11-24-2023

Data Security Strategies for Preventing Breaches Due to Insider Threats

Ojodale Achor
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Ojodale Achor

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. Cheryl Waters, Committee Chairperson, Information Technology Faculty
Dr. Donald Carpenter, Committee Member, Information Technology Faculty

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

Walden University
2023

Abstract

Data Security Strategies for Preventing Breaches Due to Insider Threats

by

Ojodale Achor

MS in Information Technology, Anglia Ruskin University (2016)

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

November 2023

Abstract

Banking insider threats have been on the rise over the past decade. Information technology (IT) leaders in banks are concerned about the impact of insider threats because most of these attacks have been carried out by individuals accessing business-sensitive data, which, if exposed, could have severe business consequences. Grounded in actor-network theory, the purpose of this pragmatic inquiry study was to explore the security strategies used by IT security managers in banking industries to prevent breaches due to insider threats. Participants were six IT security managers in the banking industry in southeastern Canada who implemented security strategies to prevent insider threats. Data were collected using semi-structured in-person interviews, field notes, industry documents, security archival records and other publicly available security documents. Using thematic analysis, six themes were identified: (a) the need for security standards, procedures, and policies, (b) need for information security education and training, (c) importance of organizational security culture, (d) importance of asset management, (e) importance of identity and access management, and (f) importance of data security. A major recommendation is for IT leaders to invest more in security controls and integrate people, processes and technologies while creating a security culture within banks to help detect and prevent insider threat attacks. The implications for positive social change include the potential to improve security awareness, reduce maliciousness, and compliance with standards and procedures to prevent breaches, which may improve customer confidence in banking.

Data Security Strategies for Preventing Breaches Due to Insider Threats

by

Ojodale Achor

MS in Information Technology, Anglia Ruskin University (2016)

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

November 2023

Dedication

I thank God for giving me strength, wisdom, and guidance throughout this study. I dedicate this study to my late father, hero, and role model, Mr. Pius Achor, for everything I learned directly and indirectly from him that made me who I am today. Also, I would like to dedicate this study to my late mother, Mrs. Margret Achor, who believed in me and inspired me to take on this journey. I am also grateful to my family, who supported and motivated me throughout my study and the entire period of my doctoral journey. Also, I would like to thank my manager, Lee Perdue, for his support and for constantly checking up on me during my research journey.

Furthermore, I would like to thank all my brothers and sisters for their encouragement and belief in me. Your kind words and motivation during my journey helped me push on despite all odds. Also, thank you to my colleague Anthony Figueredo for always looking out for me. I was incredibly motivated by all your kind words during my study. I want to thank my Vice President/CISO, Octavia Howell, for her guidance and professional support for my entire study period. I want to thank everyone who contributed in one way or another during my journey. Finally, I would like to dedicate this work to God. Thank you, Lord!

Acknowledgements

I want to acknowledge all the efforts and dedication of my chair, Dr. Cheryl Waters, for her mentorship and commitment to my study throughout the research process. Dr. Waters provided such guidance that accelerated my learning throughout the research process. All your feedback was professional and incredibly constructive. They helped me see my research study from a better viewpoint. You carefully and professionally addressed all areas that created a better perspective of my study. I want to thank Dr. Carpenter, my second committee member, for all the feedback and references to the standards and guidelines for my study. You ensured that my study met the university guidelines for doctoral research. Also, I would like to thank Dr. Patrick Mensah, the URR Reviewer, for all your feedback that helped me meet the requirements for a doctoral study. This achievement may not have been possible without your contributions to my study. Thank you to Dr. Kayode Alawonde for encouraging and inspiring me while providing professional guidance during my studies. I would also like to thank my colleague Thomas Faulk, who introduced me to Walden University and encouraged me to start this program. I thank you for your encouragement and all the inspiration during my study. I want to thank my friend and colleague Akinfe Oluwafemi for all his professional contributions to this study. I want to thank my grade six teachers, Mrs. Iyabo Agboola and Imam Salihu Adeboaji, who have always believed in me since childhood. You gave me the encouragement and confidence to dream big. I am grateful. Finally, I thank Dr. Gail Miles for her excellent leadership and kind words. Your kind words came at the most critical point during my study when I almost gave up.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Insider threats are a significant concern for organizations. Statistics show that breaches due to insider threats increased as motivations varied. Insider threats can be due to intentional and unintentional acts of employees or third-party vendors with privileged insider information. This risk could be caused by users falling for a phishing attack or employees clicking on malicious links (Abulencia, 2021). Insider threats can be damaging to organizations, especially when the victim or malicious actor has privileged access to the network. Other forms of insider threat could come from disgruntled employees who may want to steal sensitive business data or damage systems in order to damage the organization's reputation. The financial sector is among the most hit by cyberattacks because the recovery cost for financial institutions is among the most expensive for industries globally. Attackers are motivated to attack financial assets or personal information from banks and other financial institutions.

Background of the Problem

The advent of technology has improved company performance and productivity. As a result, an organization's security posture depends on how well people, technology, and processes integrate. People now have access to various tools that include sensitive organizational and customer data. This access to data, if not controlled, may expose organizations to risks due to insider threats. Jeong and Zo (2021) explained that insider threats significantly impact businesses, and 68% of businesses are vulnerable, while 52% of all businesses find it more challenging to cope with insider threats than external

attacks. Most security strategies involve perimeter security and threats outside the boundaries rather than detecting insider data misuse (Hurst et al., 2022).

Although insider threats have been increasing recently, Yuan and Wu (2021) argued that most businesses are still less prepared to differentiate behaviors of malicious insiders from regular users. According to Abulencia (2021), human factors contribute to the reasons for most security threats. Hard-form techniques such as access restrictions and email monitoring could make employees feel their privacy has been invaded (Jeong & Zo, 2021). Privacy is a growing concern for organizations (Jofre et al., 2021). Wei et al. (2021) claimed this could be due to concealment and complexity in terms of malicious intentions of insiders. However, this technique could produce an effect contrary to the intended objective. There is a need for adequate security strategies in order to detect and prevent threats from insiders due to intentional or unintentional actions.

Problem Statement

Organizations suffer significant losses due to insider threats because malicious insiders already have broad access to sensitive data. Insider threat attacks are difficult to detect (Yuan & Wu, 2021). In 2019, there was a 26% increase in security breaches compared to previous years, of which 48% were due to insider threats (Bulpett, 2020). The general IT problem is that some banks' security programs can potentially be exposed to insider threats involving protecting sensitive customers and organizational data. The specific IT problem is that some IT security managers in the banking industry lack proper strategies to implement secure procedures in order to protect sensitive customers and organizational data from insider threats.

Purpose Statement

The purpose of this qualitative pragmatic inquiry study was to explore effectiveness of the security strategies that IT security managers use in the banking industry in order to implement secure procedures to protect customer and organizational data from breaches due to insider threats. The population was IT security managers in the banking industry in southeastern Canada who were aiming to improve their data security strategies. An implication for positive change is that the results may provide banks with a new understanding of secure processes that may prompt policy and strategy changes involving protecting data from insider threats. This study may contribute to positive social change by creating security awareness for banks and reducing employee ignorance and maliciousness while ensuring compliance with standards and procedures in order to prevent breaches which may improve customers’ confidence in banking as well as

other related benefits

Nature of the Study

I chose a qualitative research method for this research study. This was used to isolate specific strategies and provide insights regarding strategies used by IT security managers to prevent insider threats in the banking industry. Qualitative methods involve developing a subjective view of a population's behavior because via complex questions about how and why implementing best practices efforts may succeed or fail (Hamilton & Finley, 2019). Quantitative research methods involve collecting data through surveys and polls and statistical analysis as well as evaluating the relationships between variables and validating hypotheses (Smith & Hasan, 2020). Because there was no need to validate a hypothesis in this study, a quantitative method was not used. Mixed methods involve integrating qualitative and quantitative approaches in order to reveal patterns of evolution and contextual variables that influence the changing patterns (Nunfam, 2021). This study involved exploring participants' views regarding security strategies rather than statistics, so mixed methods were not suitable.

