devotta et al., 2016).

I considered using a quantitative approach due its effectiveness for the analysis of data sets that were properly formatted for automated ingestion. A survey-based data set could potentially work well with quantitative modeling software. Survey-based data sets can also be used to reanalyze the data to identify new patterns due to their generally smaller confined size (Qin & Kong, 2022). Quantitative modeling can include regression, class counting, risk sums, and role counting. In one recent study, researchers identified associations among data constructs beyond previously predefined hierarchical relationships, this resulted in the identification of data outliers that could contribute to improved insider threat prediction (Greitzer, Purl, Becker, et al., 2019). An underlying assumption regarding quantitative modeling is that the data sets used were large enough to be useful for analysis. One noticeable limitation with a survey-based approach is the potential for bias by the study participants (Katz et al., 2022). The injection of personal opinions into a mathematical data set could lead to results that featured opinions versus impartial knowledge. I also considered a mixed-methods approach for the study. However, when a mixed-method approach is used, researcher bias poses a serious threat to validity and limits the impact of inferences made during research (Emary et al., 2022). Due to these potential limitations, quantitative and mixed-method approaches were ruled out in favor of a qualitative method.

Research Question

What strategies do IT security managers use to protect their organizations against insider threats?

Interview Questions

1. What strategies do the IT security professionals within your organization use to detect insider threats? The sub question was as follows: Are they effective, and how do you measure the success of these strategies?
2. What strategies could be revamped with newer technologies to better perform insider threat detection?

Conceptual Framework

I based the conceptual framework for this study on TQM. The concept of TQM was initially introduced to monitor quality in mass production manufacturing. The evolution of TQM is the accumulation of various Japanese and American philosophies, approaches, and strategies. The Japanese were the first to start the quality improvement movement, and they also applied these strategies in organizations in the United States (Milakovich, 1998).

TQM is an integrated approach and encompasses a set of practices that emphasize top management commitment, the satisfaction of customer needs, continuous improvement, employee involvement and team work, and employee empowerment (Issac et al., 2004). TQM can be defined as a philosophy and set of practices for continuous organizational improvement. The adoption of TQM enabled Japanese companies to become competitive in various sectors, including automotive and electronics; later, their

successes inspired business leaders in developed countries to adopt TQM for their organizations (Yu et al., 2020). Annual industry surveys consistently showed that insiders pose the second greatest cybersecurity threat, exceeded only by hackers, and that insider attacks are the costliest to organizations (Greitzer, Purl, Becker, et al., 2019). The TQM framework was appropriate for this qualitative study due to its encompassing of multiple employee echelons. A core philosophy in the successful implementation of TQM within an organization is the commitment of all levels of management and low-level employees to pursue the optimal path to achieve the established organizational goals (Islam & Salam, 2022). The participants were from multiple organizational levels, including leadership, midlevel management, and senior to entry-level technicians. The participants may all benefit from an improvement in insider threat detection, and their involvement was aligned with TQM's inclusive nature.

Definition of Terms

Chief information security officer: The senior executive position in an organization responsible for leading information security related programs and processes (Smit et al., 2021).

General Data Protection Regulation (GDPR): The European regulation for protecting the collection and processing of personally attributable digital information (Cejas et al., 2023).

Heating, ventilation, and air-conditioning: Systems in place to maintain proper temperature, especially as relating to information systems and servers that produce large amounts of heat within secured areas (Wang et al., 2023).

Information system security officer: Technician-level positions within an organization responsible for system security administration and compliance (Sundararajan & Ghodousi, 2021).

Insider threat: Any situation in which a member of an organization behaves or acts in an illegal or unethical manner contrary to the interests of the organization (Ho, Hancock, et al., 2016).

Machine learning: Algorithms towards the creation of a production-oriented models for data analysis (Paraskevoulakou & Kyriazis., 2023).

MATLAB: A software application for processing numerical, modeling, and simulation problems (Zeng et al., 2023).

Non-commissioned officer: A military technician-level position within an organization, often performing work and managing junior level technicians (Lane et al., 2022).

Personally identifiable information: Information relating to a consumer, that can identify them via private information, such as social security number, address, real name, phone number, etc. (Markos et al., 2018).

Professional military education: Instructional knowledge comparable to collegiate materials for leadership skill development (Weissmann et al., 2022).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions can be referred to as commonly accepted information for use in the professional research method (Kirkpatrick et al., 2022). They are important to understand

as they can aid in the construction of the study elements. By stating their assumptions, researchers can promote a dialogue during study design that ensures that areas deemed lacking can be reinforced. I assumed the potential for unconscious bias, which I sought to reduce as much as possible. Participating individuals may have been biased based on their past experiences, and it was important that the researcher maintained integrity in all interactions. I also assumed that all study participants understood the insider threat from a network security perspective and that their responses would provide tangible insight into current insider threat strategies. Their input was expected to be truthful and relevant. The quality of the results depended on the cooperation of the subjects in honestly responding to the interview questions.

Limitations

Limitations in research refer to factors that may threaten the internal validity of a study, leading to a result that may not be as accurate as originally envisioned (Shahriari & Rasuli, 2020). Limitations to a study are important to be clearly stated, as they can impact the reception of the study's findings. IT personnel and management were the primary focus of this study; the study did not reflect perceptions of organizational employees outside of these targeted participants. Due to this limitation, the findings of this study may not be applicable to some industries. The quality of the participants and the variety of IT companies for which they work may have compensated for any limitations in the number of participants.

Delimitations

Delimitations refer to limits that a researcher establishes to ensure that a targeted scope is maintained and shortcomings to the research process can be exposed (Theofanidis & Fountouki, 2018). Delimitations aid the researcher in establishing boundaries within the study to encourage a targeted focus of efforts. Research topics have the potential to grow as the researcher reacts to the influx of data during the gathering stages. For this study, there were specific organizational boundaries due to the IT focus. I targeted the IT private sector and government IT establishments.

Significance of the Study

Contribution to Information Technology Practice

This study is significant in that it may be of value to IT practitioners and organizations because of the financial damage an insider threat can produce. Routine IT industry surveys regularly indicated that an insider threat posed the second largest cybersecurity threat, next to hackers, and that insider threat attacks were the costliest to recover from (Greitzer, Purl, Becker, et al., 2019). This study may contribute to more effective IT practices by providing IT personnel and leaders with information they can use to develop strategies to improve insider threat detection in their organizational IT domain.

Implications for Social Change

The existing literature on insider threat supported that further research on some target areas could aid in security improvements. A large portion of research identified within the Walden Library over the last 5 years employed methods to increase the

detection ratio of an insider threat incident. It was unlikely that this would decrease in importance anytime soon, however; its efficacy can be limited by the real-world threat mitigations employed by organizations today. The results of further investigation may in turn contribute to a positive social change by minimizing damage to information systems and the mission. I also sought to aid in the elimination of the negative social effects of insider threat. Researchers studying insider threat often used organizational factors that applied to negative social perceptions of organizations that have been impacted. The damaging aspect of an insider threat incident can be aligned and likened to a terrorist act (BaMaung et al., 2018). This alarming connection may lead to mitigation efforts by less enthusiastic organizational leaders.

A Review of the Professional and Academic Literature

This literature review provided an overarching view of the insider threat problem faced by organizations throughout the globe. This section encompassed 119 peer-reviewed journal articles and professional articles related to the topic of insider threat. The analysis of peer-reviewed research included five areas: case study reviews, technological vulnerabilities, simulations and modeling, organizational posturing, and the study's conceptual framework. I found these areas of focus to be a common ground within the recent literature relating to the general topic of insider threat. Some of the research crossed into the boundaries of more than one of these identified areas. These instances further solidified the specific focuses within the IT landscape. The organization of these key themes informed the development of the research project. I also provided an in-depth analysis of the chosen conceptual framework, TQM. This analysis included the

origins of TQM, definitions, types of research common with TQM as a framework, and success and failures in TQM adoption. The TQM analysis was performed with a focus on its applicability to the organizational dilemma of the insider threat.

I found the 119 selected sources by using resources within the Walden University Library. Through an initial web portal query, I obtained literature from linked research libraries to include EBSCOhost, IEEE, and the ACM Digital Library. Google Scholar was also referenced for many of the chosen literature to ensure proper APA information for some of the more obscure research documents. Of the selected literature for this review, 109 of the 119 articles (92%) were within the recommended window of the last 5 years. Peer-reviewed scholarly journals were the key requirement for document searches, in an effort to eliminate the potential for less credible sources. Initial key word searches used included *insider threat*, *malicious activity*, *employee threat*, *technical controls*, *automated detection*, *defense-in-depth*, *deterrence*, and *security methods*.

Case Study Reviews

The use of case studies was a reoccurring theme with regard to recent peer-reviewed articles on the topic. This was especially the case with regard to recent incidents that gained media attention due to high-profile negative impact. As Jeong and Zo (2021) noted, insider threats can have a severe organizational impact; in their study, 68% of business leaders reported feeling vulnerable to insider attacks, and 52% of survey respondents found coping with insider threats more challenging than external cyberattacks. Cause and effect patterns were often a focus when new insider threat stories were released to the public. This was especially true when there was a breach of customer

data involved. This type of documented resource can be limited when organizations choose not to disclose information related to incidents of insider threats that they fell victim to (Schoenherr, 2022). Without the benefit of in-depth research into the full disclosures of previous insider threat incidents, sometimes case studies were opinion-based.

The recent literature included many case studies of insider threat incidents that had been made public through news outlets. The media attention that surrounded insider threat incidents often provided details that warranted further research into cause-and-effect patterns. These types of details can often go unreported when organizational leaders do not employ full disclosure procedures during an incident (Schoenherr, 2022). In recent studies, researchers used many of these publicly disclosed incidents to increase awareness of the problem by surveying steps to review current insider threat methodologies. By surveying recent incidents, classifications can be made regarding industry responses to the incidents, improving the collective defensive solutions to be used against future insider threat incidents (Homoliak et al., 2019). This method of providing a snapshot of the current state of insider threat as it was during publication offered a useful baseline of activities and thought processes of employees directly involved for better understanding insider threat.

Case study research may also promote improved security practices within an organization. As long as the research conducted is recent in nature, and could relevantly be used to address an existing problem within an organization, it could yield benefits. This method is a positive force for raising awareness for security practitioners within an

organization, as well as prompting an improvement of efforts regarding insider threat mitigations and internal programs (Greitzer, Purl, Leong, & Sticha, 2019). When research is limited by its focus on an organizational situation, it could potentially stray from an overall threat picture that could benefit from the use of a more general lens. This type of research may be less applicable for baselining the insider threat landscape for future research efforts, especially if its focus was too fine to be relevant outside of its specific landscape; however, it would still be a valuable resource for complimenting research into the insider threat topic during initial information gathering. Also, even if deemed too specific, outlier data could be gleaned from the information by skilled analysts who used these techniques to bridge information gaps that were not previously attached to such a specific information source (Lu et al., 2022).

The authors of a recent journal article catalogued recent case studies to provide a frame of reference for further study of insider threat incidents. Homoliak et al. (2019) scrutinized recently reported insider threat survey data for relevancy and categorized the findings into three components of approaches taken by perpetrators: user permission based, network level access, and blended methods. These commonly used stratagems employed by malicious actors within the last few years identify potential interview questions for IT leaders. The review also illuminated areas of concern that may have been previously overlooked as negligible by security practitioners. The review of recent incidents further established the categorization of descriptive levels among insider threat employees. There were three levels of insider threat identified: first were self-motivated actors who act under their own volition, second were recruited actors who are often

convinced or coerced by a third party, and third were planted in an organization for the expressed intent to perform malicious acts (Homoliak et al., 2019).

The accurate labeling of personas within an organization is a key component when devising organizational posturing solutions or standing up new security protocols and policies. In contrast to this approach to reviewing incidents, another method for case study review was to catalog performed professional surveys conducted among organizations. Surveys identified similar insider threat level definitions with different naming conventions. The unintentional insider threat was identified, self-motivated and coerced actors were referred to as masqueraders, and planted insiders were referred to as traitors (L. Liu et al., 2018). Survey researchers weighted the collected data with pros and cons for use in further research vectors. Both surveys shared identical component approaches for categorization. The arrival at many similar conclusions during analysis further established the respective validity of both case study reviews.

Situational case study reviews are especially relevant in today's post-Covid-19 climate. There have been many changes to the IT landscape since the beginning of the pandemic in 2020, and case studies that detailed issues during this transition period are useful to organizations anticipating the need to adapt to the change. In 2019, it was estimated that over 60% of companies throughout the world allowed remote working capabilities for their employees, and this number has drastically increased since early 2020 (Bulpett, 2020). Telework initiatives are a strategy for continuing to employee critical workers who may have personal issues that would otherwise force them to seek employment at other locations. As a remote workforces increased during this time of

continued social distancing efforts, it was likely that sustained infrastructures would potentially migrate to cloud offerings in an attempt to maintain budgetary requirements within an organization (Hubbard et al., 2021). Case studies that illuminated pros and cons of cloud migrations for IT requirements could provide blueprints for newcomers to the technological shift. Identity management was a top focus among security practitioners as workforces transition to cloud infrastructures. Per Bulpett (2020), the use of artificial intelligence and machine learning solutions for identity management and control played larger roles as businesses evolved towards more cloud-based architectures, and this yielded benefits to the IT security staff as routine administrative tasks regarding identity management were automated.

Case studies into recent insider threat attacks could also enlighten security practitioners about behavioral indicators for strengthening organizational postures against malicious activity. The Tesla Motors insider threat incident from 2020 was an example of uncovering personality traits that lent themselves to internal criminal intent against an organization. As Maasberg et al. (2020) observed, this insider attack consisted of technical sabotage via performing program-damaging programmatic changes to the core operating system code base and exporting a large amount of highly sensitive proprietary data to third parties. This individual was later described as a psychopath, Machiavellian, and narcissistic (Maasberg et al., 2020). These character traits are useful to be aware of to weed out potential employees during the hiring process. It is critical for frontline supervisors to be perceptive to the existence of these character traits in currently employed subordinates.

Regional case studies can be valuable to global security practitioners as they can illuminate problem spaces that have yet to emerge in their area of the globe. The authors of a recent case study review compiled nearly 100 insider threat incidents that were committed in the United Kingdom from 2012 to 2022. The research involved interviews with employees familiar with each insider; the interviews took place within a year of each incident, and all aspects of the activity were discussed, to include work and social details about the insider, behaviors before and after the incident, and each interviewee's understanding of the attack and how it was detected (Whitty, 2021). Many of the levels and personality traits rose to the top of the list of commonalities. With such a large set of separate incidents, this type of recent research can be helpful in identifying common behavior patterns and techniques used during insider threat incidents. These increased commonalities can be crucial for targeting areas of security lacking in an organizational threat response and prevention methodology.

In contrast to the more generalized case study reviews, a more targeted case study review can shed light on organizational elements that may be lacking in expertise and unsure what top glean from less focused research. A recent study focused upon the insider threat element within military operations engaged in peace support missions. Tibor and Lajos (2020) stated that, during peacekeeping operations, insider threat attacks often took place during initial phases involving force stabilization efforts, often stemming from verbal insults, personal failures, or some other perceived social or personal injury leading to a negative resentment. The authors shared firsthand accounts of military observations regarding insider threat, this added a firmer relevance to similar scenarios

within the military. Recent research found within the Walden Library resource was often focused on financial impact to an organization. Elements of a scenario such as the high stress military environment can offer new insight to scenario-based threat response. By adding an extra layer of scenario-based specificity to the insider threat mitigation strategy within an organizational security group, documented insider threat scenarios can be used as a blueprint to employ mitigations against potential future incidents.

With regard to insider threat research, the military and government sectors had rarely gotten research attention compared to the public and private sectors. According to Kelly (2018), governmental insider threat incidents can damage the morale of the institution as a whole and inject a lack of confidence in the governing bodies capabilities among the general public when it is learned that an insider threat has been harbored for long periods of time. In recent years, classified government leaks to the media have put government research in the spotlight. This spotlight was often centered on the vast number of documents leaked. This was the case with Army Private Manning, who leaked over 500,000 classified documents to the WikiLeaks organization, and with National Security Agency contractor Edward Snowden, who used social engineering and computer-savvy techniques to exfiltrate and leak approximately 1,500,000 highly classified intelligence documents of U.S. and partnered country origin (Gioe & Hatfield, 2021). It can be especially difficult to detect an insider threat within a classified environment, because there are extensive screening processes in place to screen out applicants who are untrustworthy, or potentially morally corruptible, and there were also more in-depth monitoring consents in place.

Insider threat incidents can also share elements of toxic workplace environments. During his 2020 trial for stealing and leaking classified information, CIA programmer Joshua Schulte's coworkers testified that his behavior before his arrest involved vandalism, bullying, and retaliations against peers (Creech, 2020). However, when compared with Edward Snowden and Private Manning, this toxic behavior seems unique within the confines of classified enclaves. A proposed strategy to better mitigate the potential for insider threat would be to increase monitoring during initial hiring phases. Illegal activity from insider threats has often started shortly after the initial employment phase, and it would be practical to reperform background investigations more frequently and to include more regular polygraph examinations (Kelly, 2018). These case studies provided a reference point for future researchers. This frame of reference can assist a researcher in remaining up-to-date with general topics.