The pragmatic qualitative inquiry design method was suitable for this study because it aligned with the research question. This design is used to isolate and address specific issues (Ramanadhan et al., 2021). I used this method to evaluate how IT security managers implement IT security strategies in the banking industry in order to prevent data breaches due to malicious insiders. The qualitative method was used to address participant's experiences and prepare detailed reports concerning the phenomenon. I used qualitative methods to explore the security strategies used in banking industries in order

to help understand the human element in security and how strategies can help prevent insider threats. The ethnography design is used to investigate and understand the culture of a group of individuals. (Thelwall & Nevill, 2021). Because this design was intended to explain something other than the culture, this design was inappropriate for this study. Also, the phenomenological design was not chosen because I did not intend to explore how the participants lived through their experiences. Phenomenology involves explaining how participants are guided by a phenomenon (Thelwall & Nevill, 2021). The narrative design aims to create thoughts through the various responses from the interview and conclude with stories with life meanings.

Research Question

What data protection strategies do IT security managers in the banking industry use to prevent data breaches due to insider threats?

Interview Questions

I conducted semi-structured interviews with participants to explore data security management strategies they used to minimize breaches due to inside threats in the banking industry. Open-ended interview questions were used to capture all necessary information from the participants.

1. What security strategies do you use to protect data and prevent breaches due to insider threats?
2. What strategies have you developed to analyze user behaviors in order to prevent data breaches?

3. What strategies have you implemented to detect and respond to security incidents that could result in a data breach?
4. What strategies do you use for risk identification and assessment to detect the possibility of a data breach?
5. Which data security management strategies best fits your business requirements and why?
6. What factors within and outside your organization determine what security strategies to implement?
7. What notification approach do you use should a breach occur?
8. To prevent data breaches, what strategies do you use for third-party and vendor management?
9. What programs do you use to help staff understand their security responsibilities?
10. What programs do you use to keep your security team updated with current security events?
11. What strategies do you use to establish security baselines, and how often are these baselines reviewed?
12. What security breach incidents have you experienced due to insider threats?
13. What additional security strategies can you provide as a conclusion for this interview?

Conceptual Framework

To explore the security strategies used by IT security managers in the banking industry to prevent breaches from insider threats, the actor-network theory (ANT) was adopted as the conceptual framework. The ANT is a framework for understanding how humans interact with inanimate objects. This theory is used to understand reality's complexity and technology's role in this context. According to Pollack and Clegg **(**2023), the fundamental concept of the theorist is centered around the interactions between humans (actors) and inanimate (actant) entities. For this study, the theory was adopted to explore interactions between the actor (IT security managers) and actant (data security strategies) within the environment (banking industry) to improve data protection strategies and prevent breaches due to insider threats.

Shaikh and Siponen (2023) argued organizational data breaches are signs of systemic issues, often due to a lack of understanding of various actors' complex interactions and relationships. Distinct entities that are both human and inanimate interact as networked systems to form a singular entity (Müller & Richmond, 2023). This theory is used to provide a broad view of the role of technology in terms of creating social processes. The research study provided a deeper insight into how employees' behavior could influence collaboration in the workplace. The theory aligns with the purpose of this study because it identified the actors (IT security managers) and actants (data security strategies) in an interaction that aims to enhance data security and prevent breaches due to insider threats.

Definition of Terms

Actors and actants: These elements can bend space around themselves and ensure that others depend on them in the interaction process (Chen & Wu, 2021).

Data loss prevention: This involves detecting sensitive data and ensuring users do not send it outside the corporate network. It is a strategy for ensuring that individuals only have access to the data they need (Montano et al., 2022).

Insider threat: Risks posed by individuals with privileged access to sensitive data within the organization (Manral & Somani., 2021).

Identity and access management: Defining and managing user roles and entitlements (Puchta et al., 2019).

User and entity behavior analysis: A security process that involves analyzing normal user activities and detecting behavioral anomalies (Yousef & Jazzar, 2021).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are critical and transferable premises that are taken to be true without proof they are real but reduce future odds that could be determined (Rademacher & Wagner, 2020). Based on specific criteria, I assumed participants had the required knowledge on the subject to respond to the interview questions.

I assumed participants participated willfully and provided honest answers to interview questions that were sufficient to determine the validity of research findings. I assumed research outcomes would be implementable and organization-agnostic, and could guide security strategies irrespective of the bank or financial institution.

Limitations

Limitations are constraints that could impact the study by limiting the scope of research outcomes and may be outside the researcher's control (Lecocq et al., 2019). Although limitations may not be intentional, they are weaknesses and could threaten the study's validity. Chang et al. (2020) emphasized research studies in IT may have limitations. One limitation of this pragmatic qualitative inquiry study was that study's outcomes may not be transferable to all financial institutions in Canada because this study explored security strategies in banks. Another limitation of this study was the sample population of security administrators and security architects who had knowledge and experiences to answer the interview questions on data protection and management strategies. This sample size may not represent the required population that is responsible for implementing security strategies in banks. The willingness of participants to disclose security breaches they had experienced within the bank may not represent the data collected on the specific theme or topic.

Delimitations

Delimitation are factors and other variables that could influence the scope of the study (Bergström et al., 2019). The location for the research was southeastern Canada specifically financial institutions within this setting. I focused on the security strategies used by IT security managers in banking industry to reduce breaches due to insider threats. Another delimitation for this study is that the participants were IT security managers with at least 5 years of experience in implementing data security strategies. The reasons why these strategies are applied are outside the scope of the study.

Significance of the Study

Contribution to IT Practice

This study is significant in that it will lead to improved security controls against insider threats which may reduce losses to the businesses and contribute to the industry's body of knowledge. Adequate data security allows companies to innovate, driving revenue growth, profit, and overall business effectiveness. Cybersecurity breaches can significantly impact business operations, brand reputation, and clientele. There are increasing concerns that security breaches occur more frequently due to technology integrations with business processes. However, improving the business security postures may positively impact their financial dispositions and overall business effectiveness. Improved security strategies may provide digital protections for the businesses and their employees from insider threats. Findings of this study may provide information for enhancing the security strategies required to prevent breaches that could result from employees and contractors with access to sensitive customer and organization data. Improved security strategies may improve business effectiveness, reputation, and customer confidence.

Implications for Social Change

Data protection involves safeguarding business-critical assets, personally identifiable information, intellectual properties, and financial data. Society is more reliant on technology, making it more prone to identity theft because individual and organizational sensitive data are now stored in the public cloud. Also, the advent of intelligent devices has brought about security threats, increasing the security landscape.

The Canadian government has recently paid more attention to cybercrimes because of increased reputational and financial damage to businesses and government infrastructure. As a result, organizations are required to comply with specific security practices. However, businesses need to ensure their employees have the necessary security awareness education to help mitigate threats. Findings of this study may lead to social change by providing banks a new understanding of secure processes that may prompt policy and strategy changes in order to protect data from insider threats. Results of this study may contribute to positive social change by creating security awareness and reducing employee ignorance and maliciousness while ensuring compliance with standards and procedures to prevent breaches which may improve customers' confidence in banking and other related benefits of safe banking activities.

A Review of the Professional and Academic Literature

This study involved exploring security strategies IT security managers use in the banking industry to implement secure procedures which protect customer and organizational data from breaches due to insider threats. Previous research studies emphasized financial implication of security breaches to organizations. However, there are other risks to the competitive advantage, performance and reputation of the businesses and their products apart from financial risks due to the exposure of sensitive data resulting from a security breach (Cross et al., 2019). Organizations must understand behavioral anomalies of privileged insiders that could result in a data breaches. This study may influence policies and strategy changes and ensure IT security managers

implement secure procedures in order to prevent data breaches caused by employees and contractors who have privileged access to sensitive organizational and customer data.

The purpose of this literature review was to understand strategies for protecting data from security breaches that can be caused by insiders within organization. Insiders are employees or contractors of an organization who are privy to data or information that is unavailable to others. My literature review included peer-reviewed articles on qualitative, mixed-method, and quantitative research studies. Also, I used literature maps to explore the research topics by outlining the study summaries. Literature maps connect identified subjects and research gaps by providing an overall view of the content of the research topic (Despujol et al., 2022). For the literature review, y strategy was to identify necessary keywords and concepts, search online databases for peer-reviewed articles with the relevant keywords, review and limit relevant documents to keep focused on the study within the intended research topic, check the credibility of the selected materials, check any recent development in the industry, and conduct and organize the literature review

Literature Search

The literature search for this article was conducted using the Walden University Library. The specified research topic was strategies required to prevent breaches due to insider threats.

This literature review involved relevant articles involving this topic and strategies for preventing data breaches due to insider threats. I also addressed future concerns or research questions that would come up in future studies. Security concerns involving user policies, procedures, security awareness, behavior analysis, privilege access, data security

and other identity and access management concerns such as privilege escalations and separation of duties were explored in this review. I used the following search terms: *security threats, insider threats, banking, financial organization, online application, data protection, data loss, security policies, security risk, data loss prevention, user behavior analysis, data breaches review, PCI-DSS and related regulations, security awareness, anomaly, security incident, banking application, online banking, regulations, security, hacking, financial loss*.

I gathered relevant information from the Walden University Library and the following databases: Science Direct, ProQuest database, Google Scholar, EBSCOhost, ProQuest, and SAGE Journals. For this literature search, I explored the security strategies of banking industries and used the ANT to develop security strategies that IT security managers can use to prevent data breaches due to insider threats. During the literature search for sources, 352 references were found of which 266 peer-reviewed sources were used for this study as references. 81% of the 266 sources were published between 2019 and 2023.

Review of the ANT

I used the ANT as the conceptual framework of the study. The ANT was collaboratively developed by Latour (1997), and Callon and Law (1997) to provide a framework for understanding how humans interact with inanimate objects. This theory explains the translation between the actors and the actants using technology and sociology of science. Human and non-human entities coexist to create an integrated system and emerge as one entity (Latour, 2011). The ANT theory involves interactivity

between the human (actors) and the non-human (actant) (Thumlert et al., 2015; Walls, 2015). The ANT as a framework had applications in earlier sociology and technology research. Al-Mhiqani et al. (2022) argued getting most appropriate solution for insider threat detection is a concern in the banking industry. Also, insider threats for most organizations burden their information security programs because of the difficulty in detection (AlSlaiman et al., 2023). Attacks from malicious insiders are often challenging to detect with traditional tools (Daubner et al., 2023).

Managers can use the ANT to acknowledge the role of a particular actant in the system and how interactions between actors and actants can build resilience. Specific characteristics of the ANT can be symmetric by treating actors and actants as the same. All human and non-human elements of the ANT framework can be perceived as equivalent (Kurokawa et al., 2017). Application of the ANT is also relevant in Information Systems. Mähring et al. (2004) explained the ANT framework is a tool that provides researchers with deeper insights regarding concepts and assumptions about a specific phenomenon.

Researchers use the ANT framework to explore the interactions within a heterogenous network and how outcomes are influenced to determine user behaviors in systems (Montenegro & Bulgacov, 2014). The ANT can also be used to understand behaviors of contractors with access to sensitive business and customer data. For this study, an insider is any employee or contractor with access to business-sensitive data. The ANT involves agnosticism, symmetry, and free collaboration as its central tenets. Agnosticism involves eliminating preconceptions or premeditated notions within systems

(Law, 1986). Symmetry involves non-human elements (IT security strategy, processes, procedures, tools) and human elements actors (IT security managers, IT security architects and administrators) who are integrated within systems. Free collaboration is the associations between human and non-human elements (Law, 1986). Understanding interactions between actors and actants could help in terms of identifying security gaps and their causes within a project (Law, 1986).

Development of IT security engagement and projects within organizations involve many actors, including project managers, security managers, security architects, security administrators, contractors, and other IT leaders. Nonhuman elements include security strategies, tools, policies and procedures, and processes. End users, stakeholders, IT leaders and employees are other actors within the IT security engagement (Marcon Nora et al., 2023). The ANT was used as a framework to describe the socio-technological collaboration of system components in the context of data protection. The ANT is used to simplify concepts involved with investigating security tools and data as actors. Issues involving governance, stakeholder engagement, monitoring and controls were related to data security.

According to Dawson and Jöns (2018), the ANT is used to demonstrate how inanimate objects and technology shape human interactions and enhance the balance of social structures that guide human practices. The ANT compensates for deviations involving the beginning of IT security process development and completion of security awareness training programs for users (Redman-Maclaren et al., 2014). Level of security

awareness promotes level of security controls in an organization (Erendor & Yildirim, 2022).

There are grey areas that must be addressed involving solving ethical issues around data privacy and security breaches relating to emerging technologies (Dhirani et al., 2023). The ANT framework provides simplicity in conceptualized findings in information technology using statistics as an actor. Burga and Rezania (2017) explained how IT governance, risk, stakeholder management, monitoring, security controls, and compliance interrelate using the concepts of actors and actants.

ANT Implementation Strategies

Information security is becoming more critical and relevant in businesses. Data has become the most critical asset for organizations, and the need to protect this has grown over time. Also, regulatory and compliance obligations have increased organizations' drive for security. However, as digitization of businesses grows, the possibility of human errors leading to security incidents also increases (Abulencia, 2021). Even with the most careful employee, it only takes a slight mistake to cause a security incident. The human element is significant and must be considered in security policies. Kammüller and Kerber (2021) explained policies must be defined to show interactions between human and technical systems. Effective security makes it feasible for organizations to innovate and drive revenue growth and productivity (Lloyd, 2020). In considering business benefits of cyber security for SMEs, security must be driven from the top down by the organization business leaders and senior management (Lloyd, 2020).

IT leaders must redefine how security is viewed to reduce security risk and prevent breaches.

Abulencia (2021) argued the number of security incidents due to human factors would continue to increase, considering recent breaches. This is enough for the businesses to examine all aspects of their security policies. Angafor et al. (2020) argued organizations are concerned with the rise in security breaches and shortage of skilled cybersecurity professionals. Hiring and maintaining cybersecurity professionals is a continuous battle for organizations (Blažič, 2021). Human elements are often seen as afterthoughts or not even considered when developing security policies. As a result, attackers often exploit this to gain unauthorized access to data or steal sensitive information from the organizations. According to Abulencia (2021), insider threats are the most human-related and complex attacks organizations can defend against. Bulpett (2020) explained cyber retaliation, long hours of system downtime, and leaked sensitive data are all consequences of insider threat attacks.

Insider threats could be due to employee mistakes, as vulnerabilities cost the organizations money. Also, insider threats can result from fraud, data leakage, identity theft, and ferocity (Brown et al., 2019). Due to the multiple access points in the networks, visibility into data access becomes difficult for the businesses to maintain (Bulpett, 2020). Also, with the increase in remote working, more businesses are moving their workloads to the cloud. Cloud adoption has increased risks of insider threats to organizations as businesses are now more reliant on their data and IT systems for effectiveness (Connolly & Wall, 2019; Deep et al., 2022). Data theft and leakage is easier

as a result of technology (Elmrabit et al., 2020). According to Das et al., (2021) cybercriminals attack cloud-hosted applications because of the presence of vulnerabilities. As a result, it becomes essential for businesses to ensure that proper users have the right access to information. According to Jaafar et al. (2019), protocol weaknesses provide cyber criminals with opportunities for exploitation by running malicious codes and improved security strategies would enhance data protection and reduce data loss for the businesses.