Technological Vulnerabilities

Scholarly researchers tended to target a specific technology and illustrate the vulnerabilities of an organization from an internal security perspective (Jurišić et al., 2023). This level of granularity can offer new insights towards threat vectors and can be useful for persuading management buy-in for mitigation efforts or instantiating new security policies and procedures. Although, depending on how narrow the focus is on the particular technology in question, results may not be applicable to organizations that do not use these niche systems.

There have been numerous studies identified using the Walden Library resource that used specific technologies and their vulnerabilities to an organization from an insider

threat perspective. This research can offer a unique picture to illustrate to organizational leadership the importance of threat mitigation tailored to a targeted system. However, given the narrow confines of this type of research, the results may not scale to other organizations that do not employ these niche systems. Z. Liu and Wang (2021) noted that access to leaked information was very beneficial for an attacker when targeting power systems, and inversely, a security practitioner's awareness of leaked information can be vital in ensuring the proper strategy is employed in defense of the affected system. In one study, the researchers focused on redistribution load attacks against U.S. power plant systems by a malicious insider. The study featured a comparison of case studies relating to this niche attack vector. Each source case study represented a publicly released cyber-attack against a U.S. power plant system. This type of targeted attack can have damaging implications similar to all other potential insider threat vectors. While focusing on proprietary information leakage regarding power systems, the potential negative impact could lead to catastrophic failures in the power service commercial space. The effects can be doubly so, due to the sensitive details of a functioning power system that were meant to be protected from release to the public. The sensitive nature of these type of secure systems could offer a high-value target for insider threat actors.

Power related infrastructure attacks have been an increasing concern in the public sector in recent years. In 2016, a Ukrainian power grid was the target of cyber-attacks twice within a calendar year, affecting service for over 225 thousand customers (Z. Liu & Wang, 2021). Due to the increased connectivity of smart grids, there is a growing concern regarding vulnerability, especially if insider threats are involved. Data integrity

attacks, also referred to as False Data Injection (FDI), have been known to bypass system security designs and negatively impact operational systems (Gönen et al., 2020). In a recent study, a smart-grid testbed was created to simulate the real-word components of a smart grid system. By successfully simulating FDI attack, the testbed became compromised and the capability for disruption was identified and documented. In a related study, where smart grids were also the focus, researchers used behavioral based network activity confined specifically within the smart grid network, in order to find outliers within the data sets. This was particularly interesting because the research did not depend on fabricated data sets. Per Bao et al. (2016), by performing a comparative analysis on real-world data, the research outcome demonstrated an improvement to the behavior rule-based approach for the detection of insider threats. The details of the study were directly correlated to real world scenarios that smart grid security practitioners could use to improve their security efforts.

Another technological area of concern was cloud computing. During the initial stages of the Covid-19 pandemic, many organizations made strides to improve their cloud presence in order to better accommodate the massive increase in telework demand (Koyama et al. 2022). In early 2020, migrated services to the cloud became a cost-cutting solution for approximately 73% of global organizations, and is expected to be a $3,000,000,000 market as of today (Alhebaishi et al., 2019). This level of reliance upon a fairly new technology for new adopters can raise security concerns that many organizations may not have effectively planned through. The larger the employee usage of the cloud infrastructure, the greater the concern may be for inexperienced cloud

security practitioners. The potential for an insider threat incident was escalated when the amount of an organizations cloud users is maximized, because the amount of data that was potentially breachable was also maximized (Althebyan, 2020). Data that are not centrally located can be a new concept for security practitioners used to managing their infrastructure on premises; however, many of the same principals of data security apply. A recent study performed on mitigating the insider threat in a cloud environment utilized many of the familiar tasks a network security professional would employ securing their own networks. Per Alhebaishi et al. (2019), the first step was to identify network maintenance tasks and their security concerns due to privilege escalation, then constraints were applied to mitigate those concerns, and finally, different use case scenarios were explored to confirm the effectiveness of the proposed solution. As cloud solutions continued to gain traction in the IT landscape, it was imperative to maintain an awareness of insider threat mitigations when security procedures were employed. In contrast to the generic security concerns of the cloud, a recent study into the threat of malicious insiders upon the mobility as a service (MaaS) model of cloud computing, opened up new avenues for security implementations due to cloud computing's vast nuanced offerings available to the public at large. The openness baked into an MaaS implementation can lead to concern regarding security. Per Callegati et al. (2018), a proposed architecture to limit the insider threat potential for MaaS, was built around the methodology to constrain the quality and quantity of data-in-transit, in an effort to optimize network route queries to target the paths to specific users for response.

Many targets of insider threat involved confidential information and records related to personal data. Per Eggenschwiler et al. (2016), within financial industry reported accounts, monetary motivations were behind the majority of insider attacks, and often involved theft of personal records. Banks and financial systems can be a lucrative cyber-target both from outside and inside the network (Arce, 2023). In two recent studies, British and Ethiopian, vulnerabilities within financial systems were researched with a focus on insider threat activity. The Ethiopian study targeted the unintentional insider threat, and recommended increased real-time surveillance of financial computing systems in order to counter innocent mistakes that can lead to levied fines and loss of customer faith (Adane, 2020). Within the United Kingdom, businesses that provided financial services were 300% more likely to be the victim of cyber-attacks than other institutions (Eggenschwiler et al., 2016).

There are other realms of technology that are susceptible to attack vectors besides extremely niche arenas. The same methodologies used for narrow focuses can also be applied to technologies gaining in popularity. The Internet of Things is an example of a technology that is experiencing an adoption boom with the security elements racing to catch up with its popularity. Per A. Kim et al. (2020), using generalized examples of insider threat, the increased attack surfaces associated with scaling Internet of Things within an organization can cause significant security concerns for security personnel. While technological vulnerability studies related to insider threat can provide useful details on the subject, most of the findings would also apply to the misuse of the technology itself without the insider threat angle leveraged. This type of relation to

insider threat research leads me to believe that any current technology could be grouped into a generalized vulnerability study and shoe-horned into the insider threat arena after the fact.

Simulations and Modeling

The use of simulations and modeling software against insider threat data sets was identified in many collegiate studies found within the Walden Library resource. Two popular study paths within this framework were targeted machine processing and the use of modeling algorithms. The use of open-source insider threat data sets was popular among these studies. Specifically, the CMU freely available public data set was often chosen for practical use in these case studies.

Modeling simulation literature can be easily splintered into two categories: modeling algorithms and targeted Machine processing. The implementation of modeling simulations against insider threat data sets was by far the most prevalent research available for this topic. There were many studies identified and discarded for similarities relating to taking a popular open-source insider threat data set, and feeding it into a newer modeling technique. The CMU publicly available insider threat data set was the most common data source used against various modeling simulations. It was often used due to its extensive data-sets containing nearly 14GB of text-based logs and communications. One study that used the CMU data set against a modeling simulation was the employment of a time-series classification of user activities to detect anomalies (Chattopadhyay et al., 2018). Network logs were heavily targeted in the data set, and the groupings of activities within a construct of time, showed promise for potentially accurate scenario-based threat

prediction. The study used a clever technique to increase the limited amount of data sets, by doubling and randomizing meta data fields to mimic a larger and more user populated network infrastructure. The results of the study, as hypothesized, were nearly identical when compared to the original data set and the extended data set, offering an interesting vector incident predictability

The use of quantitative modeling simulations can be a useful tool when applied to the right formatting of data sets. In one identified study, the researchers employed numerous quantitative modeling techniques against a survey-based data set. These quantitative models included counting, regression, sum-of-risk, class-count, and role-count. It was identified that singular insider threat indicators reflected different threat associations versus grouped threat data (Greitzer, Purl, Becker, et al., 2019). By incorporating a survey-based rated questionnaire, this survey stood out as not incorporating the popular CMU data set. The way the surveys were enumerated, this illuminated potential other ways of getting away from the heavily used CMU data set during future potential research efforts. An underlying assumption was that collected data to be modeled would be robust enough to identify noticeable outliers of the data sets during analysis. A key limitation of the study was the way data was to be modeled as collected. Largely due to its basis on structured social classes, the data could possibly be viewed strictly as opinion based rather than irrefutable mathematical data.

The use of modeling and simulation strategies ensured that as new technical models were created, there were use cases to employ it against a similar data set of legacy models (Lee & Zaidi, 2022). While this may only offer a snapshot of usefulness for an

‘as-it-stands today’ record, hopefully all of these use cases would further improve the predictability of the insider threat. One such recent study employed the use of game theory modeling to detect abnormal activity and extreme outliers. Per Joshi et al. (2021), employing a defend-attack-defend model using game theory for the insider threat attack, showed promise due to the added risk associated with insiders usually having a working knowledge of the internal defenses put in place within the organization. Key methods used in this study attempted to type-cast existing data sets used with previously used mathematical models, into the model for game theory. An element of interest when modelling scenarios for insider threat using game theory, was the implementation of cyber deception. By leading malicious actors down defense hardened paths during attacks, the security practitioner had an increased opportunity to gather valuable threat information and mitigate attacks before breaches could occur (Li et al. 2021). Deception technologies accounted for many success stories within the tech industry in recent years, and was responsible for the reduction of organization data breach costs by approximately 51%, and a 32% reduction in analysts cost for after action support (Huang & Zhu, 2021). As in previous studies, the insider threat data set from CMU was used, and an underlying assumption was that the data set provide a robustness to effectively observe data outliers within data sets with this modeling effort. The challenge with the use of game theory, was that increasingly large data sets were still limited by the design of attempting to identify a balanced equilibrium between participant data (Joshi et al., 2021). One potential limitation with this study was the baseline data availability used for user deviation detection during expected system usage conditions. The use of modeling and

simulations upon limited data sets could be deficient in terms of complexity, and when employed with less robust test data, the performance of the technique in question may not be fully evaluated properly (Nasir et al., 2021). It would be more practical and beneficial, and potentially more applicable to targeting abnormal outlier data, to attempt the same study against multiple data sets to better gauge an equilibrium within the findings of the study.

Another modeling study applied a framework against network data in order to better even out the malicious activity within the anomalous activity. This study used modeling methodologies against data sets that were situationally generated for fictitious group and user activities within a network. For the research conducted, it was an underlying assumption that the auto generated data would be relevant to tangible real-world user activity within a computer network. The framework improved the diversity of initial samples by approximating true anomalous behavior indicators and increasing data-sets to identify outliers (Yuan & Wu, 2021). An identified limitation of the study was the sole use of computer-generated data for the system, especially since it did not mention the specific level of detail within the logs, and it can be deduced that the logs were generic network activity an average system administrator would maintain, similar to the CMU data set. This led to further research opportunities for applying the same framework against known insider threat data sets. It also afforded opportunities to use a new insider threat data set as it comes along, to be used against other studies already mentioned in this analysis.

One study took a novel approach that employed a robust two-pass quantitative modeling solution against insider threat data sets, and offered a unique predictive solution, that made for compelling research. It centered upon the generation of a quantitative research framework to detect insider threat activity using multiple tools to improve results; specifically, the use of Bayesian networks and the MATLAB program to graph results offered noteworthy deliverables when implemented within a real-world scenario framework. By using risk as a quantitative measure, tipping points could be identified to increase the predictive ability of early identification of insider threat acts (Chen et al., 2016). This study used the data set from CMU with the expectation that the insider threat data set would have enough useable content for me to observe noticeable outliers of the data sets with the use of the model.

Another recent study incorporated a detailed review of the Insider Threat Detection and Prevention Protocol (ITDP), and further research into public cases of insider threat that could have benefitted from an ITDP adoption. Within the study, it was expected that the validity and usefulness of an ITDP implementation within a network infrastructure was acceptable to the reader. By incorporating statistical classifiers of user activity, an authenticity analysis could be performed to determine a credible threat (Sawatnatee & Prakancharoen, 2021). A potential limitation of the study could be the ‘forcing’ of a relatively simple tool, into other predictive areas of analysis more advanced than the capabilities of the tool itself.

The last modeling specific study in this analysis took an interesting approach to the insider threat perspective, as it focused strictly on the unintentional insider threat.

This was an often-overlooked aspect of insider threat. Within a survey polling recent incidents of insider threats in 2019, it was estimated that across 159 organizations, over 3,200 incidents took place, accumulating monetary damages approximating $8,800,000 per organization (Greitzer, Purl, Leong, & Sticha, 2019). The careless or cavalier actions of a trusted insider can be equally as damaging to an organization as a malicious insider. The focus of this study revolved around unintentional data-leakage and the incorporation of modeling simulations of human error tracking in order to predict unintentional insider threat activity. Per Abdelsadeq et al. (2019), a non-malicious insider could potentially do more damage than a threat actor, therefore a conceptual model targeting this type of incident is important. One underlying assumption was that the information collected from user data and work flows was substantial enough for a successful predictive model. One of the limitations regarding the study was the data collected that was to be modeled, mainly because it could inaccurately reflect the fields associated with a real-world mistaken insider threat incident. The study succeeded in providing new insight for countering insider threat as it targeted the non-malicious threat actor.

Other studies about insider threat research had put focus on the use of machine processing, specifically the use of neural networks to improve insider threat detection. One such study focused on deep neural network modeling and their usage for computational analysis of networking data logs. Natural language sequences could be coded to the data sets, in order to create natural language logic flows (Ma & Rastogi, 2020). As with other studies within this category, the CMU insider threat data set was also used, and shared many similar assumptions regarding whether the logs that were

used would be robust enough to observe noticeable outliers of the data sets within the model's use. Based on the popularity and efficiency of neural network processing, it was plausible that other types of source data could be used to replicate this study multiple times over.

The use of neural network models has gained attention recently for computational analysis of data sets, specifically, deep neural networks and recurrent neural networks. The CMU insider threat data set was once again the source of data, and it was assumed that this public insider threat data set would have enough detail to spot data outliers. The use of streaming techniques offered an analyst the ability to more rapidly profile anomalous data detection by potentially limitless data when fed into the deep neural network and recurrent neural network models (Tuor et al., 2017). The implementation of data streaming techniques for processing opened up interesting avenues for real-time analytics for insider threat predictions.

Another machine learning focused study provided new techniques to identify anomalies with the CMU insider threat data set. Machine learning for computational analysis of networking system logs was the focus of this study. By running the popular open-source data set through cutting edge machine language techniques, new workflows could be generated for analysis and improved alert reporting (Le et al., 2020). The research also incorporated an organization profile of employees to promote the ability to target possible threats. This enhancement of base-level data aided in improving results. The double-technique used would likely help with incorporating relevant findings and

compounding mitigation efforts into a multi-layered strategy for combating the insider threat.

By incorporating industry standard data science tools, such as Google's TensorFlow program, neural network studies could offer further improvement to the insider threat problem. TensorFlow could be trained to identify potential threats from multiple data formats, to include images, logs, etc., and the neural network algorithm used could aid in classifying malicious activity (Koutsouvelis et al., 2020). The advanced visualization software used by Google's TensorFlow project was assumed to be functional enough to identify abnormal activity. A noted limitation of the study was the baseline data availability for detecting user deviations from expected normal conditions, as it was narrowly focused upon networking data.

Another machine processing specific study pertained to the application of deep learning applied to insider threat network logs. The study used a singular computer-generated system data set, and could be a limitation compared to other studies. Per Yuan and Wu (2021), insider threat detection research pertaining to deep learning was not prevalent in recent literature, and future research could create new avenues of direction. The study opened new areas of thought due to its open-ended analysis of future avenues of research, this could lead the audience to think about new topics that may not have been previously considered for research.

Organizational Posturing

Another component that could be employed by network security managers for insider threat protection outside of the technical controls, was the behavioral aspect of

organizational employees. Organizational social psychology could aid in better applying security protocols for employees that may have a higher risk level than others for insider threat potential. Per Sticha and Axelrad (2016), instances of damaging insider threat activity could often be traced back to disgruntled employees that had negative or destructive opinions of their employer, and behaved in counterproductive manners to peers and projects. There was precursor indicative behavior that, if flagged prior to the incident, could have been responded to by the security managers relating to the level of access the individual had at the time.

Early identification of potentially malicious activity was one side of the coin for preventing damages from an insider threat incident. The other side of the coin was ensuring all efforts were made by network security personnel to eliminate this same potential within their realm of control. Per Carson (2017), employers that do not remove active credentials for ex-employees, made it easy for a disgruntled individual to gain access to organizational data that could have led to significant financial damages if leaked. Organizations without proper employee termination procedures to secure their proprietary information and limit network access to authorized individuals only, were not acting in a manner that promotes security within their internal mitigation processes. Monetary fines were often times associated with the leaking of personal information and they could fall squarely upon these organizations that do not perform a due diligence in securing their infrastructure.

An identified trend in the literature for the topic of insider threat was to rely heavily on psychological principles (Reid et al., 2017). Seminal authors in the field of

psychology were often referenced in current studies. For example, it was not uncommon to see references to psychology journals dating back 30 or more years (Stróż & Francuz, 2017). Another trend was the awareness of privacy concerns. Each source for this paper identified a need to understand and to make efforts not to encroach upon the rights of privacy for participants and organizational employees. This trend of privacy often tended to limit data collection efforts.

A commonly held assumption in the psychological field was that the delinquent activity of a trusted employee was often related to the ethical behavior of management or others in leadership roles (Cabana & Kaptein, 2021). For example, ethical leaders could be viewed as moral role models in an organization, promoting ethical conduct by setting ethical standards that subordinates could observe and emulate (Vianello et al., 2010). Another common assumption shared by researchers used in this analysis was that predictive algorithms could benefit towards mitigation of the threat. Experts in the field of neural networks and machine learning tended to agree that the usage of these technological advances could further improve the predictive modeling to achieve a higher detection rate (Fanzhi et al., 2018).

The primary area of contention within research of the insider threat, was the focus on behavior versus technology (Lin et al., 2021). Studies tended to take a stance either for a behavior-based approach or a rule-based approach to mitigate insider threat (Singh et al., 2019). Experts agreed that there were merits to both approaches, however the bias was easy to identify during literature research. These divergent perspectives led studies either towards or away from a psychology related route. Another divergence in recent

literature was the push to distance a study from current best practices. Experts often stated that the current landscape of anomaly detection was not useful. A recent example was the recent media leak from a National Security Agency Georgia contractor. It was not until after a Top-Secret document was already leaked to the press that analytics were able to identify the handful of employees who accessed it within a given time frame (Collins, 2017). Recent studies tended to either promote an improvement of current practices, or a revamping of these practices using cutting-edge advancements in technology.

As an accompaniment to organizational posturing to combat insider threat, researchers had experimented with employing socially grounded theories. Referenced in a few separate articles, the protection motivation theory, had been proposed as a tool for an organization's staff members. Initially predominant in the health care industry, protection motivation theory was well suited to gaining an understanding of security relating to employee contexts of obligation, awareness, and reward for organizational morality (Vrhovec & Mihelič, 2021). Per Greitzer, Purl, Leong, and Sticha (2019), organizational response to insider threat continued to be a challenge due to the level of employee and management resources required to effectively mitigate the problem. These elements of behavior could be used by organizational employees outside of the technical security realm, and leveraged by hiring managers and human resource staff during new hire screening. Per de Valk (2019), pre-screening criteria for insider threat potential can include personal gauges of an individual’s candidacy for increased risk. Areas of living, education, and social media publicized data, can aid in identifying red flags during

background investigations prior to employments. The focus of insider threat through a social or psychological perspective was a useful contrast to the technical IT related focus often used by network technicians and technical leaders. This type of problem-solving compliment can lead to a strengthened effort towards the insider threat problem space. While many technical solutions involved the analysis and identification of threats and vulnerabilities based upon system-generated data-sets (Jabbour & Jabbour, 2021), including non-technical behavioral approaches can add an extra dimension to the organizational posture. Changes in co-worker demeanor can often times be chalked up to temporary mood or situational considerations, and it can be difficult to decipher malicious intent from peers. Per Bell et al. (2019), after many situational reviews of insider threat incidents during the investigatory phase, it was often uncovered that colleagues who knew the perpetrator, noticed changes in behaviors before or during the insider attack was conducted. For an effective organization to properly combat the insider threat, it was important for all employees to be vigilant and to be wary of suspicious social changes. Per Rodbert (2020), employees primarily focused on security efforts, would be the ones who exhibited satisfaction and happiness in their duties. This behavioral indicator could be a measuring tool for senior management to leverage survey options for supervisors within the organization. A useful method identified within numerous journals, was the incorporation of employee surveys. Surveys have the ability to uncover bias in the workplace. Statistically, men were more likely to commit insider threat crimes within an organization, and these stats could lead to a gender-bias with regard to preventative measures in the workplace (Giddens et al., 2020). By targeting

biases relating to insider threat, new opportunities for success using employee surveys could improve organizational posturing. This refocused survey-based approach can identify areas of organizational security that may have been lacking due to oversight. In contrast to other survey related research, where the primary focus is on the prevention of insider threat, this research offered new ways to look at the problem by uncovering barriers to thought that may have been previously disregarded or unknown to security practitioners within an organization, and could lead to numerous points of failures in insider threat prevention.

An interesting blend of technical and social monitoring for increasing security posturing was incorporating a reviewing mechanism for employee social behaviors that leave a digital trail for collection (Dawood et al. 2023). Network login details and premises entry and exit logs can be a fundamental starting point for this level of monitoring. Per Mills et al. (2017), the analysis of employees' patterns of behavior can lead to the identification of suspicious activity based on seemingly normal data sets. For these types of organizational analysis, it was a critical precursor to identify what constitutes "normal" behavior regarding the logs in question. This form of implementation at the organizational level would require trusted agents to create legitimate baseline data sets. Research conducted indicated that employing this countermeasure would improve posturing against the inside threat problem. While this effort alone was an improvement, stacking similar sociotechnical methods was an interesting way to gain even more security benefit. Per Alsowail and Al-Shehari (2021), by stacking comparative security countermeasures into a multilayers of protection tiers;

such as employee vetting, access and privilege reviews, and awareness training at all employee levels, security practitioners can create a more informative and holistic picture of an employee's modeled behavior throughout their tenure of employment within the organization. Increasing layers of protection promoted a defense-in-depth or detection-in-depth strategy that has been shown to increase the probability of malicious activity detection, even if one of the companion layers of defense has been compromised (Schwab, 2021). There were numerous resources available to the security practitioner regarding understanding and using employee indicators for mitigating insider threats. Documented ontologies relating to socio-technical classifications can be a useful starting point for designing new internal mitigations and processes. Per Elifoglu et al. (2018), it was often thought that complex hacking tools are used to perpetrate insider threat incidents; however, case studies have shown that most incidents were consequential to human errors attributed to negligence, mistakes, and overly reckless actions.

Ontologies for cybersecurity and insider threat may be distinguished based on the types of constructs represented.

> Ontology frameworks focused on technical factors specify terminology and relationships that describe an attack event. For example, the Structured Threat Information Expression (STIX) ontology represented a wealth of knowledge on cybersecurity threats, by integrating technical ontology frameworks [e.g., Common Weakness Enumeration (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC)] (Greitzer, Lee, et al., 2019).

Flexibility for protecting against the insider threat is paramount with regard to the ever-changing challenges that new technologies and social changes can bring to organizations at any level (Kavak et al., 2021). Staffing competent security personnel can be as equally important as the mitigations put in place by the IT security department. The Covid-19 pandemic has introduced many new stumbling blocks for organizations that were not previously prepared for the boom in work-from-home scenarios. Per Chapman (2020), the insider threat problem has grown for security professionals working during Covid-19, due to the large number of remote employees connecting to corporate networks from personal devices, and the scenarios where these connections were conducted by individuals that may be deficient in training due to geographic separation. Security processes were likely to have been relaxed during these growing pain stages where organizations that were not prepared, had to ensure productivity and operational tempo were not impeded. Employee training was a large concern during these transitions to remote working. There has been an increase in Covid-19 related internet scams, and a recent study showed that websites relating to the coronavirus were 50% more likely to inject malware into the online session (Chapman, 2020). This is a major concern for remote employees that use company issued equipment, as they may be in a situation to not ensure the device is updated in a prompt manner by the on-site security team.

Another concept to be wary of from a management perspective is obtrusive scenarios as it relates to employee monitoring (Stafford, 2022). An interesting approach to this concern is to employ passive monitoring to employee communications. This negates the potential for employee uncomfortableness with more intrusive forms of

compliance monitoring. Per Tan et al. (2019), the incorporation of psycholinguistics as a monitoring tool can automate analysis of text-based interactions within an organization, to include sentiment analysis of email and text-based chat interactions. While a worthwhile tool if implemented correctly, it can be expected to produce percentages of false positives during early stages of implementation, and it would be important to staff personnel with the skillset and available work schedule necessary to properly tune the system to lower this percentage. A key component that can prove useful in proper tuning of a psycholinguistic passive monitoring system is the understanding of motivation and opportunity as it relates to an employee's potential to commit an insider threat incident. By assessing psychological and emotional states of trusted insiders within an organization, malicious conduct may be easier to identify prior to an incident (Tan et al., 2019). It can be a challenging effort to properly define and erect mitigations for the opportunities within an organization for a trusted insider to perform malicious acts. Per Safa et al. (2018), the act of limiting employee opportunities for malicious activity was directly corelated to the ability to discourage these acts within an organization. This can be a useful strategy for low level managers during performance evaluations. By better understanding performance elements and employee duties, opportunities for malicious actions could trimmed from the employee purview. This type of performance review can also be compounded with the issuance of a performance-based survey about subordinates. A recent research study performed injected scenario-based surveys when conducting performance reviews. This was a unique path towards measurable metrics, as it engaged the employees directly to aid in classifying potential performance-based attributes that

could predict an insider threat vulnerability. Performance based indicators were introduced into employee feedbacks, such as printing or sending large amounts of data outside the organization, and detectors were used against the indicators such as number of pages printed or volume of data sent outside the network (Brown et al., 2019). The employee reactions to the indicators can be gauged going forward to identify changes in performance patterns related to the conveyed indicators. This type of openness promoted an atmosphere that can limit the opportunities for malicious activity due to the employee's awareness of different monitoring tactics by security public relations actioners within the organization. It is important for the levels of leadership to be aware of changes to the organizational climate. Management practices deemed unfair by employees, such as layoffs, pay cuts, demotions, or delaying promotions, can be the catalyst that malicious employees used when justifying their criminal insider threat activities (Elifoglu et al., 2018).

An organization's ability to compound strategies and tactics to counter malicious employee activity can be often limited only by the aptitude and perseverance of the security team (Mtukushe et al., 2023). As mentioned in numerous modeling and simulation studies, the use of open-source insider threat data sets proved useful to a competent network security engineer. Per Chattopadhyay et al. (2018), there were many social triggers that had been identified as relating to an insider threat attack, such as personality conflicts, isolation, disgruntled, and have been documented as factors involved in malicious insider events. These events were prevalent in the open-source data sets, and proactive security practitioners can take internal strides to identify suspicious

activity from common logs. By incorporating encoded definitions of common log activity, an organizations IT department can apply the techniques to real-time network logs used within the company. This can further compliment a daily log analysis routine within an organization, and increase likelihoods of identifying malicious activity before it happens. The capability of automation further adds weight to this strategy, as network techs become familiar with outlier data within logs, automated detections can be coded to provide morning reports without wasted staff hours being required to continually process the daily data collections. In contrast, there can often be shortsighted impacts with regard to automation strategies. Per Saxena et al. (2020), automation challenges due to false alarms can result in unavailability of critical systems, this was especially problematic during periods where time-sensitive emergency situations can become a costly burden to an organization if employees are unable to access key systems. It is important for teams implementing automated security systems within an organization, to be cognizant of high-availability requirements for directly connected and adjacent critical systems, and to have time sensitive plans in place to reinstate systems taken offline or locked down from false positive events.

Closely related to reducing opportunities for malicious insider activity, deterrence was also a directly focused methodology in recent literature. Factors of deterrence are elements of an organization that increase the difficulty for employees to participate in certain activities (Bedford & van der Laan, 2021). A popular strategy within a social confine is the situational crime prevention (SCP) theory. Per Jeong and Zo (2021), elements of SCP that increased its chances of success within an organization included; a

reduction of anticipated rewards for the perpetrator, increasing the perception the risks involved, and increasing the perception for the level of effort to complete the malicious act. This theory has the benefit of easy adoption by numerous stakeholders within an organization, from the security practitioners, to senior management and all staff in between. It is strengthened by a shared stake and commitment to prevent malicious activity. The theory's primary goal was to paint an organizational picture of deterrence that the cons of insider threat perpetration far outweigh the pros. The social aspects of SCP can be conducted by a wide range of leaders with varied technical abilities, technical strategies such as encryption, incident management, and data destruction policies, can function under the SCP umbrella and compliment the overarching methodology (Padayachee, 2016). A recent study demonstrated that the perception of malicious activity was propagated within an organization under a veil of severe consequences coupled with intelligent design of deterrence mechanisms, which led to a high factor of influence from the SCP strategy (Safa et al., 2018). In contrast, it has also been identified within studies that employ an aggressive SCP strategy, that employee trust can be negatively impact within an organization. As companies enforce more restrictions upon employees in an effort to deter malicious activity, this can lead to damage of trust-based social dynamics as bilateral relationships are deemed as more authoritarian in nature (Jeong & Zo, 2021). This contrast highlights the need for rational judgment to be at the forefront within management circles and the issuers of policies relating to deterrence, as the focus of an organization to push potential insider threat actors to believe their plans would be unfeasible to attempt, it is equally as important not to alienate productive and

trusted team members. SCP implementations within an organization can establish known guidelines within a security policy, and also through stakeholder involvement, empower employees at all levels to properly prevent and even counteract malicious acts from within.

Designing new security methodologies for an organization's security improvements, has the benefit of group input regardless of specialty. Instilling an exhaustively detailed methodology for mitigating insider threat can be an effective tool, if an organization employed the proper personnel to ensure the level of granularity for security is accomplished. Per Nasir et al. (2021), key enabling criteria for insider threat success, were a user base lacking in awareness and training, an increase in technological complexities, and an increase in the number of users with elevated or unnecessary system access permissions. For an organization's employed methodology to promote good security, accountability for these enablers must be part of the methodology's foundation. Research into methodology design showed that identifying enablers early, can lead to stronger controls within a structured framework, and was important to understand that there exists a many-to-many relationship between security controls and insider threats; therefore, the implication was that other controls likely existed to mitigate a single insider threat vector (Roy et al., 2021).

From a reactionary standpoint, management actions and decisions must be considered when seeking to understand the social potential for insider threat acts with an organization. A recent study furthered the understanding of the relationship between management competence and employee policy acceptance. Per H. L. Kim et al. (2019),

management responses to crisis directly influenced employee behavior after a crisis, and research concluded that the perception of managers' capabilities influenced employee groups intention and willingness to comply with internal policies. This was likened to a lack of confidence in leadership leading to a difficulty in the retention of valued employees. When IT leaders institute security policies, it is imperative that they do so in a competent manner that conveys a betterment to the organization. One strategy for conveying competence is to continuously strive to improve an organizations security posturing to keep up with new threats. It is not efficient to secure an organization with a one-time setup that is left alone afterwards. Per Schwab (2021), security countermeasures that were installed and not routinely revisited and updated for relevancy, remained in a static state, while active threats to those countermeasures and systems as a whole continued to evolve and open up new threat paths. Perceptive leaders within an organization can contribute to employee social indicators for insider threat by elevating their attention to behaviors during policy changes or instantiations. It has been established that key behavioral traits were important to measure when regarding insider threat, as they had been directly linked to documented malicious activity within corporations; these behavioral traits include risk taking, self-centeredness, and arrogance (Saxena et al., 2020).

Routine system use of employees can provide a valid measurable indicator of outlier detection within a network. In a recent study, business processes with a networked system were logged for timestamps and usage. Due to the regularity and predictability of standard system use, a threshold was easily identified, that provided management with a

reliable indication mechanism to detect outlier data, such as abnormal user login and out of band timestamps for usage (Oh et al., 2019). This level of design can be common among junior network security technicians, and does not usually involve the heavy mathematical aptitude that research identified in the models and simulation section may require. There were also many online resources to aid a security team in scaffolding a new implementation of a similar or complimenting design within their organization in a rapid fashion.

Different cultures can often have different outcomes to the similar organizational strategies (Whitty, 2021). An interesting study performed in Korea focused on deterrence factors for poor security practices by increasing employee punishment for malicious behavior. Specifically with regard to phishing and the unintentional insider threat risk. Per B. Kim et al. (2020), research concluded that employee punishment was a successful deterrent for compliance with organizational policies for countering phishing attacks, however it was identified that the higher an employee's position, the more likely they were to be victims of phishing, regardless of punishment or increased training. In contrast to this punishment focused deterrence research, in Russia, a recent study focused on the aspect of positive psychological reinforcement of the work environment (Lewis et al., 2017). Positive psychology can be a useful strategy for not only enforcing compliance, by identifying non-compliance, through monitoring of employee performance of protective behaviors, and focusing efforts to improve what is working correctly versus focusing efforts upon what is deficient during performance analysis (Zaitsev & Malyuk, 2016). This positive strategy can lead to breakthroughs in areas where compliance has been

difficult to properly enforce, regardless of training or admonishment. It would prove interesting to apply these types geographically specific studies upon different nation states that have radically differing social norms within their respective geographic cultures.

Conceptual Framework

TQM has been around for many decades, dating back to the 1950's, and still to this day, has the backing and implementation of respected organizations worldwide (Tahira et al., 2020). Customer based businesses have long benefitted from its focus on improving internal performance, producing higher-quality products, and increasing customer satisfaction (Benzaquen et al., 2021). TQM has seen practical application for nearly 70 years, and has seen increase in interest within the scientific community since the 1990s (van Kemenade, 2022). The main tie-in for TQM for application of an insider threat strategy, was the employees banding together as a team to prevent a negative impact to their organization's brand. From a top-down perspective, TQM can be thought of as a management system focusing on all aspects of improving quality (Paraschivescu, 2020). When customers lose faith in an organization due to a failure in security, that translates to a potential loss of future revenue. In terms of IT systems, one of the most useful elements of a properly instituted TQM framework, was a reduction in redundant efforts (Putri et al., 2017). Within IT security establishments, streamlining processes is a must for highly efficient teaming. By embracing the core principles of TQM: leadership commitment, continuous improvement, employee education and training, and customer satisfaction, each tier of the organizational hierarchy can help in elevating each other

(Khalfallah et al., 2022). With the amount of media attention that insider threat incidents garner in today's security-conscience climate, loss of public trust can ruin an organization financially. Implementations of TQM today can be thought of as an overarching corporate focus targeting customer satisfaction (Dubey et al., 2018). It is not uncommon to see organizations today with a chief information officer who reports directly under a chief information security officer. This demonstrated a commitment to information security, and illustrates a focus on customer trust. TQM in practice was susceptible to successes and failures similar to other adoptions of improvement methodologies. Successful implementation of TQM often stems from a complete immersion in the methodology. A common factor in TQM failures, lied in the level of implementation. Failures are often identified in organizations that do not commit to a complete implementation, this less than full commitment illustrated a rejection of TQM (Campos et al., 2022). Limitations in TQM adoption can usually be identified by stakeholder readiness to assess their own weaknesses in an effort to improve the organization as a whole (Egwunatum et al., 2022).