Actors categorize and enroll other actors using inanimate actors to reinforce their collaboration and values (Thumlert et al., 2015). IT leaders have adopted the ANT to gain insight among stakeholders, primarily when technology drives changes in the business strategies (Thumlert et al., 2015). The ANT can be adopted for non-human elements, as adopted in this study to explore the strategies that IT security managers use to prevent breaches due to insider threats. The term actor as used in this study represented stakeholders such as IT security managers that function within a system. Montenegro and Bulgacov (2014) explained the ANT is essential when exploring the success of small and medium organizations. The non-human elements include but are not limited to the IT security strategies, while the human elements are the IT security managers, Security architects, administrators, and other stakeholders.

The ANT evaluates the collaborations and the reasons for the success or failure of IT security endeavors because it draws a relationship between the people, locations, and objects as it relates to IT security concepts of data, people and policies (Montenegro & Bulgacov, 2015). The interactions that exist between people, processes and technology

within the environment because of the security strategy constitutes the sociological settings (Ghelani, 2022).

ANT Relationship with Information Security Risks

IT leaders are concerned about the rise in security breaches due to insider threats (Jackson, 2015). Therefore, increasing the business investment in data protection would enhance security and reduce costs. Fei et al. (2021) explored how deception attacks tamper with data integrity and the need for strategies to enhance data security and reduce costs due to cyber-attacks. This technique proactively provides extra layers of security to complement traditional security controls (Ge et al., 2021). It was explained that there is a potential harm to consumers when businesses cannot protect their sensitive data. Although, it was argued a hard-form security solution could restrict some levels of personal autonomy, leading employees to violate the security policies. Making the employees feel their privacy is evaded, and they tend to be irresponsible with their actions and commit an insider threat attack. Govender et al. (2021) proposed varied opportunity situations could increase the motivation for maliciousness and attack without necessary controls. Organizations must investigate reducing insider threats as work-from-home culture has become the new norm (Chapman, 2021). Monetary benefits are among the motivations for insider threats, and organizations are looking for ways to reduce emotional stress and satisfy employees' needs to reduce any form of dissatisfaction (Jeong & Zo, 2021).

Despite various approaches analyzed to understand the psychology of insiders, many IT security managers do not have the means to pre-empt these attacks (Yuan &

Wu, 2021). According to Upadhyay and Sampalli (2020), elevated user privileges, among others, could result to a breach of vulnerable and unpatched databases. Also, high-profile data breaches are due to failures by organizations to implement necessary security strategies to address vulnerabilities in their systems and networks. Chapman (2021) argued organizations must implement more stringent network security controls and policies while evaluating the role of the individuals in the network security strategy. Database managers must develop countermeasures and implement security strategies to protect the organization's assets from cybercriminals. Yuan and Wu (2021) argued organizations must not depend only on technology to ensure the security of their sensitive assets and prevent insider threats- but a security framework must also be driven from the top down and enforced across organizations to develop a security-focused culture. Deason et al. (2022) explored how managers can adopt the actor-network theory to understand the role of actants in the network and how interactions with the actors can build resilience. This is beneficial for this study because the strength of employee relationships can improve the adaptive capacity to protect the business asset from malicious insiders.

Iskandarova (2017) explained that the actor-network theory provides cognizance of the intricacy of policies within a network. Using the actor-network theory, Pieters (2011) analyzed trust relationships within the computer sciences context. Other studies have adopted the actor-network theory to explore collaborations, commitment, and trust boundaries to explore the relationships between IT leaders and organizations to minimize project constraints (Mendez et al., 2014; Shahin et al., 2014). Moreso, Kurokawa et al.

(2017) adopted the actor-network theory to examine the cycles in human performance related to guidance, continuation, and stoppage in an enterprise IT environment. A study by Montenegro and Bulgacov (2015), explained the effect of social interactions in financial and political systems and how it contributes to the IT industry enhancement. The actor-network theory was adopted for this study to understand the collaboration between actors (IT security managers) and actants (Security strategies) to explore the risks posed by privileged insiders who may have access to customers and business-sensitive data. An effective risk management program protects the business and its reputation. The actor-network theory helps the business understand actors in risk management (stakeholders, risk managers, security architect, auditors, risk assessors) and actants (IT security strategy, risk management strategy, software) and how they interact to help prevent breaches and provide a competitive edge for the business.

ANT Relationship with Insider Threats Detection

Recently, deep feedforward neural networks, Convolutional Neural Networks (CNN), and Graph Neural Networks (GNN) were proposed for insider threat detection. When a deep learning approach was used, there were challenges relating to the data characteristics from insider threat detection (Yuan & Wu, 2021). Machine learning and deep learning anomaly detection tools and techniques have been developed but unsuitable for insider threat detection because of their unique characteristics and insider threats behaviors (Yuan & Wu, 2021). On the contrary, removing excuses and reducing provocations may not influence an individual's attitude toward preventing security misconduct (Safa et al., 2019). Although it was expected that sanctions, rewards or

incentives would prevent misbehavior if used to motivate users. The reduction in provocations and excuses did not impact the behaviors of an individual toward preventing security misbehaviors (Safa et al., 2019). Aka (2019) addressed concerns around sustainable innovation and how managers can develop this innovation. In another approach, predictive models were implemented using linguistic analysis to obtain the risk level of an employee. Methods were implemented to analyze data using machine learning to detect anomalous emails (Janjua et al., 2020).

Besides technical and cyber approaches, identifying and incorporating insiders' behaviors as insider threat risk indicators is a common challenge. Machine learning with textual analysis showed a significant contribution over the years. Supervised learning can be helpful only when the confirmed response is known because of its classification and regression problem (Janjua et al., 2020). On the contrary, opportunity regulation could cause employees to feel disrespected and justify disgruntled behaviors toward their organizations rather than understanding their moral obligation to protect the organization's assets (Jeong & Zo, 2021).

It is essential to understand the role of insiders in security breaches. Because the human element is considered the weakest link and often the cause of security breaches in many organizations, the chances of a breach increase as the organization grows (Abulencia, 2021). Unfortunately, many security solutions are only focused on the technology rather than the people aspects of security. Despite the increase in breaches and global concerns by organizations about cyber-attacks, only a few publications focus on the user behavioral aspect of insider threats, specifically from the perspective of IT

security managers. Numerous studies dwell on the behaviors of security practitioners to detect and prevent attacks from an external source. Some studies believe that increasing the efforts around controls and risk while reducing the incentives may motivate employees to prevent security incidents in the organization (Safa et al., 2019). Insider threats are among the most challenging risks to defend against as the threats originate from within the organization and, in most cases, are trusted with some elevated privileges. Safa et al. (2019) argued most insider threat incidents are related to employees' intentional and unintentional actions and inactions. Understanding and analyzing the behaviors of employees and contractors with access to sensitive organizational assets would help pre-empt and prevent security breaches before they happen.

Importance of the ANT as a Foundation for this Research

A conceptual framework provides concepts, proposed theories, assumptions and research limitations with expectations and possible outcomes. In other words, conceptual frameworks can be visual diagrams or documented products that provide a narrative of the significant ideas to study (Thomas & Tee, 2022).

The ANT was used as the foundation in this study to explore the strategies IT security managers use to implement secure procedures to protect business and customer data from insider threats. The ANT was a vital part of the foundation of this research study. Previous research has provided value in using the ANT for introducing ideas and major research concepts in translating data security assemblages (Kurokawa et al., 2017). The primary idea of the theory enables researchers to equally evaluate all scientific

claims within the research component as it involves human and non-human elements of the phenomena (Kurokawa et al., 2017). Iyamu and Mgudlwa (2018) argued the ANT simplifies the complex socio-technological aspects between science and technology. Also, adopting the ANT in previous studies provided insight into the interactions between business processes, people, and technology for data protection.

In addition to the benefits, the ANT as a framework is a sociological theory of technology that defines a foundation for IT security researchers to explore various phenomena about human interactions and the environment through technology. Pokorny (2023) used the ANT to assess participants' perspectives in recognizing prior learning (RPL). The ANT is essential as a foundation for this study because it addressed the technical and social components of IT. Most IT studies only extensively deal with technology's social and technical aspects because the researchers are mostly focused on the social aspect (Hanseth et al., 2004). The ANT serves as a bridge for all gaps from the beginning of an IT security project until it is completed, which includes the actor's training, networking components and the project commitment (Redman-Maclaren et al., 2014). IT security managers' collaborations are essential to sustain IT security-based operational projects that address individual behaviors, impact, and collaborations (Hardy et al., 2011). The ANT was relevant for this study because it was adopted in examining how user behaviors could influence secure procedures that could be used to protect data in a consolidated management operations (Redman-Maclaren et al., 2014). Alison et al., 2019 emphasized that user intentions can be influenced, which may result in organizational behavioral changes.

Dumay and Rooney (2016) identified that the actor-network theory emphasizes the relating meanings to procedures and substances, which was essential when considering how user behaviors could influence the organizational culture that could result in insider threats. According to Poornima (2023), the actor-network theory was used as a framework to probe the effectiveness of how financial institutions and asset management companies sell mutual funds. The actor-network theory was used by IT project managers as a theoretical and methodological concept to analyze processes and the interactions between human and non-human project resources (Floricel et al., 2014). Using the actor-network theory, social and technical aspects of interaction can be effectively treated separately (Floricel et al., 2014). I used the actor-network theory as a conceptual framework to explore the security strategies that IT security managers used to prevent breaches due to insider threats. IT security managers can use the actor-network theory to evaluate the risks employees, and contractors pose with access to sensitive customers and business data (Floricel et al., 2014). The IT security managers used the actor-network theory to understand the motivations of malicious insiders and develop security strategies to prevent breaches due to insider threats (Walsham, 1997). The role of technology can also be appreciated by using the actor-network theory (Cresswell et al., 2010). IT security managers used the actor-network theory for risk assessment and evaluation of social aspect of IT security strategies (Cresswell et al., 2010). I used the actor-network theory to evaluate social aspects of IT security strategies and the security breaches due to insider threats.

IT security managers can adopt the actor-network theory to evaluate security risks and breaches (Gunawong & Gao, 2017). In other words, IT security managers can use the ANT framework to perform a security risk assessment of insider threats in organizations (Floricel et al., 2014). Also, IT security managers can use the actor-network theory when dealing with third-party vendors and contractors that may have access to sensitive business and customer data to prevent security breaches (Floricel et al., 2014). According to Monteiro (2000), the ANT is suitable for IT security process evaluations to understand user behaviors and motives for maliciousness. By applying the ANT as a framework for this study, I understood the security strategies that IT security managers used to prevent breaches due to insider threats. IT security managers used the actor-network theory to improve collaboration and build employee trust in order to reduce the risk of security breaches (Floricel et al., 2014). Tortia and Sacchetti (2023) explained that risk management efforts must include both end users and business stakeholders for effectiveness. The actor-network theory can be adopted when analyzing an organization's social aspects of security risks (Pollack et al., 2013). Adopting the ANT, I intended to understand the IT security strategies used by IT security managers to prevent breaches due to insider threats.

Supporting Theories

Moving Target Defenses Theory (MTD). Zhuang et al. (2015) discussed the foundation of MTD theory while developing a relative cybersecurity theory. According to Narayanan et al. (2019), MTD theory applies to real-time attack vectors as a deception to reduce the risk of data integrity attacks. Also, Zhuang et al. (2015) argue MTD theory

would be a game changer in cybersecurity as it proposes a dynamic defense system rather than static defenses. According to MTD theory, the system's objective is to abolish the attacker's opportunity for time, especially in the reconnaissance phase of the attack.

Also, another goal of the theory is to minimize the attack surface. According to Tan et al. (2019), as a game changer, MTD theory circumvents the attacker's mission by ultimately modifying the system vulnerabilities on the network. This theory provided a great alternative to the ANT because it tries to understand the interaction between the attacker and the network resources to reduce the attack surface and prevent security breaches by eliminating the attacker's time edge. Because of the uncertainty of the attack surface, MTD theory becomes difficult to exploit and more resilient to diverse attack forms (Yungaicela-Naula et al., 2022). The framework could limit the effect of an injection attack by reducing the attacker's potential to understand the network environment (Giraldo et al., 2022).

Contrasting Theories

General Systems Theory. Many organizations develop strategies that align with the business functions and objectives to provide a competitive advantage (do Céu Morais Cláudio & Santos, 2023 January). The general systems theory (GST) was introduced by Von Bertalanffy (Turner & Baker, 2019). GST was later developed and revamped by introducing the systems perspective to represent a concept between humans and science. GST as a framework is focused on module interdependence rather than isolations of models. However, there is a gap in that the framework focuses on the system's functions, structure, and process rather than the behaviors or the collaboration between human

actants and nonhuman elements. Although there are several references to the GST, its application would require further testing before they can be used in real-life solutions (Katrakazas et al., 2020)

GST analyzes how user behavior can impact data security because of the interaction between an insider and the actants within the system. GST framework evaluates functions as input with a corresponding output and processes within the system as activities and dynamics. However, user behavior may not necessarily provide input to the system as they may sometimes be premeditations and malicious intentions that could result in insider threats. Although, Machine Learning solutions have been exploited in detecting malicious insiders (Asha et al., 2023), integrating people, technology, and processes by understanding the existing interaction is necessary to develop secure procedures that can prevent insider threats. The ANT framework is distinct in that it is focused on the collaboration and association between the components of a system (Elder-Vass, 2015; Jackson, 2015; Law, 2008). Also, the ANT framework can be adopted in understanding IT security risks to develop processes that can help prevent breaches due to insider threats (Pollack et al., 2013).

Theory of Constraints

The theory of constraints (TOC) was developed by Goldratt and Cox (1984). The postulation of the theory was based on finite programming software for optimizing production systems. Determining the system constraints that could prevent it from achieving the desired goal was one of the primary objectives of the theory. System constraints are system features or components that could impact performance or

objectives (Rand, 2000). According to Goldratt and Cox (1984), the primary aim of the business strategy is to enhance performance and increase productivity over a given period. As a result, the primary step to be considered when adopting this theory is to identify any obstacle that can impact system performance Goldratt and Cox (1984). Most importantly, preventing inertia from becoming a significant constraint after determining a limiting factor is critical for the theory (Ikeziri et al., 2019). Therefore, IT security managers must identify weaknesses in their processes to ensure process improvement and prevent security breaches (Ikeziri et al., 2019).

According to Goldratt and Cox (1984), constraint optimization is vital to effectively exploiting system constraints. In addition, Ikeziri et al. (2019) proposed that IT security managers must focus on identifying and eliminating process bottlenecks that malicious individuals could exploit. IT security managers must ensure process optimization to a level that would provide adequate security awareness as a compensating control for the identified constraints. The effectiveness of the security program of any organization is conditional on its employees' level of security awareness and education (Alshaikh et al., 2021; Bada & Nurse, 2019). Continuous improvement must be ensured to identify process bottlenecks for optimization. Also, organizations must ensure security is built into its products (Díaz et al., 2019). Rand (2000) agreed that the initial constraints might no longer impact the business process after eliminating the bottleneck. IT security managers can adopt the TOC framework to develop management strategies (Nishio et al., 2022). However, da Silva (2022) suggested that TOC framework can be adapted to risk and project schedule management to achieve significant value by using existing project

resources. Project risks and schedule management may not translate to data security during a security project. The TOC framework may be more effective in security project planning rather than security strategy development. The TOC framework can be applied to fast-track schedules and enhance project controls (Steyn, 2002). Therefore, the TOC framework was not suitable for this study as the objective was not to manage project risks, but rather to develop strategies that can be used to prevent security breaches due to insider threats.