Transition and Summary

After extensive research into the topic of insider threat, it was clear that there were a few specific areas that could benefit from further research. Most of the existing research over the last half-decade revolved around methods to improve detection of a potential insider threat incident. While this was a critical piece to insider threat mitigation, it was often limited by the status of existing insider threat mitigation employed throughout today’s organizations. One topic that would prove beneficial for

further research would be to dive deeper into the U.S. Government processes and procedures for mitigating insider threat incidents. Within recent years, the most high-profile insider threat incidents have been top-secret government related. This would be a worthwhile target of further research, especially if these high-profile data leaks led to loss of life for government employees.

Another identified key element within recent literature reviews that has been overlooked, was the current landscape. An argument for further research could be made for; what are the current strategies employed by organizations, of various sizes, to counter the insider threat from within? While most non-quantitative research revolved around case-study reviews of previous noteworthy incidents, there was minimal research regarding the current status of insider threat organizational risk management.

A vital new step in improving an IT organization's posturing against the insider threat, could be to better understand the current landscape. A qualitative study into existing efforts could provide insight into a current 'snapshot' of processes and procedures that have been adopted, and why. This opens up many new potential studies, especially as focus could be target towards small, medium, and large sized organizations. As well as local, regional and global reaching organizations.

Section 2: The Project

In this section, I explored my role as the researcher and the data collection process I used to perform this doctoral study. Participants and their role in the research method were clearly defined, and the population and sampling of data were also addressed. I discussed the ethical procedures I followed, and I detailed the data analysis to illuminate reliability and validity of the study.

Purpose Statement

The purpose of this qualitative multiple-case study was to identify the strategies used by IT security managers to protect their organizations against insider threats. The population for this study were IT security managers in the private sector and U.S. government facilities in the continental United States. Contacts made during the last 5 years of employment who shared an interest in preventing insider threat were invited to participate in this study. The contribution to social change may be the potential limiting of negative impacts to internal systems from an insider threat, including unauthorized disclosure of classified data and loss of proprietary information. These acts can cause irreparable damage to an organization public reputation, as well as the potential for the loss of life within classified information mission domains (BaMaung et al., 2018).

Role of the Researcher

A researcher undertaking a doctoral study can occupy numerous roles throughout the study's lifecycle. My primary role in this study encompassed data collection and analysis. It was important to maintain an impartial role with regard to bias during every phase of the doctoral study. Castelló et al. (2021) observed that, without a targeted focus

on preventing bias during concept writing, the researcher's experiences can be apparent in the documentation.

A researcher with many of years of IT professional experience within technical and management duties must consistently be wary of biases within the research process. In conducting this study, it was crucial that I not interject any of my areas of expertise into data collection and analysis activities. During data collection, I did not engage in technical discussions that might sway participants to respond in any way other than organically, based on their position or experience. I have been a network security professional in the IT industry for over 20 years. I have worked in numerous positions where insider threat detection and mitigation were a core duty. I have performed these efforts within the U.S. government and within the private sector.

Prior to researcher interactions, it was important to accept that biases are ever-present and that cognitive efforts be made to address them in a manner that did not interfere with the goal of collecting data through the interview process. According to Enemchukwu (2022), every individual exposed to society, social media, film, and television has been socialized to develop biases on a broad spectrum of exposed topics. It was important to pay attention to physical reactions during the interview to not project bias or opinion upon the interviewee. Unconscious bias is a biological brain response to recognize patterns and conserve energy to promote physical safety (Slaughter & Ahn, 2021). It is critical that a researcher be well versed in the topic of the interview, not display emotional reactions to any participants reactions, or offer input during the interview. These actions can lead to potential barriers to further clarifications or

participation. Winkel (2019) emphasized the importance for the researcher to identify the personal lens with which their own experiences can leverage insight to improve communication during the interview process. Proper understanding of personal bias can help in the design of an effective interview protocol. The use of an interview protocol can aid in aligning the process with the optimal data collection outcome of the communication. The use of an interview protocol during qualitative data collection can improve the reliability of the data, as well as increase interview effectiveness for adhering to allotted times (May et al., 2018). Identifying time constraints per proposed interview question may ensure that the qualitative data collection is complete.

The safety of all study participants is also a primary role of a researcher. I constantly referred to the *Belmont Report* during the research process. This report offered a framework for ensuring respect for persons and heeding ethical codes (see Redman & Caplan, 2021). Any failure to comply with confidentiality must be identified and adequately addressed according to the standards expected by the participants and Walden University. The researcher's role also aligns with the expected ethical considerations promoted by Walden University. As the researcher, I was bound by personal and professional ethical standards that I needed to uphold throughout this study's lifecycle. Interviews and information gathering sessions needed to align with ethical standards at all times.

Participants

The target population for this study included civilian and contractor network professionals within the U.S. government as well as technical leaders and security

process implementation officers within the private sector. A key distinction for the technical leaders was that the group included junior and senior-level employees. The geographic location of the interviewees was centered on U.S. military locations throughout the continental United States and on Silicon Valley private sector organizations. I leveraged existing contacts of mine I made over the last 5 years as primary participants. I expected that further participants would be identified during the introductory contact phase for the initial participants. This population was appropriate to the study due to their firsthand dealings with insider threat mitigations in their organization. It was expected that existing contacts would branch out to identify like-minded peers who shared an interest in improving their networks against the insider threat. Homoliak et al. (2019) noted that the insider threat problem can be addressed more effectively by conducting interviews with technical professionals who are actively promoting a solution to the problem within their organization's infrastructure and operating framework.

Research Method and Design

Method

The research method chosen for this doctoral study was the qualitative method, mainly due to the decision to employ a case study design centered around participant interviews. A major benefit in employing a qualitative design was that the data captured during an interview could enhance descriptions of experiences from participants in a straight forward and focused manner (Asmaningrum & Tsai, 2018). I initially considered using a quantitative and mixed-methods approach for this research but opted against

using them. I identified numerous insider threat literature used in this study from the Walden Library resource that featured the use of the qualitative method. The interview methodology has often been viewed as a pillar of an in-depth qualitative process (Hughes et al., 2020). Conversely, the quantitative approach has largely been seen in research conducted with less reliance on the interview process. Yığ (2022) stated that the use of the quantitative methodology was generally present in research relying on mathematics and numerical content analysis to garner results. The use of large data sets, however, can increase data collection and analysis times (King & Huang, 2023). As such, I opted against the use of a quantitative method. The mixed-methods approach was also discounted for this study, due to the lack of reasons for using a quantitative approach. The mixed-methods approach intertwined quantitative and qualitative methods during a study (Mikalef et al., 2019). I found it unnecessary to use a quantitative approach, which meant, by extension, that a mixed-methods approach was not appropriate.

Research Design

I selected a case study design for this study because of its wide range of data collection possibilities. These included in person, survey, telephonic, or correspondence collection methods. When incorporated into an interactive framework, interviews conducted on peers can become a vital component of the research process (Devotta et al., 2016). One design approach ruled out for this study was an ethnographic design. Because ethnographic research involved participating in the actual environment of the study, the time away from writing and research can be tremendous (Parkin, 2017). Another design approach not selected for this study was phenomenological. For an insider threat study, a

phenomenological approach would entail participants who were affected firsthand by the threat, and given company reputation safeguarding, employees would be less likely to divulge relevant details (Ho, Kaarst, et al., 2018). Employing a phenomenological approach involves delving into the particulars of the cases in an effort to gain insight into a personal perspective of the context and to identify how the participant makes sense of the phenomenon (Cuthbertson et al., 2020). By further examining documented insider threat cases, new mitigation strategies can be identified.

Population and Sampling

The primary criteria for selecting participants were their ability to effect change within an organization with regard to insider threat prevention and protection. The targeted population for this study included network security professionals in implementing insider threat mitigations within government and private sector businesses within the continental United States. The technical background and experiences of the sample population was a key consideration to ensure successful qualitative research that produces findings that are representative (Ellis, 2020). A sample size of five participants was acceptable to gain insight into the varying techniques used by organizations of different sizes to counter the insider threat problem. Data saturation was achieved when all of the predefined codes were identified from the interview transcripts. The qualitative sampling attained theoretical saturation after all of the research codes had been observed at least once (van Rijnsoever, 2017).

Ethical Research

There were a number of ethical considerations when undertaking a study that involved interactions with members of the public. One example of an ethical challenge was to ensure integrity in the research process and that it is free from bias. I needed to ensure that in all communications during the study I refrained from personal bias. The introduction of bias could inadvertently influence participant responses. An example was Edward Snowden, the National Security Agency analyst who leaked over 50,000 classified documents in 2013 (Wescott, 2020); most people are on one side or the other with regard to his character and actions (Gioe & Hatfield, 2021). Referencing him in a positive or negative light could frame an interview question in a way that could interfere with the respondent's true position on the subject. I strove to use unbiased and appropriate language in participant interactions during the research process.

A key element of ethical research is informed consent (Godskesen et al., 2023). Each participant was issued a consent form to sign prior to involvement in the study. This consent form documented the ethical protection guidelines as they applied to each participant. Specifically, their right to confidentiality with regard to the published study. Participation in this study was voluntary, and participants were free to disengage at any time if uncomfortable with any facet of the study. As a researcher, care was taken to assuage any personal issues to not interfere with maximum participation. Each step for security of participation and data collection was identified in the consent form. The following items were addressed:

- All collected data in a digital medium was encrypted when stored. They were stored on DVD and external hard drives for a period no less than five years. They were housed in a personal safe.
- No identifying information regarding participants was left unattended at any time.
- All findings and final aspects of the study were made available to all participants.

Each participant was selected based on their positions within IT organizations, directly in tune with the positive outcome of this study. Each participant had an opportunity to better fortify their IT landscape based on maximum participation of this study.

Another ethical example was the protection of participants. In preparation for the study, I produced signed consent forms for all participants. These forms ensured participants were aware of their rights with regard to their responses, and the use of their responses going forward (Creswell & Creswell, 2018). This was especially important when anonymity concerns were attributed to data that an employer may seek reprisal for a participant's response. The underlying ethical value for a scholarly study was the authenticity of the collected data, and the protection of all participants involved. I obtained approval from Walden University's Institutional Review Board before conducting the study (approval no. 03-20-24-0986343).

Data Collection

Instruments

Instruments used for data collection were centered around recorded interviews. The use of video teleconferencing programs, such as Apple Facetime, Skype, or Zoom, aided in overcoming geographic separation of participants, as well as social distancing concerns in light of the Covid-19 pandemic. I used a smartphone to record the audio (not video) of interviews. Paper interview responses were also available for participants adverse to the two options for data collection. Internal validity was enhanced throughout the data collection process. Each interview was transcribed digitally and participant's technical employment was scrutinized to ensure their skillsets fell into the desired information security realm. Transcripts of interviews were reviewed in real time along with interview playback, to ensure complete accuracy in the digital record.

Data Collection Technique

Interviews were employed for collecting data during the research process. Semi-structured participant interviews were the primary tactic; however, accommodations were made available for any participant wishing other methods of information sharing. Video interviews were requested, and audio-only interviews was the second choice. Per Creswell and Poth (2018), analysis of collected data could be limited when it did not include verbal and non-verbal cues. By gaining real-time feedback from a participant's non-verbal clues, potential pivot points during the interview were used to gain further insight into the security strategies used to mitigate insider threat. This was an advantage for robust data collection, because non-verbal factors and steering the interview based on

immediate feedback could lead to more targeted information (C. Liu et al., 2016). A disadvantage of semi-structured interviews, was the time required and logistics of scheduling multiple participants in a conducive manor (Edmunds, 2017). Reacting to scheduling conflicts or unavailability for participants to engage in a semi-structured interview, the option for completing a survey of interview questions was made available. The primary data collection technique consisted of participant interviews.

Data Organization Techniques

It was expected that collected data would be organized in a manner conducive to answering the research question. Per Probst (2015), a recursive relationship can become evident during a researcher's interviews, as responses from participants can impact the dynamics of the qualitative study, and uncover interdependencies between research design and data collection. A qualitative study had a recursive relationship between the research design and data collection when there was a strong connection to the research question. If the research question influenced the research design, and the data collection is relative to the research question, then a recursive relationship can be established.

The primary means of data collection consisted of audio/visual recordings of interviews. Videoconferencing software was the preferred medium, with the participants choosing which software solution (e.g., Skype, Zoom, etc.) they were most comfortable using. As data were collected and organized, there was the potential for me to change my thought processes based on receipt of new information. I maintained a reflective journal throughout the data collection and analysis phase, in an effort to understand and document any personal and professional growth in the areas of insider threat. By gaining

new understandings along the way, it was possible that cataloging of data sets may be altered in ways not identified prior to analysis. Cataloging and securing of collected data was an important aspect of the research process. Using the Walden University guidelines as a reference, I intended to use an encrypting scheme for all data at rest. Any digital items stored were encrypted with a 512 AES (Advanced Encryption Standard). A disposal plan for all collected data was discussed with participants that have any concerns regarding the topic and delineated at the time of interview conclusions.

Data Analysis Technique

During the literature review for the topic of insider threat, data points became apparent that I could potentially use during my research to identify codes and themes for data analysis. Upon completion of participant interviews, an in-text coding section was added to apply codes to the interview transcript. The themes were minimizing risk, threat type, and system monitoring. The codes were as follows:

- training (minimizing risk),
- employee agreements (minimizing risk),
- intentional (threat type),
- unintentional (threat type),
- authentication methods (system monitoring),
- logging (system monitoring), and
- decentralized security (system monitoring).

The approach to develop codes and themes during data analysis involved reading and documenting emergent ideas. Creswell and Poth (2018) suggested that a researcher

become fully immersed in the contents of an interview, by rereading the transcript several times, in order to gain a broad sense of its content prior to disassembling it into smaller parts. Participant interviews were read multiple times to make note of terms that were often repeated. I employed Linux shell scripting to a text copy of the interviews. Each interview transcript was filtered into three separate documents. The first document displayed each word on a single line, the second document displayed each word and the next word on a single line, and the third document displayed each word and the previous word on a single line. This allowed for sorting and numbering uniqueness commands to identify and rank repeated terms. The resulting sorted and ranked files were compared to my initial documentation of the interviews. It was expected that each of the codes and themes would be present, or generally described in the higher ranked portion of the sorted output files. Additional codes may be uncovered during this file analysis. Triangulation was then used on the separate data sources. The triangulation method for data analysis can aid the researcher in minimizing bias (Shin et al., 2022). Codes and themes were deciphered from the interviews, transcripts, and notes taken from each interaction. Identified themes were sorted via weighted scores for their amount of related data from the combined interviews. This score was defined by the amount of translated text per theme, and amount of context each theme was referred to by individual participants. A second pass was performed on the themes to identify commonalities for theme groupings. This second pass narrowed the themes to down five used in this study.

By employing a tight focus and direct route for analysis codes and themes, an acceptable justification can be made for efficacy (Brooks et al., 2023). As this study

revolved around analyzing participant interviews, it was imperative that codes and themes within the data set were identified early in the analysis process to reduce the potential of unforeseen errors. By identifying security and ethical standards early in this study, a successful adherence to the Walden University guidelines for data retention could be accomplished

Reliability and Validity

Reliability

To ensure quality and reliability of qualitative data collected, it was important to employ a focus on participants' meanings (Ridge et al. 2023). By targeting the specific meaning a participant conveys about a problem, as opposed to the researcher perspective that is brought into the fold through bias or literature (Creswell & Creswell, 2018), a more rooted data set was obtained. To produce a more reliable analysis, a methodological triangulation of data points can be conducted upon each interview participant individually (Ofori-Duodu, 2019). Each conducted interview, was transcribed and provided to the interviewee to ensure all collected data reflected their input accurately. This transcript reviews improved reliability by confirming the intended data interpretation. To promote efficiency, the data was analyzed within the purview of potentially answering the research question. By conducting an iterative and continuous analysis of the collected data, reliability in the findings was increased with regard to answering the research question. In order to ensure effective data saturation of the collected information, follow-up interviews were agreed upon by participants when further details emerged that required more data collection.

Validity

Validity of the data collected and analyzed within a doctoral study can add significant weight to the usefulness of the study for the future. Various design tools and software visualization tools were expected to be used to promote this validity. Per Creswell and Poth (2018), computer programs contain many features for analysis to visualize codes and themes and their interrelationships. By identifying codes and themes early in the analysis process, an early determination was made whether the collected data was sufficient for concrete validity.

Transferability was an often-pursued attribute of this research. Transferability refers to the potential for the qualitative research to be transferred to other contexts and settings (Tuval-Mashiach, 2021). During the course of literature review, psychological studies, with research far from the technical realm, have touched on the insider threat from a social perspective. The results of this research, although based in a technical construct, was expected to be applicable to non-technical research related to the insider threat problem.

Transition and Summary

With the conclusion of Section 2 for this study, the purpose statement and the role of the researcher was defined. The participants, the research method and design, and the population and sampling have been identified. Per the Walden University doctoral guidance, procedures for ethical research, data collection, and instruments have been accounted for. Also, techniques for data collection, data organization, and data analysis have been defined. Finally, reliability and validity for the elements of the study have been

itemized. Section 3 includes the application of professional practice, and the implications for change identified in the research data collection.

Section 3: Application to Professional Practice and Implications for Change

In this section, I presented the findings of this qualitative study. Each interview conducted with participants took place over the telephone and was recorded with the participant's permission. I asked interview questions pertaining to the research question, which was, what strategies do IT security managers use to protect their organizations against insider threats? I asked three additional questions based on initial responses, which were, are their strategies effective, how do they measure success of these strategies, and what strategies could be revamped with newer technologies to better perform insider threat detection? Data saturation expectations were met for each participant, and the themes presented are the result of this saturation. Each conducted interview was transcribed and, as part of the member checking process that I used, provided to the participants for their review to ensure proper context and clarity in their responses.

Overview of Study

The core purpose of this qualitative study was to identify strategies used by IT security managers to protect their organizations against insider threats. This was accomplished by conducting semi-structured interviews with participants in the IT security field, specifically with current and relevant insider threat experience. The presentation of findings included themes that were identified during the data analysis phase of this study.

During the proposal stage of this study, I had originally planned to interview at least 10 participants to achieve enough data to reach saturation. However, the first three

interviews were professionals with robust experience combatting the insider threat. The themes identified in this section manifested clearly during those first three interviews. I continued with two more interviews, and it became evident that I had reached data saturation at a level high enough to effectively complete the data collection phase. This alteration from the original plan was communicated to my committee chair and cochair, and approval was granted to cease collection after the fifth interview was successfully completed.

Presentation of the Findings

The participation in this study was kept confidential, and the five participant responses in the findings of this study were referred to with their respective codenames. Table 1 includes participants' codenames, job titles, and interview dates.

Table 1

Participant Job Titles and Interview Dates

Participant	Codename	Job title	Interview date
Participant 1	PI	Chief information security officer	April 29, 2023
Participant 2	P2	Network security manager	May 13, 2023
Participant 3	P3	Chief information security officer	May 27, 2023
Participant 4	P4	Information security manager	May 28, 2023
Participant 5	P5	Chief information officer	June 17, 2023

Theme 1: Risk Acceptance/Risk Tolerance

As observed during the literature review, the topic of risk was the most prevalent theme present with regard to insider threat research. This further supported the findings during the interview process for this study, as each participant confirmed that risk was the primary factor driving every aspect of their implemented insider threat strategies. A key

component in understanding risk within the confines of an organization is to accept that there are often multiple factors associated with identifying and ranking risk levels (Bada & Chua, 2021). P3 noted,

> when it comes to thinking about how to protect against insider threats, the first thing you have to start with is understanding what the most important assets you have, what are your crown jewels, what are the things that need protection the most. From an insider threat perspective, you're probably going to have a hard time trying to protect all of the things all of the time, so you have to really figure out what are the most important things to your organization.

With regard to government facilities, it was common to focus on the protection of classified information, but there were many other areas of concern when thinking about insider threat (Alhajjar & Bradley, 2022). These facilities can have areas of concern outside of the realm of technical security, specifically physical security. There was an expectation of a level of risk tolerance associated with these scenarios, as multiple organizations may require accesses. A good example were the locations that house networking infrastructure equipment. The locations of routers and switches that form the backbone of an internal network tend to be locked in communications closets within many disparate facilities. Each of these employ heating, ventilation, and air-conditioning and fire suppression systems that may be maintained by employees outside of network security technicians.

Cataloging all notable risks within an organization is a useful strategy for proper insider threat mitigation. P3 commented that a common strategy in the private sector for

insider threat prevention efforts is the creation of a risk register. Smidt et al. (2022) noted that the use of a risk register can be a critical tool for achieving strategic objectives, assessing performance, and managing risk within an organization. The use of a risk register can afford an organization a baseline for identifying critical systems and data that can grow and shrink as needed over time.

Within government organizations, insider threat risk was often associated with control over classified documents and information leakage (Darnton, 2022). Due to the increased severity tied to disclosing classified information, it can often difficult for leadership to commit to an acceptable tolerable risk. As a prior military network security analyst, I can confirm that every commander I have worked under had a zero tolerance for leaking classified information. Due to the nature of the information to be protected, it was unlikely for military leaders to formerly document a risk acceptance. P4 stated,

> If you look at the fallout from the Snowden leaks, the NSA [National Security Agency] director at the time publicly offered to resign over the incident. There was overwhelming support from the U.S. government for him not to do so, as it didn't appear to be helpful in fixing the problem. It is interesting however that the Commander of the facility where Snowden worked, quietly resigned shortly after. From a career standpoint, this furthers the position of risk intolerance for insider threat activity. If a career officer with an impeccable record can have their career derailed prior to making Admiral, this is going to leave a lasting mark on all the junior leaders seeing how impactful an insider threat incident can be for those in the upper chains of command.

Government organizations tend to have tighter control over the procedures in place to combat insider threat incidents. A common strategy was to employ signed acknowledgements relating to safeguarding classified information. P2 described this level of influence as being less controlled in the private sector. This was often due to the span of geographic locations under an organization's purview. Another factor was the more stringent privacy laws associated with these disparate locations. P1 noted,

> There were buildings where we shared a floor with another company. You had to walk out of your office, then badge in to use the bathroom. There was a badge swipe to get into a lactation room for female employees. And because of that we were not allowed to collect badge in/out information for that building. Then we had other offices with no badges. The operating environment was so diverse, the risk tolerance was dictated by the environment we were in.

The failure to mitigate insider threat activity can have a negative impact on an organization's financial posture. A key element that ties risk to TQM was the focus on ensuring all employees strive for an optimal state of performance. An acceptable risk strategy within an organization that employs TQM had a higher chance of approval from internal leadership. According to Lepistö et al. (2022a), risk acceptance using a TQM framework encouraged organizational buy-in by encompassing elements from aspects relating to system deployment, managing risk, and stakeholder management, to efficiently reduce risks to products and operations. A primary goal of TQM is a transparency of compliance within the confines of the relationship between the customer and the organization. A solidified TQM deployment within a trusted organization clearly

identified events and procedures defined in an organizations risk plan and shares the magnitude of associated failures with the customer (Pellegrino et al., 2020).

Theme 2: Operating Environment Limitations

Limitations in the operating environment were a key component in defining risk exposure. Themes 1 and 2 complemented each other, in that they were interwoven and helped in illuminating areas of concern with regard to mitigating insider threat. Varying privacy policies can severely limit the insider threat capabilities from an investigative perspective (Li et al., 2021). These limitations due to policy can be seen in regulatory restrictions that are imposed by countries where organizations expand into. In 2018, Europe instituted a new data protection policy: GDPR. This data focused initiative placed tight controls related to data sets that were personally identifiable, and applied to organizations that track or provided data services relating to European subjects, even if they were not located in Europe (Bonatti et al., 2020). This can cause problems when analytics are triggered based on activity, that fall under this policy. P1 stated, “our analytics went off and I couldn’t query it because it’s a violation of privacy, so, you can’t talk insider threat without talking privacy and regulatory environments because you just legitimately cannot do insider threat in certain countries.” These policies protecting user data can have a negative impact against organization’s that are non-compliant. In 2020, Barclay’s bank was fined $1,000,000,000 for a keystroke logging security effort that was deemed in violation of GDPR (Ennis, 2020).

Within the government, limitations are much less stringent when compared to the private sector. P4 stated,

> performing insider threat detections and monitoring at a government building is surprisingly limitless. Every machine has reminder stickers that state: any usage of this device is subject to monitoring. Network security technicians, with the proper credentials, are allowed to login as a targeted employees and view profile activity and histories. Where this gets harder to do, are systems that require increased access permissions. Fewer technicians are approved to control these systems, and issues that crop up during investigations may stall when those technicians are unavailable due to illness or leave statuses. These limitations can be further exacerbated during minimum manning situations due to exercises or Covid.

Limitations in an operating environment were not only attributed to regional policy constraints. Many factors can limit the abilities of an organization to competently enact a successful insider threat strategy, to include operational budgets, staffing, and technical proficiencies. P4 & P5 identified organizational funding as a key component attributable to a successful insider threat mitigation program. Within the government sector, sometimes, the displacement of competent personnel can lead to a shortfall in staffing. When high performing individuals are tasked elsewhere, funding becomes an issue, because you are unable to hire against employee billets for personnel that are tasked for remote military deployments. P2 noted,

> there was 1 year where our staff had an unusually high personnel turnover. This is common in the government, and you don’t have much say in the replacements that are assigned to you, so you have to work with what you got. I had this stellar

> NCO [non-commissioned officer] who specialized in ML [machine learning], and wanted to employ a sentiment analysis model in a data lake using collected chat records and emails. After going through the hoops for funding and getting his proposal approved, he was tasked to deploy for a year. This was an "all eggs in one basket situation", and the project was shelved until his return due to the disinterest/aptitude of the remaining technicians.

Understanding imposed limitations on an implemented strategy was important for achieving TQM. This in-depth understanding of where gaps in security and protocols may exist, can help drive new innovations towards effectively addressing these gaps. A successful TQM implementation enforces a detailed understanding of all organizational elements related to process functionality to ensure proper operational security (Nazir et al., 2023). Limitations to an organization's operating environment must be documented thoroughly for a proper TQM implementation. While this may seem like it opened doors for a less than optimal product offering to its customers, it can lead to a level of trust that is a cornerstone of the TQM principle. Per Acquah et al., (2023), TQM must be adopted extensively to all organizational sectors, as past implementations have proven organizational benefits in the form of sustained competitive advantages through product quality, profitability, and customer satisfaction.

Theme 3: Employee Profiling

An important piece of an organization's insider threat program, was to identify employee positions and permissions (Prentice, 2021). When profiling employees, it was useful to categorize each one by the potential levels of threat they can pose. Categories

included identifying those with elevated permissions, such as administrators. It was important to employ varying levels of scrutiny against employees with different levels of access. This included access levels and access types. By employing an employee profiling strategy, P1 noted,

> what we would do is we'd say that this user did it on all of these rules and detections. this window of time, and these different rules were weighted. So, what we did is we took high, medium, low, and we just weighted them 3, 2, 1. And then we added them up to see who had the highest score. And we're like, that's how we ranked it. That was it. So, it's like that aggregate over time is the way to do it.

Promoting a synergy with human resources, in an effort to become better in tune with employee behavior, was a worthwhile strategy to improve insider threat predictability and response (Moore et al., 2018). Within the confines of the government sector, there can be much less separation between personal performance of duties and direct supervisory involvement regarding under-performance of these duties. Supervision of subordinates is handled at the lowest levels, and there was often full transparency of an employee's profile among varying echelons of leadership. P4 stated,

> in the military, dealing with behavior that is commonly associated with insider threat precursors, is much different than in the private sector. Low-level supervisors spend many hours in PME [professional military education] focusing on correcting derelict behavior. There tends to be a level of isolation mixed with defiance observed in employees leading up to classified document theft and leaks.

> This behavior indicator is being integrated into junior PME courses, so our leaders can try to get in front of the problem at the lowest level of supervision.

A key component of understanding the threat vectors associated with a potential insider threat within an organization was identifying who has access to what. P3 stated,

> insider threat, since those are employees, becomes one of the top issues of a CISO these days, making sure that your internal people aren't exposing you. At the end of the day there are probably two main threat vectors. Either you're an insider threat as an employee who clicks on a link or shares information externally, or you've got third party integrations. Whether it's a cloud solution or a third-party solution that has some kind of access to the organization, or some kind of access to facility system networks to help people to work, or temporarily help people to do work. Those two vectors end up leading to the most exposure to data and issues.

By ensuring the employees that fall into these two categories were identified and updated regularly within an employed risk register, leadership was better equipped to promote a successful insider threat strategy. Employing software tools to manage employee profiles can also significantly help with the expanding scope of potential threats. P5 stated,

> in the navy, we adopted a permission management software, that publicly shares accesses assign to every employee. From a security standpoint, this allows ISSOs [information system security officers] to monitor and control approved system accesses by granting the required access permissions to those who have a need to

know. This strategy also allows other employees to check the accesses of individuals prior to sending emails to those individuals that may not be cleared to receive classified materials they are not approved for.

Employee profiling is a useful tool in pursuit of TQM. Collected metrics on employee activity can be a great indicator for potential security issues. Deviations in routines can be a warning sign that, while employees within an organization may personally strive for excellence in their duties, automated data collection can help fill in the gap of substandard performances that may lead to an unintentional insider threat incident. Promoting a culture of ensuring employees are granted the least number of accesses and privileges to perform their duties is important when looking at insider threat through a TQM lens. By enacting employee profiles, TQM studies have shown a direct correlation between employee job satisfaction and transparency of performance, promoting a culture of shared success and reliance (Hamsinah et al., 2023). Openness relating to successful performance of employees can also improve morale within organizations that fully embrace the importance of TQM.

Theme 4: Proactive Measures

Penetration testing was a popular strategy to proactively detect flaws in an organization’s insider threat strategy (Al Sadi et al., 2023). Testing can incorporate many aspects, from internal phishing emails to different levels of personnel within the company, to actively attempting access to unauthorized areas using a targeted users’ credentials. P4 stated, you can compare the daunting task of preventing an insider threat incident to the differences between an IT security organization's red and blue team; a red

team operator only needs one unpatched vulnerability to gain access, while the blue team must be aware of all of these vulnerabilities and how to mitigate them correctly.

During nearly all discussions on insider threat with peers in the IT realm over the years, it was commonly agreed upon that it was impossible to 100% mitigate the potential for insider threat. These discussions often tread into the realm of the unreasonable, culminating in the termination of every employee except one, to eliminate a potential insider threat incident. One participant has identified an IT organizational scenario where the potential for insider threat can be completely mitigated. After many years performing network security focus efforts tailored to insider threat prediction and response, this participant became weary of always being one step behind, and rarely leveraging their programming skills due to the broad spectrum of procedural requirements necessary for an effective strategy. Before accepting their current position in a new tech startup, there was a freedom to incorporate insider threat mitigations into the organizational foundation, using the following strategy: P5 described,

> First and foremost, I acknowledge that any organization with proprietary information, and more than one employee, will not be able to fully implement the strategy I use at my work. Our product is an open-source python library, that is hosted freely on Gitlab. The CEO secures rounds of funding for the continued development, and all employee salaries/expenses are locked into a distribution plan for at least a year in advance. All 18 employees are gifted the laptop and cellphone of their choice, and have their internet and cell phone plans paid for. Every employee has the updated codebase on their systems, and no one employee

> can do irreparable damage to it. There is nothing to steal, as everything associated with employment is theirs to keep.

The government, and the military especially, is branded in structure and of the expectations that following the rules is demanded. It was a standard practice to expect that established rules are followed to the letter. As mentioned in theme 3: employee profiling, consent to monitoring is not only common practice in the government, it was labeled on every monitor within the organizations. P4 noted,

> As a proactive measure, all employees are required to sign acknowledgements that they will protect classified information and prevent, to the best of their abilities, any deviations from policy. Employees are expected to report any of the deviations immediately to their direct supervisors. Interactive computer-based training modules are established to maintain compliance, and compliance with this training is tracked at least on an annual basis. This proactive measure offers an attribution to individuals and groups within an organization that are derelict in following procedure.

A common consensus among all participants regarding proactive measures to mitigate an insider threat incident, was the requirement to staff network security employees that had a fundamental understanding of common principles of organizational security. Each participant of this study highlighted prior experience with insider threat methodologies as a baseline requirement during the hiring process of network security professionals. P2-P5 all commented that a fundamental understanding in strategies identified within CompTIA or SANS security certifications would elevate resumes to the

top of the pile for potential employment candidates. P4 noted, that any security position vacancy within their organization would not entertain any applicant that did not already possess an active, or within the last 6 years, CompTIA Security+ certification. P4 stated, “an employee’s understanding of fundamental security concepts, such as man traps, physical security, and technical controls, is crucial for identifying and improving existing security implementations. This level of understanding helped the entire team look for new ways to enforce these principles within an organization, and be focused on security as new technologies and procedures are adopted.”

A common pitfall for proactive measures, were what areas to focus efforts upon, when an organization has limited staffing. P1-4 all expressed a level of frustration involved when a less than adequate staff is involved in the security process. This can be related to number of employees staffed, available funding within the organization, as well as the competence of existing staff. P2 noted,

> When dealing with government classified data, it can be a crapshoot when targeting focus areas, there is a volume and cost prioritization of what you're going to do. It’s probably more advantageous for us to focus on usb over print, and then someone prints the one document that you don’t want them to print, that does so much damage. Where they could’ve taken a whole hard drive worth of stuff and it would’ve had less damage than one document.

Proactive measures played a key role in achieving TQM within an organization. These measures were what separated an average insider threat strategy from a superior one. Continual improvement was an essential element of a successful TQM deployment,

relying heavily on proactive measures to effectively prevent potential organizational problems and reduce corrective actions as they crop up (Sinha & Dhall, 2020). The key to a successful TQM implementation is to utilize its principles in every available strategy composed within an organization. Studies have identified that a TQM implementation was strongest, when its dimensions were pursued as a proactive strategy (Yu et al., 2020). This does not imply that organization's that failed to adopt TQM principles early in their lifecycle were not able to benefit from TQM. For organizations that had not focused on TQM during their organization's early growth stages, a willingness to proactively setup TQM processes can lead to positive change within the organization (Hudnurkar et al., 2023). Per Kaur et al. (2020), taking proactive changes towards TQM adoption, at any stage, can improve organizational efficacies. Regarding maintaining an awareness of collegiate resources and related news for proactive steps to mitigate the insider threat, when instituting a robust TQM design, proactively utilizing available scholastic resources helped to strengthen a TQM implementation (Alauddin & Yamada, 2022).