Complex Adaptive System Theory

The complex adaptive system (CAS) theory describes the procedures that involve how these agents evolve, and it postulates the origin of quality assurance in the process. This is a natural sciences theory that explains the interactions among agents and how they evolve in a logical manner (Schiffling et al., 2022). The theory provided a valuable tool to understand natural phenomena, such as human responses to situations and problem-solving ability. The CAS theory has been found helpful as a framework when exploring agent threshold and system resilience (Carmichael & Hadzikadic, 2019). The framework explores how agents interact among themselves and their environment to understand their behaviors because of the interaction (Carmichael & Hadzikadic, 2019). The primary idea behind the CAS theory is that system-level features cannot generally be identified for a single entity or individual agent. Hence, the systems must be studied holistically to understand the agents' collective nature and interactions (Rapport et al., 2022).

According to Carmichael and Hadzikadic (2019), complex systems from different platforms may seem different externally but possess similar underlying qualities. For

instance, complex systems from distinct areas showed standard features and effects across domains. In other words, one cause and dynamics from one domain may provide insights into essential properties of other similar features in other domains (Carmichael & Hadzikadic, 2019). The CAS theory can be used in management and social environments where organizations are seen as actors interacting with systems and businesses (Srinivasan & Mukherjee, 2018). The CAS theory is explained as agents and components of dynamic systems that interact in a particular manner (Afzaal & Zafar, 2016). However, social scientists expressed concerns about the actors' enactment in the interaction (Van Brussel et al., 2016). Scholars found the actor-network theory more potent than the CAS theory because it transitions from one state to another (Van Brussel et al., 2016). Therefore, the CAS theory is not suitable for this research. The ANT as a framework aims to understand the interactions between human and non-human entities and the forms they take because of the relationship.

Insider Threats

A business insider is any employee or contractor with privileged access or information about the business. Insider threats are malicious acts of commission or omission by either an employee or contractor of a company. Although insider threats are a significant concern to organizations, malicious insiders still exploit vulnerabilities in systems and processes (Abaid et al., 2023). Identifying the attack patterns of insider threats can be very important in providing the mechanism to combine the different metrics and anomaly features. Insider threats concerns have been persistent over time, and the effectiveness of detection tools has yet to be proven (Erola et al., 2022). Using

tools to detect network anomalies is a common countermeasure for preventing insider threats. However, some user behaviors may not be visible to security tools. For example, security tools may not detect user intentions for maliciousness. Also, malicious employees may use social engineering to gather sensitive data from innocent or careless colleagues to perform an insider attack on an organization. For instance, phishing attacks have become complicated, and it becomes difficult to differentiate a fake email from a genuine one (Binks, 2019).

Erola et al. (2022) proposed that organizations should combine security policies with alerts to detect deviations in user behaviors from the norm to prevent insider threats. Certain behavioral anomalies could indicate an attack (Erola et al., 2022). However, many false positives have been generated as a result. Studies proposed using machine learning (ML) to detect insider threats, of which the choice of the most appropriate class of ML is a significant challenge (Nasser et al., 2022). It is difficult to capture and accurately differentiate between the behavior of a malicious insider and a regular user because of challenges relating to the features of underlying data (Yuan & Wu, 2021). This is mostly attributed to a malicious insider's subtle and adaptive nature. The motivations may vary from one insider to another, but the impact of an insider threat remains enormous to organizations. Insider threats involve theft, data loss or sabotage, which could have reputational, financial, and legal consequences for the organization.

Historically, financial institutions focus more on detecting and mitigating external threats using perimeter security tools like intrusion prevention systems and firewalls (Borenius et al., 2022). However, Eggenschwiler et al. (2016) explained that recent

discussions among business leaders have expanded to include some employees, contractors and vendors that could be trusted to handle sensitive business information. Although awareness of insider threats has increased over the years, more than the response to insider threat management is needed due to a need for understanding of the threat (Eggenschwiler et al., 2016). Safa et al. (2018) explained that motivations and opportunity remain the two major factors to be considered when investigating incidents relating to insider threats.

The outcome of a study on insider threats showed that certain prevention measures, such as expanding the risk and efforts required to commit a crime, reducing incentives, and eliminating excuses, may result in more adoption of unpleasant attitudes that may lead to misbehaviors (Safa et al., 2018). A negative response to misbehaviors could positively influence employees' motives of engagement, which could reduce insider threats within an organization (Safa et al., 2018). Also, Safa et al. (2018) argued organizations would only realize an effective cybersecurity management strategy if it paid attention to the roles of users in the fight against insider threats. Organizations must focus more on user behaviors, intentions and attitudes when developing security strategies to prevent breaches due to insider threats (Safa et al., 2018). In another study, Green et al. (2020) explored victims' financial and emotional experiences due to the impact of identity-based cybercrime. Adding that the psychological effect of identity-based crime is the same as that of other cybercrimes (Green et al., 2020).

According to Zainol et al. (2012), security policies enforcement, new hire enrollment procedure, segregation of duties, and logical and physical access controls

could help mitigate insider threats. Improving the internal control systems may also reduce insider threats with financial motivations (Zainol et al., 2012). Although internal control systems may provide great preventive control against internal threats, more is needed to detect user maliciousness and its act to commit an insider threat attack. Insider threat detection and control should focus on the behavioral aspect of the risks by implementing necessary safeguards on the individual behavior and environment (Rice & Searle, 2022).

Human Element in Security

There are several concerns about the human element in information security and the security challenges they pose. The number of security incidents in the public sector has dramatically increased, with 22% affecting the United Kingdom health industry, of which two-thirds are related to human factor (Evans et al., 2019). Also, Evans et al (2019) mentioned that the human element is considered the weakest link in the cyber chain. According to Holland (2020), technical controls alone cannot address the threats posed by the staff and contractors of an organization, as the cybersecurity landscape no longer has a perimeter. Technology is expected to enable humans to carry out a specific task and, as a result, is driven by people. While these tools can be predictable, the human who controls or uses them may not be predictable.

People are complex because they can make and own their actions and decisions, sometimes good or bad. Also, human beings are prone to making mistakes, and sometimes people make the same mistakes multiple times because of the unpredictability nature of humans. Human errors can be considered the consequence, not the cause of

organizational failures (Evans et al., 2022). Therefore, because it is challenging to prevent people from repeating the same mistakes, security experts consider the human element the weakest link in the cyber chain. Campean (2019) suggested that a human-focused approach to security awareness and training should be explored.

Lin et al. (2022) developed a concept around proactive security behavior to examine the relationship between people's creativity and organizational context to promote involvement and decision-making within IT governance. Lin et al. (2022) concluded that employees of organizations constitute serious security threats because they are often prone to making bad decisions. Previous research explored the motivations and intentions of employees who constitute insider threats using deterrence, prevention, and detection controls. Deterrence and prevention controls would only reduce computer abuse among the staff of an organization (Lin et al., 2022). Also, blame culture is prevalent in organizations without established security controls to mitigate the security challenges caused by human errors, which could result to data breaches (Evans et al., 2022).

Security breaches due to human error significantly impact customers, organizations, employees, vendors, and the public, which may result in financial, legal and reputation consequences (Evans et al., 2022). Cheng and Walton (2019) explained that data breach disclosures have a negative implication on the market shares and the business in general. Also, (Evans et al. (2022) concluded that the number of human errors far exceeds what is reported in recent security literature. One most common causes of human error are the inability to detect and correct these errors, as there are no apparent provisions to reverse an unintended action because people perform repetitive tasks. Also,

cyber-attacks are intended to exploit the human element vulnerability because it is perceived to be the weakest link in the cyber chain (Evans et al., 2022). The human element that interacts with systems must always be considered (Grobler et al., 2021).

It is suggested that employees should have a certain level of security awareness training as a security control. Evans et al. (2022) argue that this suggestion is focused on mitigating intentional attacks that exploit human weakness. However, it is ineffective for an unintentional human mistake which is the cause of most security breaches. Examples of unintentional human error include sharing sensitive data with a third party, accidental data loss, and unauthorized information disclosure. One could think that insider threat motivations are always intentional, but the actions of an insider that could cause harm to the organization can sometimes be accidental (Abulencia, 2021). Organizations must understand user behaviors and implement controls to detect and mitigate anomalies. Haapamäki and Sihvonen (2019) suggested that organizations must implement effective security controls that would protect against unauthorized user access to business-critical data.

Integrating people, process and technology would provide the collaboration required to develop a secure procedure to protect data from security breaches due to insider threats. Abulencia (2021) argued most security incidents occur due to exploitation of the human element vulnerability. Although it may not be realistic to eliminate all the risks relating to human, organizations must take necessary actions to prevent the chances of threats happening (Abulencia, 2021). Abulencia (2021) explained that human factor in

security is critical and should be considered when developing security strategies and policies for an organization.

Banking Industry Security Policies

Financial services providers ensure necessary safeguards and a degree of assurance for transactions and customer accounts (Wodo et al., 2021). Also, regulatory obligations aimed to improve data security and compliance with its requirements (Wodo et al., 2021). Although it is believed that banking operations are easy to commence and available, the risk and security concerns to transactions and customer data may be enormous. From a closer perspective, the entire ecosystem of banking security includes third parties and vendors who may not necessarily be in the banking business (Wodo et al., 2021). According to Ghelani et al. (2022), IT leaders develop cybersecurity strategies to identify and mitigate security risks and threats to sensitive business and customer data. IT leaders must identify what steps to be taken in the event of a security incident and minimize the impact by using the best practice approach to incident management. Vinoth et al. (2022) explained that the banking industries must develop appropriate policies and procedures supporting business objectives and decision-making processes to achieve minimal residual risks. Considering the role of third parties and vendors in the banking space, it is vital to address security concerns in the banking industry from a holistic viewpoint – including all stakeholders, processes and regulations involved in the banking operations.

There is an increasing threat to customer data, posing severe concerns to the current data-driven ecosystem. IT leaders have invested in security systems and training in employee security awareness (Wodo et al., 2021). However, the threat landscape is

evolving with increasing threat actors. Research analysis shows that the rate at which new technologies are implemented supersedes the integration of methods and procedures to safeguard data, and this does not reflect the level of security awareness campaigns required to ensure the secure use of banking services (Wodo et al., 2021). Some challenges with the banking industry include the lack of security controls, poor control objectives, lack of awareness of current threats, lack of security skill set and shortage of staff with an increasing occurrence of security incidents due to employee mistakes.

However, Crumpler and Lewis (2019) suggested that expanding apprenticeship skills to young graduates could be a solution. Thakur and Purandare (2022) reported that 35% of the entire data breaches in recent times target the financial industries. Wodo et al. (2021) explained that human behaviors constitute a significant risk in banking operations, whose effect may increase with interconnectivity and online applications. Banks and other financial industries are significant targets of cyberattacks because of the monetary incentives. According to Ahmad et al. (2020), the threat landscape is evolving, and the threat actors are more organized and sophisticated. The motivation for an attack on banks includes cash benefits, fraud, extortions, and political and ideological consequences.

Security concerns in the financial industries have become more popular as a business concern in recent times, especially in online banking and transaction globalization (Farzan et al., 2013). To effectively mitigate the risks of cyber threats to the banking industries, it is expedient to integrate a robust security framework into its cybersecurity governance strategies (Altaf et al., 2022). Employees and contractors constitute privileged insiders in the banks, and they need to be aware of cybercriminals'

tactics and prepared for the increasing level of attacks (Wodo et al., 2021). IT leaders must ensure they develop a risk management strategy and create a security awareness sufficient to mitigate the increasing level of cyber-attacks in banking industries (Dharmawansa & Madhuwanthi, 2020). According to Lemieux (2015), 21% of account takeover cyber incidents for 2013 were reported, with 9% resulting in a successful fund transfer from the banks.

The banks and their leadership must ensure that they maintain up-to-date industry best practice policies and procedures relating to cybersecurity (Johri & Kumar, 2023). Implementing the security framework is a great idea. However, IT leaders must ensure security policy enforcement and compliance with enterprise security practices and procedures (Kuzminykh et al., 2022). Employees and contractors must enroll in regular information security awareness training to provide the necessary education to build a secure culture that can withstand social engineering and other cyberattacks. A lack of security awareness can result in cyber-attacks in an organization (Alzubaidi, 2021).

Need for Security Awareness and Organizational Readiness

Security awareness provides organizational readiness when dealing with insider threat concerns. Organizational readiness provides the foundation for every organization to address security concerns affecting every segment of the organization (Rodbert, 2020). Employees must understand their roles and how it is vital to the security of the organization's sensitive assets and the overall security-conscious culture (Rodbert, 2020). Most employees in large organizations do not think they are valued as an essential part of the business. It is important to note that when an employee is valued and engaged, it

plays a critical role in the organization's security efforts (Rodbert, 2020). Mittal et al. (2010) explained that organizational security strategies must integrate people, systems, and policies. Therefore, it is essential to integrate technical and non-technical controls and industry best practices to prevent insider threats (Lessa & Gebrehawariat, 2023).

Security awareness provides formal education or training on the various security threats and how they can be recognized and prevented to keep the organization safe. Organizations must build a culture that is security-focused and must be intentional in the enforcement of its security policies. Grassegger and Nedbal (2021) argued that a security awareness program is an essential aspect of an organization and its failure to provide awareness, and other security initiatives may result in security incidents due to user behaviors. The human factor and information security are strongly related and critical factors for every organization as it is considered the weakest link in security (Campean, 2019). User roles must be defined, and every user must understand the business expectations and how their roles can help the organization achieve its objectives. Hart et al. (2020) demonstrated an ideal security policy and how it should assist users in understanding their roles and responsibilities and how they can help protect the organization's information system. A robust security awareness program drives organizational awareness, knowledge, and confidence to identify and respond to security threats. Security awareness programs must reflect the organizational security policies as major risk mitigation and clearly defines acceptable and unacceptable use or behaviors (Hart et al., 2020).

Adequately trained users play a vital role in the organization's security posture and reduce the chances of human errors that could potentially result in a data breach. Organizations must ensure that a security awareness program is an essential aspect of the security framework to minimize the risks of security threats. With the right level of awareness, employees would have the appropriate knowledge of the industry's security best practices and understand the common aspects of social engineering attacks. Security awareness training must be more expansive than existing employees as new hire security education must be mandatory for every new employee to ensure an effective security awareness program. Security awareness programs must ensure that security policies are communicated and enforced. Enforcing a security-conscious culture is an essential aspect of an organization's security strategy to create awareness and help IT security managers understand employee behaviors and how they can impact security procedures within the organization (Bada & Nurse, 2019).