Theme 5: Measurement of Success

As mentioned, under the discussion of proactive measures, penetration testing was a valuable methodology for measuring success. Internal auditing was a worthwhile companion strategy for measuring success. P1-P5 all identified internal auditing of system accesses and security frameworks as invaluable resources to continually improve and measure success. Using current auditing practices, one participant, who has been in the Information Security field for 15 years, claims to have successfully eliminated the insider threat within their current organization, although there were many precise

organizational elements required to be instituted to achieve success. P5 stated that continued success was reliant on a continual reassessment of all process and procedures within their organization. A worthwhile method for continued success was the extensive documentation of applied security measures.

Government organizations can have a more targeted focus for insider threat towards safeguarding classified information (Kelly, 2018). Measuring success can often come down to no attributable information leaks associated with a specific military base or government organization. P2-4 identified prolonged time frames without insider threat or security incidents, was a reasonable measure of success for their security strategies.

Organizational training was another critical element for success. Training programs could effectively be utilized under each of the themes in this study, but in their root goal, it was to get personnel to successfully comply with processes and procedures. P1-5 each touched on training as a key organizational requirement for improving an insider threat strategy within an organization. P4 noted, “training programs are great for raising awareness, but can be frustrating from a security standpoint. We had one of our site managers successfully complete an email phishing training, and an hour later click on a phishing email that compromised his laptop.” It was crucial after every security incident within an organization, to revisit existing training programs relating to the incident, and perform updates or reinforcements as necessary, to ensure the training outcomes stuck with the employees.

Each participant in this study shaped the themes identified. These themes promoted a measure of success towards mitigation of the insider threat within their

respective organizations. Actions taken by the participants, can form a blueprint for steps towards measuring success. P3-5 each commented how properly documented efforts and gaps in an insider threat strategy can measure the robustness, or shortcomings, of an organization's security posture. This can be pivotal in quick turnaround coverage of previously unidentified gaps. P4 noted, "it's important to stay up to date with current events and security forums. Many security implementations within the last year, were areas our team didn't realize were vulnerabilities, until we read about an incident exploiting an unknown vulnerability."

Measuring success was the evaluation of all conducted efforts towards TQM. For IT-based organizations, the insider threat strategy was often chained to the overarching network/system security strategy. For private sector companies, improvements in stock price and annual revenues can be a valid indicator for success measurement. Regarding for-profit organizations, TQMs positive effect on an organization's performance can be measured by their sales and revenue (Yu et al., 2020). TQMs dimensions should span many aspects of an organization's strategies to aid in its success. In order to properly measure success and performance of an organization's TQM implementation, self-assessment of processes was a core concept for identifying areas for improvement, including comparing issues faced by an organization's competitors (Lepistö et al., 2022b). Successful training programs rooted in TQM can be useful in measuring success. Per Dooley and Flor (1998), TQM-based training initiatives that focused towards learning objectives, over check-lists, afforded an organization to measure success against these objectives.

Applications to Professional Practice

The results of this study can be used by companies actively employing countermeasures to combat insider threat incidents. During analysis of collected data, it became clear that there were strategies identified that were not routine procedures throughout the participant's organizations. It is important for IT organizations to maintain a current approach to tackling the insider threat problem. By performing internal process inspections within a security practitioners' realm of responsibility, they can successfully identify gaps in their approaches, that may be mitigated by the implementations identified in this study.

Implications for Social Change

The implications of this study's findings for positive social change and the strategies applied may offer senior security managers avenues to improve their customer's confidence in their employed practices. By incorporating the findings of this study within an organization's insider threat strategy, a robust framework can be documented for customer feedback. This level of openness related to security posturing can instill confidence in the populace regarding the respect an organization has when handling personal information. This led to another implication for social change, which was a sense of security an organization's customers have when personally identifiable information was used during online transactions. Since the beginning of this study, there have been numerous data breaches that exposed customer personally identifiable information to unknown entities. Recently, the popular stock trading app, Robinhood, was hacked, and 5,000,000 users' personally identifiable information was absconded with

(Johnson, 2023). From a consumer perspective, there is often no delineation between a data breach from a trusted insider, or an outside entity. Insider threat data leaks tied in closely with outside data breaches, as the mitigations for both share many of the same procedures.

The findings detailed in this study further added to the existing body of knowledge available in peer reviewed resources on the topic of insider threat. Real world examples can illuminate previously unknown steps to improve security within an organization. Security professionals relying solely on past experiences or strategies learned from educational institutions may fall short in their efforts to strengthen their internal capabilities. In addition, further implications for social change included the promotion of securing the personal information of global customers. This is especially vital for social perceptions when organizations employed the collection and storage of personal information for analytical purposes, as the user's information is potentially at a high risk for data theft (Al-Harrasi et al., 2023). On the topic of today's society, securing personal digital information has been a growing concern over the last couple decades for IT companies. Collegiate institutions can employ updated areas of strategies identified in this study to further improve lessons for improved insider threat mitigation efforts within an organization.

Recommendations for Action

Upon completion of data collection, this study offered an interesting array of perspectives on insider threat strategies. While often times, the terms used by participants were different, the core concepts were predominantly shared among each of them. A

recommendation for action would be for IT security managers to perform an internal assessment of their existing strategies, and identify any gaps that this study can aid in solving. By using the identified themes as a blueprint, strategies implemented by the experienced leaders who participated in this study can be utilized by anyone actively tackling the insider threat problem. A good first step would be to identify all areas of risk within their organization. Implementing a risk register is a common method for identifying areas to target for strategy improvement. Next, it is crucial to understand technical limitations affecting their operating environment. Becoming familiar with the regional security policies can help target security compliances. Employee profiling strategies is another recommendation for improving insider threat methodologies within an organization. Cataloging levels of permissions granted to employees can help target areas that are more vulnerable due to potentially unnecessary accesses. These actions can constitute proactive measures within an organization. Further proactive measures recommended for action are to identify gaps in training that could compromise critical systems. An action to aid in measuring the success of insider threat strategies implemented would be to perform rigorous and routine self-assessments of security implementations. Any technical manager or information security professional paying attention to the findings of this study, could benefit by becoming familiar with the themes identified, and applying them to gaps identified within their respective organization's security framework.

Recommendations for Further Study

During this qualitative study, I noticed many participants adopted new technologies to help combat insider threat within their respective organizations. A recommendation for further study would be to identify cutting edge technologies that have been introduced into the IT landscape since the conclusion of the data analysis contained in this study. It became clear during my analysis, that many new strategies can be created from reviewing new technical advancements through the lens of insider threat mitigation. I work with a data scientist specializing in mathematical analysis relating to machine learning, and every week he briefs us on new white papers released in the data science fields. While these documents often pertained solely to data efficiencies and new ways to extrapolate data from large data sets, they can have far reaching potential in the sphere of insider threat. A solid recommendation for further study would be to catalog these publications regularly and perform reviews of them using an insider threat perspective or scenario.

Reflections

This study began nearly 3 years ago, and has been an exciting adventure as a security professional. Prior to starting my journey at Walden University, I had no prior knowledge of qualitative research procedures, or conceptual frameworks. I had a limited view of how I thought my dissertation would unfold, and that view grew exponentially with each completed class towards a doctorate in IT. When analyzing collected data, it was surprising that there was not a common terminology among the participants. I initially planned to perform syntax comparisons to identify themes, however the verbiage

for each of these themes differed slightly. This was especially true when comparing terms used between the private sector and government entities. Understanding the context of the participant's statements, versus terms used, became more important during the analysis phase of this body of work. As a senior computer security manager, it was a humbling experience to strip away personal biases while conducting this study. It was especially humbling interacting with the participants in this study, as the more I documented areas of expertise relating to insider threat, the more I realized I was less effective in my current duties. I have already began implementing lessons learned from the data collection phase of this study, and I am starting to see more of the big picture as it related to mitigating the insider threat problem with a technical organization.

Summary and Study Conclusions

Designing and implementing an effective strategy to eliminate or reduce insider threat is not easy, nor is it perfectly documented for simple implementation within an organization. The leveraging of TQM for this study illustrated the importance of promoting an insider threat understanding at all employment levels within an organization. While senior leaders may be viewed as ultimately accountable for failures resulting in an insider threat incident, their ability to succeed is directly tied to the diligence of each echelon of responsibility.

It is also important to maintain an understanding of the changing landscape of the information security profession. As new technologies are adopted within an organization, new vulnerabilities are often included in this adoption. The themes identified in this study share a commonality among varying organizations tackling the shared problem. By

aligning the adoption of new technologies with the identified themes, IT leaders can improve their posturing from a security standpoint.

References

Abdelsadeq, Z. A. A., Omar, S. N., Basir, N., & Heng, N. F. N. B. M. R. (2019). Unintentional insider threats countermeasures model (UITCM). In *Proceedings of the 2019 International Conference on Cybersecurity (ICoCSec)* (pp. 53–58). IEEE. https://doi.org/10.1109/ICoCSec47621.2019.8970986

Acquah, I. S. K., Quaicoe, J., & Arhin, M. (2023). How to invest in total quality management practices for enhanced operational performance: Findings from PLS-SEM and fsQCA. *The TQM Journal*, *35*(7), 1830–1859. https://doi.org/10.1108/TQM-05-2022-0161

Adane, K. (2020). Development of advisory knowledge-based expert system to identify and mitigate unintentional insider threats in financial institutions of Ethiopia. *IUP Journal of Computer Sciences*, *14*(3), 7–23.

Al Sadi, A., Berardi, D., Callegati, F., Melis, A., Prandini, M., & Tolomei, L. (2023). A Structured Approach to Insider Threat Monitoring for Offensive Security Teams. *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), Consumer Communications & Networking Conference (CCNC), 2023 IEEE 20th*, 628–631. https://doi.org/10.1109/CCNC51644.2023.10060017

Alauddin, N., & Yamada, S. (2022). TQM model based on Deming prize for schools. *International Journal of Quality and Service Sciences*, *14*(4), 635–651. https://doi.org/10.1108/IJQSS-09-2021-0131

Alhajjar, E., & Bradley, T. (2022). Survival analysis for insider threat: Detecting insider threat incidents using survival analysis techniques. Computational &

Mathematical Organization Theory, 28(4), 335–351. https://doi.org/10.1007/s10588-021-09341-0

Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2023). Towards protecting organisations' data by preventing data theft by malicious insiders. *International Journal of Organizational Analysis*, *31*(3), 875–888. https://doi.org/10.1108/IJOA-01-2021-2598

Alhebaishi, N., Wang, L., Jajodia, S., & Singhal, A. (2019). Mitigating the insider threat of remote administrators in clouds through maintenance task assignments. *Journal of Computer Security*, *27*(4), 427–458. https://doi.org/10.3233/JCS-191306

Alsowail, R. A., & Al-Shehari, T. (2020). Empirical detection techniques of insider threat incidents. *IEEE Access*, *8*, 78385–78402. https://doi.org/10.1109/ACCESS.2020.2989739

Alsowail, R. A., & Al-Shehari, T. (2021). A multi-tiered framework for insider threat prevention. *Electronics*, *10*(9), Article 1005. https://doi.org/10.3390/electronics10091005

Althebyan, Q. (2020). Mitigating insider threats on the edge: A knowledgebase approach. *International Arab Journal of Information Technology*, *17*(4A), 621–628. https://doi.org/10.34028/iajit/17/4A/6

Arce, D. (2023). Cybersecurity For Defense Economists. Defence & Peace Economics, 34(6), 705–725. https://doi.org/10.1080/10242694.2022.2138122

Asmaningrum, N., & Tsai, Y.-F. (2018). Nurse perspectives of maintaining patient dignity in Indonesian clinical care settings: A multicenter qualitative study.

Journal of Nursing Scholarship, *50*(5), 482–491. https://doi.org/10.1111/jnu.12410

Bada, M., & Chua, Y. T. (2021). Understanding risk and risk perceptions of cybercrime in underground forums. In *2021 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1–11). IEEE. https://doi.org/10.1109/eCrime54498.2021.9738790

BaMaung, D., McIlhatton, D., MacDonald, M., & Beattie, R. (2018). The enemy within? The connection between insider threat and terrorism. *Studies in Conflict & Terrorism*, *41*(2), 133–150. https://doi.org/10.1080/1057610X.2016.1249776v

Bao, H., Lu, R., Li, B., & Deng, R. (2016). BLITHE: Behavior rule-based insider threat detection for smart grid. *IEEE Internet of Things Journal*, *3*(2), 190–205. https://doi.org/10.1109/JIOT.2015.2459049

Bedford, J., & van der Laan, L. (2021). Operationalising a framework for organisational vulnerability to intentional insider threat: the OVIT as a valid and reliable diagnostic tool. Journal of Risk Research, 24(9), 1180–1203. https://doi.org/10.1080/13669877.2020.1806910

Bell, A. J. C., Rogers, M. B., & Pearce, J. M. (2019). The insider threat: Behavioral indicators and factors influencing likelihood of intervention. *International Journal of Critical Infrastructure Protection*, *24*, 166–176. https://doi.org/10.1016/j.ijcip.2018.12.001

Benzaquen, J., Carlos, M., Norero, G., Armas, H., & Pacheco, H. (2021). Quality in private health companies in Peru: The relation of QMS & ISO 9000 principles on

TQM factor. *International Journal of Healthcare Management*, *14*(2), 311–319. https://doi.org/10.1080/20479700.2019.1644472

Bonatti, P. A., Ioffredo, L., Petrova, I. M., Sauro, L., & Siahaan, I. R. (2020). Real-time reasoning in OWL2 for GDPR compliance. *Artificial Intelligence, 289*, Article 103389. https://doi.org/10.1016/j.artint.2020.103389

Brooks, S. K., Patel, D., & Greenberg, N. (2023). "Exceptionally challenging time for all of us": Qualitative study of the COVID-19 experiences of partners of diplomatic personnel. PLoS ONE, 18(11), 1–27. https://doi.org/10.1371/journal.pone.0293557

Brown, D. P., Buede, D., & Vermillion, S. D. (2019). Improving Insider Threat Detection Through Multi-Modelling/Data Fusion. *Procedia Computer Science, 153, 100–107*. https://doi.org/10.1016/j.procs.2019.05.060

Bulpett, B. (2020). Safeguarding against the insider threat. *Network Security, 2020(6), 14–17*. https://doi.org/10.1016/S1353-4858(20)30068-4

Cabana, G. C., & Kaptein, M. (2021). Team Ethical Cultures Within an Organization: A Differentiation Perspective on Their Existence and Relevance. Journal of Business Ethics, 170(4), 761–780. https://doi.org/10.1007/s10551-019-04376-5

Callegati, F., Giallorenzo, S., Melis, A., & Prandini, M. (2018). Cloud-of-Things meets Mobility-as-a-Service: An insider threat perspective. *Computers & Security, 74, 277–295*. https://doi.org/10.1016/j.cose.2017.10.006

Campos, N. J. F., De Vera, A. A. A., Gonzales, E. J. M., Guevarra, J. M. A., Ubaldo, N. L., & Vigonte, F. G. (2022). The Impact of Quality Commitment on the

Implementation of TQM in Hensa 168 Rubber Corporation. *IUP Journal of Operations Management*, *21*(1), 43–58

Carson, J. (2017). The evolution of the digital insider trader. *Computer Fraud & Security*, *2017*(8), 12–15. https://doi.org/10.1016/S1361-3723(17)30071-4

Castelló, M., McAlpine, L., Sala-Bubaré, A., Inouye, K., & Skakni, I. (2021). What perspectives underlie "researcher identity"? A review of two decades of empirical studies. *Higher Education (00181560)*, *81*(3), 567–590. https://doi.org/10.1007/s10734-020-00557-8

Cejas, O. A., Azeem, M. I., Abualhaija, S., & Briand, L. C. (2023). NLP-Based Automated Compliance Checking of Data Processing Agreements Against GDPR. IEEE Transactions on Software Engineering, Software Engineering, IEEE Transactions on, IIEEE Trans. *Software Eng*, *49(9), 4282–4303*. https://doi.org/10.1109/TSE.2023.3288901

Chapman, P. (2020). Are your IT staff ready for the pandemic-driven insider threat? *Network Security*, *2020(4), 8–11*. https://doi.org/10.1016/S1353-4858(20)30042-8

Chattopadhyay, P., Wang, L., & Tan, Y. (2018). Scenario-based insider threat detection from cyber activities. *IEEE Transactions on Computational Social Systems, Computational Social Systems, IEEE Transactions on, IEEE Trans. Comput. Soc. Syst*, *5(3), 660–675.* https://doi-org.ezp.waldenulibrary.org/10.1109/TCSS.2018.2857473

Chen, T., Han, T., Kammueller, F., Nemli, I., & Probst, C. W. (2016). Model based analysis of insider threats. *2016 International Conference On Cyber Security And*

Protection Of Digital Services (Cyber Security), Cyber Security And Protection Of Digital Services (Cyber Security), 2016 International Conference On, 1–3. https://doi.org/10.1109/CyberSecPODS.2016.7502350

Collins, K. (2017). *How U.S. Law Enforcement Caught Reality Winner, the NSA Contractor Charged With Leaking Top-Secret Materials*. NextGov/FCW. https://www.nextgov.com/digital-government/2017/06/how-us-law-enforcement-caught-reality-winner-nsa-contractor-charged-leaking-top-secret-materials/138426/

Creech, G. E. (2020). "Real" Insider Threat: Toxic Workplace Behavior in the Intelligence Community. *International Journal of Intelligence & Counterintelligence, 33(4), 682–708*. https://doi.org/10.1080/08850607.2020.1789934

Creswell, J. W., & Creswell, J. D. (2018). Research design: qualitative, quantitative & mixed methods approaches Thousand Oaks, CA: Sage.

Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches. Thousand Oaks, CA: Sage.

Croix, A., Barrett, A., & Stenfors, T. (2018). How to...do research interviews in different ways. *Clinical Teacher, 15(6), 451–456*. https://doi.org/10.1111/tct.12953

Cuthbertson, L. M., Robb, Y. A., & Blair, S. (2020). Theory and application of research principles and philosophical underpinning for a study utilising interpretative phenomenological analysis. *Radiography, 26*(2), e94–e102. https://doi.org/10.1016/j.radi.2019.11.092

Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. Symmetry (20738994), 15(11), 1981. https://doi.org/10.3390/sym15111981

Darnton, C. (2022). The Provenance Problem: Research Methods and Ethics in the Age of WikiLeaks. American Political Science Review, 116(3), 1110–1125. https://doi.org/10.1017/S0003055421001374

de Valk, G. (2019). On Screening and the Insider Threat - a Methodological Exploration. *National Security & the Future, 20(1/2), 35–50.* https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=242d39dd-5fad-4b51-8e66-fcd72899528e%40redis

Devotta, K., Woodhall-Melnik, J., Pedersen, C., Wendaferew, A., Dowbor, T. P., Guilcher, S. J. T., Hamilton-Wright, S., Ferentzy, P., Hwang, S. W., & Matheson, F. I. (2016). Enriching qualitative research by engaging peer interviewers: a case study. *Qualitative Research, 16(6), 661–680.* https://doi.org/10.1177/1468794115626244

Dieterle, A.-K., & Duchek, S. (2023). Implementing Strategic Resilience Through Cooperation Projects with Start-ups: a Multiple Case Study. Schmalenbach Journal of Business Research (SBUR), 75(4), 549–586. https://doi.org/10.1007/s41471-023-00173-z

Dooley, K. J., & Flor, R. E. (1998). Perceptions of success and failure in TQM initiatives. *Journal of Quality Management, 3(2), 157.* https://doi.org/10.1016/S1084-8568(99)80111-4

Dubey, R., Gunasekaran, A., Childe, S. J., Papadopoulos, T., Hazen, B. T., & Roubaud, D. (2018). Examining top management commitment to TQM diffusion using institutional and upper echelon theories. *International Journal of Production Research*, *56*(8), 2988–3006. https://doi.org/10.1080/00207543.2017.1394590

Edmunds, T. K. (2017). Perceived Barriers to SME-College Collaboration: The Case of the Province of Manitoba. *College Quarterly, 20(2).* https://eds.p.ebscohost.com/eds/detail/detail?vid=0&sid=09158fd2-e14c-49c6-8ff7-7311d669b0e2%40redis&bdata=JkF1dGhUeXBlPXNoaWImc2l0ZT1lZHMtbGl2ZSZzY29wZT1zaXRl#AN=EJ1142557&db=eric

Eggenschwiler, J., Agrafiotis, I., & Nurse, J. R. (2016). Insider threat response and recovery strategies in financial services firms. *Computer Fraud & Security*, *2016(11), 12–19*. https://doi.org/10.1016/S1361-3723(16)30091-4

Egwunatum, S. I., Anumudu, A. C., Eze, E. C., & Awodele, I. A. (2022). Total quality management (TQM) implementation in the Nigerian construction industry. *Engineering, Construction and Architectural Management*, *29*(1), 354–382. https://doi.org/10.1108/ECAM-08-2020-0639

Elifoglu, I. H., Abel, I., & Taşseven, Ö. (2018). Minimizing Insider Threat Risk with Behavioral Monitoring. *Review of Business, 38(2), 61–73.* https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=03a4cff5-5fb1-4329-9c11-98df2ce924d5%40redis

Ellis, P. (2020). Sampling in qualitative research (1). *Wounds UK, 16(3), 82–83*. https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=e749952e-9a07-4875-94f9-ee46a620ac32%40redis

Emary, P. C., Stuber, K. J., Mbuagbaw, L., Oremus, M., Nolet, P. S., Nash, J. V., Bauman, C. A., Ciraco, C., Couban, R. J., & Busse, J. W. (2022). Risk of bias in chiropractic mixed methods research: a secondary analysis of a meta-epidemiological review. *Journal of the Canadian Chiropractic Association, 66(1), 7–20*. https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=efff9d51-abc1-4c88-bf92-ffe0df853fd7%40redis

Enemchukwu, E. A. (2022). When handling microaggressions, be aware of your own biases. *Urology Times, 50(5), 40–41*. https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=f2ab9d6f-b3d1-4d70-91a1-46370263234a%40redis

Ennis, D. (2020). *Barclays faces $1.1B fine over alleged monitoring of employees*. BankingDive. https://www.bankingdive.com/news/barclays-fine-ICO-monitoring-employees/583231/

Fanzhi, M., Fang, L., Yunsheng, F., & Zhihong, T. (2018). Deep Learning Based Attribute Classification Insider Threat Detection for Data Security. *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Data Science in Cyberspace (DSC), 2018 IEEE Third International Conference on, DSC*, 576–581. https://doi.org/10.1109/DSC.2018.00092

Giddens, L., Amo, L. C., & Cichocki, D. (2020). Gender bias and the impact on managerial evaluation of insider security threats. *Computers & Security, 99*. https://doi.org/10.1016/j.cose.2020.102066

Gioe, D. V., & Hatfield, J. M. (2021). A damage assessment framework for insider threats to national security information: Edward Snowden and the Cambridge Five in comparative historical perspective. *Cambridge Review of International Affairs, 34(5), 704–738*. https://doi.org/10.1080/09557571.2020.1853053

Godskesen, T., Björk, J., & Juth, N. (2023). Challenges regarding informed consent in recruitment to clinical research: a qualitative study of clinical research nurses' experiences. Trials, 24(1), 1–12. https://doi.org/10.1186/s13063-023-07844-6

Gönen, S., Sayan, H. H., Yılmaz, E. N., Üstünsoy, F., & Karacayılmaz, G. (2020). False data injection attacks and the insider threat in smart systems. *Computers & Security, 97*. https://doi.org/10.1016/j.cose.2020.101955

Greitzer, F. L., Lee, J. D., Purl, J., & Zaidi, A. K. (2019). Design and Implementation of a Comprehensive Insider Threat Ontology. *Procedia Computer Science, 153, 361–369*. https://doi.org/10.1016/j.procs.2019.05.090

Greitzer, F., Purl, J., Becker, D. E., Sticha, P., & Leong, Y. M. (2019). Modeling expert judgments of insider threat using ontology structure: Effects of individual indicator threat value and class membership. *In Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Greitzer, F. L., Purl, J., Leong, Y. M., & Sticha, P. J. (2019). Positioning Your Organization to Respond to Insider Threats. *IEEE Engineering Management Review*, *47*(2), 75–83. https://doi.org/10.1109/EMR.2019.2914612

Gunasekhar, T., Rao, K. T., & Basu, M. T. (2015). Understanding insider attack problem and scope in cloud. 2015 International Conference on Circuits, Power & Computing Technologies [ICCPCT-2015], 1–6. https://doi.org/10.1109/ICCPCT.2015.7159380

Gupta, M., & Sharman, R. (2012). Determinants of Data Breaches: A Categorization-Based Empirical Investigation. Journal of Applied Security Research, 7(3), 375–395. https://doi.org/10.1080/19361610.2012.686098

Hamsinah, H., Sunarsi, D., Narimawati, U., Munna, A. S., & Pawar, A. (2023). The Influence of Total Quality Management (TQM) and Organizational Culture on Employee Job Satisfaction that Impacts Employee Performance (Case Study on Cooperatives in South Tangerang City). *Ekuilibrium: Jurnal Ilmiah Bidan Ilmu Ekonomi, 18(2), 156–168*. https://doi.org/10.24269/ekuilibrium.v18i2.2023.pp156-168

Ho, S. M., Hancock, J. T., Booth, C., Burmester, M., Liu, X., & Timmarajus, S. S. (2016). Demystifying insider threat: Language-action cues in group dynamics. *In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 2729-2738). IEEE*. https://doi.org/10.1109/HICSS.2016.343

Ho, S. M., Kaarst, B. M., & Benbasat, I. (2018). Trustworthiness attribution: Inquiry into insider threat detection. Journal of the Association for Information Science & Technology, 69(2), 271–280. https://doi.org/10.1002/asi.23938

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR), 52(2), 1-40*. https://doi-org.ezp.waldenulibrary.org/10.1145/3303771

Huang, L., & Zhu, Q. (2021). Duplicity Games for Deception Design With an Application to Insider Threat Mitigation. *IEEE Transactions on Information Forensics and Security, Information Forensics and Security, IEEE Transactions on, IEEE Trans.Inform.Forensic Secur, 16, 4843–4856*. https://doi.org/10.1109/TIFS.2021.3118886

Hubbard, T., Klimavicz, J. F., Wong, S., & Steinhoff, J. C. (2021). Zero Trust in a Virtual Cybersecurity World. Journal of Government Financial Management, 70(2), 12–19.

Hudnurkar, M., Ambekar, S., Bhattacharya, S., & Sheorey, P. A. (2023). Relationship of total quality management with corporate sustainability in the MSME sector: does innovation capability play a mediating role? *The TQM Journal, 35(7), 1860–1886*. https://doi.org/10.1108/TQM-03-2022-0095

Hughes, K., Hughes, J., & Cocq, F. P.-L. (2020). Introduction: making the case for qualitative interviews. *International Journal of Social Research Methodology, 23(5), 541–545*. https://doi.org/10.1080/13645579.2020.1766756

Hsu, J.-H., & Wu, C.-H. (2023). Applying Segment-Level Attention on Bi-Modal Transformer Encoder for Audio-Visual Emotion Recognition. IEEE Transactions on Affective Computing, 14(4), 3231–3243. https://doi.org/10.1109/TAFFC.2023.3258900

Islam, A., & Salam, A. (2022). Multiattribute Decision-Making of TQM Performance of Hospitals Using TQM Digraphs. *Mathematical Problems in Engineering, 1–17*. https://doi.org/10.1155/2022/3119888

Issac, G., Rajendran, C., & Anantharaman, R. N. (2004). A conceptual framework for total quality management in software organizations. *Total Quality Management & Business Excellence, 15(3), 307–344*. https://doi-org.ezp.waldenulibrary.org/10.1080/1478336042000183398

Jabbour, G. (Gus), & Jabbour, J. J. (2021). Mitigating the Insider Threat to Information Systems Using Fully Embedded and Inseparable Autonomic Self-Protection Capability. *IADIS International Journal on Computer Science & Information Systems, 16(1), 81–95*. https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=b4193177-db24-4f3c-9345-e0ae59ff69e7%40redis

Jeong, M., & Zo, H. (2021). Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques. *Telematics and Informatics, 63*. https://doi.org/10.1016/j.tele.2021.101670

Johnson, C. A. (2023). Data Breach Class Actions: How Article III Standing Analysis Should Evolve After TransUnion, LLC v. Ramirez. *Minnesota Law Review,*

107(5), 2249–2283. https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=a9h&AN=163652871&site=eds-live&scope=site

Joshi, C., Aliaga, J. R., & Insua, D. R. (2021). Insider threat modeling: An adversarial risk analysis approach. *IEEE Transactions on Information Forensics and Security, Information Forensics and Security, IEEE Transactions on, IEEE Trans.Inform.Forensic Secur, 16, 1131–1142*. https://doi-org.ezp.waldenulibrary.org/10.1109/TIFS.2020.3029898

Jurišić, M., Tomičić, I., & Grd, P. (2023). User Behavior Analysis for Detecting Compromised User Accounts: A Review Paper. Cybernetics & Information Technologies, 23(3), 102–113. https://doi.org/10.2478/cait-2023-0027

Katz, J., Heidkamp, R. A., Khatry, S. K., LeClerq, S. C., Manandhar, P., Munos, M. K., Bryce, E., Thorne-Lyman, A. L., & Lama, T. P. (2023). How does social desirability bias influence survey-based estimates of the use of antenatal care in rural Nepal? A validation study. BMJ Open, 13(7). https://doi.org/10.1136/bmjopen-2022-071511

Kaur, M., Singh, K., & Singh, D. (2020). Assessing the synergy status of TQM and SCM initiatives in terms of business performance of the medium and large scale Indian manufacturing industry. International Journal of Quality & Reliability Management, 37(2), 243–278. https://doi.org/10.1108/IJQRM-07-2018-0192

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity, 7(1), 1–13. https://doi.org/10.1093/cybsec/tyab005

Kelly, W. E. (2018). Insider Threats: Enemies Within Our Government. *American Intelligence Journal, 35(2), 7–11*. https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=d9c57c25-46f7-49ba-9a1f-312e97379415%40redis

Khalfallah, M., Ben Salem, A., Zorgati, H., & Lakhal, L. (2022). Innovation mediating relationship between TQM and performance: cases of industrial certified companies. *The TQM Journal*, *34*(3), 552–575. https://doi.org/10.1108/TQM-01-2021-0019

Kim, A., Oh, J., Ryu, J., & Lee, K. (2020). A Review of Insider Threat Detection Approaches With IoT Perspective. *IEEE Access, Access, IEEE*, *8*, 78847–78867. https://doi.org/10.1109/ACCESS.2020.2990195

Kim, B., Lee, D.-Y., & Kim, B. (2020). Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks. *Behaviour & Information Technology, 39(11), 1156–1175*. https://doi.org/10.1080/0144929X.2019.1653992

Kim, H. L., Hovav, A., & Han, J. (2019). Protecting intellectual property from insider threats: A management information security intelligence perspective. *Journal of Intellectual Capital, 21(2), 181–202*. https://doi.org/10.1108/JIC-05-2019-0096

King, I. J., & Huang, H. (2023). EULER: Detecting Network Lateral Movement via Scalable Temporal Link Prediction. ACM Transactions on Privacy & Security, 26(3), 1–36. https://doi.org/10.1145/3588771

Kirkpatrick, S. I., Guenther, P. M., Subar, A. F., Krebs-Smith, S. M., Herrick, K. A., Freedman, L. S., & Dodd, K. W. (2022). Using Short-Term Dietary Intake Data to Address Research Questions Related to Usual Dietary Intake among Populations and Subpopulations: Assumptions, Statistical Techniques, and Considerations. *Journal of the Academy of Nutrition and Dietetics, 122(7), 1246–1262*. https://doi.org/10.1016/j.jand.2022.03.010

Koutsouvelis, V., Shiaeles, S., Ghita, B., & Bendiab, G. (2020). Detection of Insider Threats using Artificial Intelligence and Visualisation. *2020 6th IEEE Conference on Network Softwarization (NetSoft), Network Softwarization (NetSoft), 2020 6th IEEE Conference On*, 437–443. https://doi.org/10.1109/NetSoft48620.2020.9165337

Koyama, H., Nakagawa, Y., Tanimoto, S., Endo, T., Hatashima, T., & Kanai, A. (2022). A Study of Risk Assessment Quantification for Secure Telework. 2022 12th International Congress on Advanced Applied Informatics (IIAI-AAI), Advanced Applied Informatics (IIAI-AAI), 2022 12th International Congress on, IIAI-AAI, 574–580. https://doi.org/10.1109/IIAIAAI55812.2022.00115

Lane, R., Short, R., Jones, M., Hull, L., Howard, L. M., Fear, N. T., & MacManus, D. (2022). Relationship conflict and partner violence by UK military personnel following return from deployment in Iraq and Afghanistan. *Social Psychiatry and*

Psychiatric Epidemiology, 57(9), 1795–1805. https://doi.org/10.1007/s00127-022-02317-8

Le, D. C., Zincir-Heywood, N., & Heywood, M. I. (2020). Analyzing data granularity levels for insider threat detection using machine learning. *IEEE Transactions on Network and Service Management, Network and Service Management, IEEE Transactions on, IEEE Trans. Netw. Serv. Manage, 17(1), 30–44*. https://doi-org.ezp.waldenulibrary.org/10.1109/TNSM.2020.2967721

Lee, J., Alghamdi, A., & Zaidi, A. K. (2022). Creating a Digital Twin of an Insider Threat Detection Enterprise Using Model-Based Systems Engineering. 2022 IEEE International Systems Conference (SysCon), Systems Conference (SysCon), 2022 IEEE International, 1–7. https://doi.org/10.1109/SysCon53536.2022.9773890

Lepistö, K., Saunila, M., & Ukko, J. (2022a). Facilitating SMEs' profitability through total quality management: the roles of risk management, digitalization, stakeholder management and system deployment. *The TQM Journal, Vol. 34 No. 6, pp. 1572-1599*. https://doi.org/10.1108/TQM-07-2021-0204

Lepistö, K., Saunila, M., & Ukko, J. (2022b). The impact of certification on the elements of TQM exploring the influence of company size and industry. *International Journal of Quality & Reliability Management, 39(1), 30–52*. https://doi.org/10.1108/IJQRM-11-2020-0362

Lewis, C. A., Khukhrin, M., Galyautdinova, S., Musharraf, S., & Lewis, M. J. (2017). The Positive Functioning Inventory: A Russian translation. *Indian Journal of Positive Psychology*, *8*(3), 284–287

Li, H., Luo, X., & Chen, Y. (2021). Understanding Information Security Policy Violation from a Situational Action Perspective. Journal of the Association for Information Systems, 22(3), 739–772. https://doi.org/10.17705/1jais.00678

Lin, L., Li, S., Lv, X., & Li, B. (2021). BTDetect: An Insider Threats Detection Approach Based on Behavior Traceability for IaaS Environments. 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), 2021 IEEE Intl Conf on, ISPA-BDCLOUD-SOCIALCOM-SUSTAINCOM, 344–351. https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00055

Liu, C., Lim, R. L., McCabe, K. L., Taylor, S., & Calvo, R. A. (2016). A Web-Based Telehealth Training Platform Incorporating Automated Nonverbal Behavior Feedback for Teaching Communication Skills to Medical Students: *A Randomized Crossover Study. Journal of Medical Internet Research, 18(9), e246*. https://doi.org/10.2196/jmir.6299

Liu, L., De Vel, O., Han, Q., Zhang, J., & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials, IEEE, IEEE Commun. Surv. Tutorials, 20(2), 1397–1417*. https://doi.org/10.1109/COMST.2018.2800740

Liu, Z., & Wang, L. (2021). Defense strategy against load redistribution attacks on power systems considering insider threats. *IEEE Transactions on Smart Grid, Smart Grid, IEEE Transactions on, IEEE Trans. Smart Grid, 12(2), 1529–1540*. https://doi-org.ezp.waldenulibrary.org/10.1109/TSG.2020.3023426

Lu, G., Zhang, H., Liu, T., Liao, K., & Feng, C. (2022). Experimental Evaluation of Insider Threat Detection Methods Based on Temporal Representation. 2022 IEEE 10th International Conference on Information, Communication and Networks (ICICN), Information, Communication and Networks (ICICN), 2022 IEEE 10th International Conference On, 682–688. https://doi.org/10.1109/ICICN56848.2022.10006539

Ma, Q., & Rastogi, N. (2020). DANTE: Predicting Insider Threat using LSTM on system logs. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Trust, Security and Privacy in Computing and Communications (TrustCom), 2020 IEEE 19th International Conference on, TRUSTCOM*, 1151–1156. https://doi.org/10.1109/TrustCom50675.2020.00153

Maasberg, M., Van Slyke, C., Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. *Communications of the ACM, 63(12), 64–80*. https://doi.org/10.1145/3408864

Markos, E., Labrecque, L. I., & Milne, G. R. (2018). A New Information Lens: The Self-concept and Exchange Context as a Means to Understand Information Sensitivity of Anonymous and Personal Identifying Information. *Journal of Interactive Marketing, 42, 46–62*. https://doi.org/10.1016/j.intmar.2018.01.004

May, L. Y., Ismail, R., Ismail, N. H., & Hamzah, M. I. (2018). Interview Protocol Refinement: Fine-Tuning Qualitative Research Interview Questions for Multi-Racial Populations in Malaysia. *Qualitative Report*, *23*(11), 2700–2713

Mikalef, P., Boura, M., Lekakos, G., & Krogstie, J. (2019). Big data analytics and firm performance: Findings from a mixed-method approach. *Journal of Business Research, 98,* 261–276. https://doi.org/10.1016/j.jbusres.2019.01.044

Milakovich, M. E. (1998). The State of Results-Driven Customer Service Quality in Government. *National Productivity Review (Wiley), 17(2), 47–54*. https://doi.org/10.1002/npr.4040170208

Mills, J. U., Stuban, M. F., & Dever, J. (2017). Predict insider threats using human behaviors. *IEEE Engineering Management Review, Engineering Management Review, IEEE, IEEE Eng. Manag. Rev, 45(1), 39–48*. https://doi.org/10.1109/EMR.2017.2667218

Moore, A. P., Cassidy, T. M., Theis, M. C., Bauer, D., Rousseau, D. M., & Moore, S. B. (2018). Balancing Organizational Incentives to Counter Insider Threat. *2018*

IEEE Security and Privacy Workshops (SPW), Security and Privacy Workshops (SPW), 2018 IEEE, SPW, 237–246. https://doi.org/10.1109/SPW.2018.00039

Mtukushe, N., Onaolapo, A. K., Aluko, A., & Dorrell, D. G. (2023). Review of Cyberattack Implementation, Detection, and Mitigation Methods in Cyber-Physical Systems. Energies (19961073), 16(13), 5206. https://doi.org/10.3390/en16135206

Nasir, R., Afzal, M., Latif, R., & Iqbal, W. (2021). Behavioral Based Insider Threat Detection Using Deep Learning. *IEEE Access, Access, IEEE, 9, 143266–143274*. https://doi.org/10.1109/ACCESS.2021.3118297

Nazir, S., Ali, M., & Shah, A. (2023). The Relationship of Tqm and Agile Manufacturing and Its Impact on Apparel Mill Performance. *New Horizons (1992-4399), 17(1), 83–104*. https://doi.org/10.29270/NH.17.1(23).06

Ofori-Duodu, M. S. (2019). Exploring Data Security Management Strategies for Preventing Data Breaches. Walden Dissertations and Doctoral Studies. https://scholarworks.waldenu.edu/dissertations/7947

Oh, J., Kim, T. H., & Lee, K. H. (2019). Advanced insider threat detection model to apply periodic work atmosphere. *KSII Transactions on Internet & Information Systems, 13(3), 1722–1737*. https://doi.org/10.3837/tiis.2019.03.035

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

Paraschivescu, A. O. (2020). Total Quality Self-assessment. *Economy Transdisciplinarity Cognition*, *23*(1), 36–47

Paraskevoulakou, E., & Kyriazis, D. (2023). ML-FaaS: Toward Exploiting the Serverless Paradigm to Facilitate Machine Learning Functions as a Service. *IEEE Transactions on Network and Service Management, Network and Service Management, IEEE Transactions on, IEEE Trans. Netw. Serv. Manage, 20(3)*. 2110–2123. https://doi.org/10.1109/TNSM.2023.3239672

Parkin, S. (2017). Observant participation with people who inject drugs in street-based settings: reflections on a method used during applied ethnographic research. *Addiction Research & Theory*, *25*(1), 39–47. https://doi.org/10.1080/16066359.2016.1196675

Pellegrino, R., Costantino, N., & Tauro, D. (2020). The role of risk management in buyer-supplier relationships with a preferred customer status for total quality management. *The TQM Journal, Vol. 32 No. 5, pp. 959-981*. https://doi.org/10.1108/TQM-04-2019-0107

Prentice, M. M. (2021). The securitized workplace: document protection, insider threats and emerging ethnographic barriers in a South Korean organization. Journal of Organizational Ethnography, 10(3), 258–273. https://doi.org/10.1108/JOE-02-2021-0010

Probst, B. (2015). The Eye Regards Itself: Benefits and Challenges of Reflexivity in Qualitative Social Work Research. *Social Work Research, 39(1), 37–48*. https://doi.org/10.1093/swr/svu028

Putri, N. T., Yusof, S. M., Hasan, A., & Darma, H. S. (2017). A structural equation model for evaluating the relationship between total quality management and employees' productivity. *International Journal of Quality & Reliability Management, 34*(8), 1138–1151. https://doi.org/10.1108/IJQRM-10-2014-0161

Qin, N., & Kong, D. (2022). Access to Credit and Entrepreneurship: Evidence from China. Economic Development & Cultural Change, 71(1), 295–331. https://doi.org/10.1086/714440

Redman, B. K., & Caplan, A. L. (2021). Should the Regulation of Research Misconduct Be Integrated with the Ethics Framework Promulgated in The Belmont Report? *Ethics & Human Research, 43(1), 37–41*. https://doi.org/10.1002/eahr.500078

Reid, I. D., Gozna, L. F., & Boon, J. C. W. (2017). From Tactical to Strategic Deception Detection: Application of Psychological Synthesis. Journal of Strategic Security, 10(1), 1–21. https://doi.org/10.5038/1944-0472.10.1.1528

Ridge, D., Bullock, L., Causer, H., Fisher, T., Hider, S., Kingstone, T., Gray, L., Riley, R., Smyth, N., Silverwood, V., Spiers, J., & Southam, J. (2023). "Imposter participants" in online qualitative research, a new and increasing threat to data integrity? Health Expectations, 26(3), 941–944. https://doi.org/10.1111/hex.13724

Rodbert, M. (2020). Why organisational readiness is vital in the fight against insider threats. *Network Security, 2020(8), 7–9*. https://doi.org/10.1016/S1353-4858(20)30092-1

Roy, P., Sengupta, A., & Mazumdar, C. (2021). A Structured Control Selection Methodology for Insider Threat Mitigation. *Procedia Computer Science, 181, 1187–1195*. https://doi.org/10.1016/j.procs.2021.01.316

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications, 40, 247–257*. https://doi.org/10.1016/j.jisa.2017.11.001

Sanders, G. L., Upadhyaya, S., & Wang, X. (2019). Inside the Insider. IEEE Engineering *Management Review, 47(2), 84–91*. https://doi.org/10.1109/EMR.2019.2917656

Sawatnatee, A., & Prakancharoen, S. (2021). Insider Threat Detection and Prevention Protocol: ITDP. *International Journal of Online & Biomedical Engineering, 17(2), 69–89*. https://doi-org.ezp.waldenulibrary.org/10.3991/ijoe.v17i02.18297

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. R., & Burnap, P. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics, 9(1460), 1460*. https://doi.org/10.3390/electronics9091460

Schoenherr, J. R. (2022). Insider Threats and Individual Differences: Intention and Unintentional Motivations. IEEE Transactions on Technology and Society, Technology and Society, IEEE Transactions on, IEEE Trans. Technol. Soc, 3(3), 175–184. https://doi.org/10.1109/TTS.2022.3192767

Schwab, B. K. (2021). Insider Threat Management: Operating Environments, Detection Methods and Mitigation Strategies. *Journal of Physical Security, 14(1), 13–34*.

https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=9f58822f-fb8a-4e79-a155-dd6c341e406a%40redis

Shahriari, P., & Rasuli, B. (2020). No study is Ever Perfectly Flawless: Exploring Research Limitations in Theses and Dissertations of Iranian Higher Education Institutes. *Iranian Journal of Information Processing & Management, 36(1), 95–126*. https://www.sid.ir/FileServer/JF/441139910304

Shin, G. D., Jeon, K., & Lee, H.-E. (2022). Public library needs assessment to build a community-based library: Triangulation method with a social media data analysis. *Library and Information Science Research, 44(1)*. https://doi.org/10.1016/j.lisr.2022.101142

Singh, S., Sharma, P. K., Moon, S. Y., Moon, D., & Park, J. H. (2019). A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. *Journal of Supercomputing, 75*(8), 4543–4574. https://doi.org/10.1007/s11227-016-1850-4

Sinha, N., & Dhall, N. (2020). Mediating effect of TQM on relationship between organisational culture and performance: evidence from Indian SMEs. *Total Quality Management & Business Excellence, 31(15/16), 1841–1865*. https://doi.org/10.1080/14783363.2018.1511372

Slaughter, M., & Ahn, J. N. (2021, March 1). To Make Better Decisions, Mitigate Bias: Unconscious biases can get in the way of decision making. *TD Magazine, 75(3), 48*. https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=f340ae76-00e9-463a-9de3-6678a95e3523%40redis

Smidt, L., Pretorius, C., & van der Nest, D. P. (2022). Current Use of the Risk Register to Integrate Strategy and Risk- and Performance Management: A Case of a University of Technology in South Africa. *Journal of Accounting, Finance and Auditing Studies; Yalova Vol. 8, Iss. 4, pp. 140-171*. https://doi.org/10.32602/jafas.2022.031

Smit, R., van Yperen Hagedoorn, J. M. J., Versteeg, P., & Ravesteijn, P. (2021). The Soft Skills Business Demands of the Chief Information Security Officer. *Journal of International Technology & Information Management, 30(4), 41–61*. https://doi.org/10.58729/1941-6679.1522

Stafford, T. F. (2022). Platform-Dependent Computer Security Complacency: The Unrecognized Insider Threat. IEEE Transactions on Engineering Management, 69(6), 3814–3825. https://doi.org/10.1109/TEM.2021.3058344

Sticha, P., & Axelrad, E. (2016). Using dynamic models to support inferences of insider threat risk. *Computational & Mathematical Organization Theory, 22(3), 350–381*. https://doi.org/10.1007/s10588-016-9209-1

Stróż, P., & Francuz, P. (2017). Event-Related Potential Correlates of Attention to Mediated Message Processing. *Media Psychology*, *20*(2), 291–316. https://doi.org/10.1080/15213269.2016.1160787

Sundararajan, V., & Ghodousi, A. (2021). The Most Common Control Deficiencies in CMMC noncompliant DoD contractors. *ISSA Journal, 19(2), 31–36*. https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=tsh&AN=148533292&site=eds-live&scope=site

Tahira, M., Slaeem, R., & Haider, G. (2020). Government Special Education's Principals' Perceptions about Total Quality Management (TQM in Education): A Qualitative Research. *International Journal of Curriculum and Instruction, 12*(2), 149–163

Tan, S., Na, J., & Duraisamy, S. (2019). Unified Psycholinguistic Framework: An Unobtrusive Psychological Analysis Approach towards Insider Threat Prevention and Detection. *Journal of Information Science Theory and Practice, 7(1), 52–71*. https://doi.org/10.1633/JISTaP.2019.7.1.5

Theofanidis, D., & Fountouki, A. (2018). Limitations and Delimitations in the Research Process. *Perioperative Nursing, 7(3), 155–163*. https://doi.org/10.5281/zenodo.2552022

Tibor, H., & Lajos, H. I. (2020). Major Issues of Insider Threat and Attack Based on Lessons Learned in the Area of Operations. *Revista Academiei Forţelor Terestre, 25(2), 108–114*. https://doi.org/10.2478/raft-2020-0013

Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017). Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. *arXiv preprint*. arXiv:1710.00811

Tuval-Mashiach, R. (2021). Is replication relevant for qualitative research? *Qualitative Psychology, 8(3), 365–377*. https://doi.org/10.1037/qup0000217

van Kemenade, E. (2022). Patterns emerging from the TQM paradigm in relation to the 21st century complex context within TQM journal. *The TQM Journal*, *34*(3), 494–514. https://doi.org/10.1108/TQM-01-2021-0003

van Rijnsoever, F. J. (2017). (I Can't Get No) Saturation: A simulation and guidelines for sample sizes in qualitative research. *PLoS ONE, 12(7), 1–17*. https://doi.org/10.1371/journal.pone.0181689

Vianello, M., Galliani, E. M., & Haidt, J. (2010). Elevation at work: the effects of leaders' moral excellence. *Journal of Positive Psychology, 5*(5), 390–411. https://doi.org/10.1080/17439760.2010.516764

Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers & Security, 106*. https://doi.org/10.1016/j.cose.2021.102309

Wang, Z., Yu, P., & Zhang, H. (2023). Privacy-Preserving Regulation Capacity Evaluation for HVAC Systems in Heterogeneous Buildings Based on Federated Learning and Transfer Learning. IEEE Transactions on Smart Grid, Smart Grid, IEEE Transactions on, IEEE Trans. *Smart Grid, 14(5), 3535–3549*. https://doi.org/10.1109/TSG.2022.3231592

Weissmann, M., Björkqvist, J., & Wiklund, P. (2022). Staff Rides as a Pedagogical Tool in Professional Military Education (PME): Planning and Conducting Historical Staff Rides. *Journal on Baltic Security, 8(2), 61–82*. https://doi.org/10.57767/jobs_2022_0014

Wescott, C. G. (2020). Dark mirror: Edward Snowden and the american surveillance state. *Governance, 33(4), 976–979*. https://doi.org/10.1111/gove.12537

Whitty, M. T. (2021). Developing a conceptual model for insider threat. *Journal of Management & Organization, 27(5), 911–929*. https://doi.org/10.1017/jmo.2018.57

Winkel, A. F. (2019). Every doctor needs a wife: An old adage worth reexamining. *Perspectives on Medical Education, 8(2), 101-106*.DOI: https://doi.org/10.1007/S40037-019-0502-9

Yığ, K. G. (2022). Research trends in mathematics education: A quantitative content analysis of major journals 2017-2021. *Journal of Pedagogical Research, 6(3), 137–153*. https://doi.org/10.33902/JPR.202215529

Yu, G. J., Park, M., & Hong, K. H. (2020). A strategy perspective on total quality management. *Total Quality Management & Business Excellence, 31(1/2), 68–81*. https://doi.org/10.1080/14783363.2017.1412256

Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. *Computers & Security, 104.* https://doi-org.ezp.waldenulibrary.org/10.1016/j.cose.2021.102221

Zaitsev, A. S., & Malyuk, A. A. (2016). Development of Information Security Insider Threat Classification Using Incident Clustering. *Bezopasnost' Informacionnyh Tehnologij, 23(3), 20–29*. https://doaj.org/article/eec2762710b54969bb54c1be8938ae28

Zeng, L., Hu, Y., Lu, C., & Pan, L. (2023). Performance evaluation of lithium battery pack based on MATLAB simulation with lumped parameter thermal model.

Energy Science & Engineering, 11(7), 2614–2629.

https://doi.org/10.1002/ese3.1477