According to Alzubaidi (2021), security awareness programs must be continuously reviewed to assess their effectiveness in minimizing security threats. The policies and procedures developed by organizations should protect their digital assets from threats and vulnerabilities. However, these policies and procedures must be widely accepted within the organization and ensure management involvement to ensure effectiveness (Hu et al., 2012). Employees' noncompliance with security policies and procedures remains a significant risk to the organization. Strategic leadership must coordinate all actions to ensure continuous monitoring and policy enforcement to ensure compliance and reduce the risk due to insider threats (Lehto & Limnéll, 2021). Businesses can mitigate their

security challenges and make their security policies effective when their employees have adequate security awareness training, and the program is implemented to cultivate a security culture (Kurpjuhn, 2019).

Security awareness programs should involve every employee, from top management to users. Tejay and Mohammed (2023) explained that business management with the right security awareness training improves corporate and business efficiency while enhancing technological performance by creating the right attitude and interactions between users and information assets. Security awareness programs in an organization help minimize the risk of security breaches that may result in losing customers and business-sensitive data. An effective security awareness program simulates common security mistakes that employees can make in real-world scenarios to help provide a better understanding of how to identify and prevent them.

Transition and Summary

Section 1 included a discussion of the conceptual framework, significance of the study, literature review and IT security management concepts and themes. Themes include the impact of insider threats and the several industry approaches implemented to prevent these threats. I explained risks of insider threats to the businesses and how they are a significant concern to businesses. The section includes a review of security strategies for preventing insider threats and identifying gaps. Section includes data collection and analysis methods that were used to answer the research question and ensure reliability and validity.

Section 2: The Project

The purpose of this qualitative pragmatic inquiry study was to explore the effectiveness of the security strategies that IT security managers use in the banking industry to implement secure procedures in order to protect customer and organizational data from breaches due to insider threats. The population was IT security managers in the banking industry in southeastern Canada who were aiming to improve their data security strategies. An implication for positive change is that the results of this study may provide a new understanding of secure processes that may prompt policy and strategy changes to protect data from insider threats in the banking industry. The study's outcome may contribute to positive social change by creating security awareness in banks and reducing employee ignorance and maliciousness while ensuring compliance with standards and procedures to prevent breaches which may improve customers' confidence in banking and other related benefits of safe banking activities.

Role of the Researcher

I have been in the IT industry for almost two decades, and I started my career as a network engineer, after which I advanced to a security specialist. Currently, I am a security architect for my organization. In this role, I am responsible for defining security requirements, developing control objectives, and ensuring that the organization’s critical assets have the proper controls. Over the years, I have gained extensive experience involving security practices and implemented several security solutions for my organization. However, I have not had the opportunity to explore or work on security strategies involving insider threat prevention. As a result, I have gained interest in

understanding insider threats, their impact, and how they can be prevented in my organization. The first time I became interested was when working with a real estate investment firm, where I deployed a network admission control system to help detect rogue systems and prevent unauthorized access to the network. This broadened my understanding of security threats and increased my curiosity about the impact an insider threat could have on organizations. Also, I am interested in understanding the strategies used by IT security managers in the banking industry to prevent breaches due to insider threats.

As organizations grow, the tendencies of human-caused security incidents increase because human elements are generally the weakest link in security (Abulencia, 2021). As a result, I decided to research insider threats in financial institutions by understanding the behavior of malicious insiders and the risk to the business. Previous studies suggest that users' personalities can be used to determine if a person would engage in activities that could result in insider threats (Harms et al., 2022). I discovered that some actions of an insider might not be deliberate, but the consequences to the business could be grave. Even with the most security-conscious individuals, a single click or mistake could lead to a severe security incident (Abulencia, 2021).

In qualitative research, the researcher is one of the primary data collection instruments (Wa-Mbaleka, 2020). As the primary data collection instrument and sole researcher, I conducted the study and collected and organized the data. Data collection and analysis go through a modified iteration during qualitative research study (Johnson et al., 2020). Also, I was responsible for data analysis and presentation of findings as well

as eliminating all bias. During the data collection stage, I used an interview protocol, and interviews were conducted until data saturation was achieved. Data saturation is often used for sample size estimation in qualitative research (Guest et al., 2020). In addition to open-ended interview questions, I used observations, field notes, interview transcripts, security documentation and publicly available policy documents. Interviews provide empirical data during the data collection stage of qualitative research (Kaur et al., 2021). To ensure that open-ended questions were free from bias, I ensured that academic peers and committee members reviewed them. Member checking was used to ensure the validity of the results.

As a security architect with almost two decades of experience in IT security, I have been involved in data security projects where I had access to sensitive data. I ensured data were comprehensive enough during analysis by using the same data collection methods for all participants. Equality is achieved, and bias is reduced when the same data collection instrument is used for all participants. I proactively ensured that all bias was eliminated by using peer review.

I also reviewed the Belmont Report from the United States Department of Health and Human Services. The Belmont Report provides principles and guidelines for protecting research study participants (US Department of Health & Human Services, 1979). The Belmont Report was used to address concerns involving regulations and guidelines for protecting research participants (Brothers et al., 2019). I ensured that each participant participated voluntarily with consent and knew they could opt out at any time. I ensured that the participants are respected and that their privacy rights were protected.

To ensure I adhered to ethical processes, I ensured all participants were not from the same locations and did not have any personal relationships with me, either in my current or previous place of work. Results from risk analysis were made available to participants to help them decide to participate in the study.

In addition, I avoided bias during the selection process for the participants by ensuring that selection criteria were based on the knowledge and ability to answer the research questions. Open-ended questions provided the opportunity to ask transitional and followup questions. Data were presented to peers and committee members for review to ensure that bias were eliminated. I ensured that I gained participants' trust by seeking their consent prior to interviews and assuring them their information would be kept confidential and they had the liberty to withdraw at any time. Establishing a good working relationship and gaining participants' confidence during data collection for a research study is vital and ensures the free release of information (Atakav et al., 2020).

Participants

Participants were IT security managers with at least 5 years of experience involving data security strategies used in banking institutions for protecting sensitive data. Participants were selected from the banking industry within southeastern Canada. Participants' experience involved data security as well as IT security principles. All participants successfully implemented security strategies to prevent insider threats, were security managers in the banking industries, located within the southeastern part of Canada and had a minimum of 5 years of experience in IT security. For this research, I used purposive sampling.

I used LinkedIn, seminars and webinars as a means of contacting participants. Social media platforms can be used to reach a wide range of participants, and the number of consent may increase as a result (Protudjer et al., 2023). I gave each participant informed consent and an invitation to participate in the research study. Consent must be willfully given, specific, informed, clear and separated from other terms and conditions (DLA Piper Intelligence**,** 2020). This allows the participants to understand that their participation is voluntary, and they can withdraw their consent at any time (Murry et al., 2023). I made initial contact with the potential participants via their emails and phone calls, after which interested participants were shortlisted. According to Auxier et al. (2019), recruiting research participants can sometimes be challenging because of schedule constraints and participants' availability.

Also, I ensured that I built trust and established a good working relationship with the participants by ensuring they understood the importance of the research while assuring them that their information would be protected during and after the study. Establishing a good working relationship and gaining participants' confidence during data collection for a research study is vital and ensures the free release of data (Atakav et al., 2020). Participants' privacy assurance, data confidentiality and informed consent are essential and must be put into consideration (Aldbis et al., 2023).

Research Method and Design

Research Method

I used the qualitative research methodology, which included a pragmatic qualitative inquiry study. The qualitative research method allows the researcher to explore different strategies used by industry experts for a given phenomenon (Côté-Boileau et al., 2020). According to Cornejo et al. (2023), qualitative methods offer solutions that are suitable for multidimensional investigations and explorations of problems. Qualitative research methods are used to explore problems and provide evidence of the event from the participants' viewpoints and experiences (Saleh et al., 2023). Also, Cornejo et al. (2023) explained that qualitative researchers could build patterns, themes and data categories using inductive reasoning rather than deductive to gain an in-depth understanding of the problem.

I chose the qualitative research method because this study explored and gained a deeper insight into the strategies used by IT security managers to prevent breaches due to insider threats. I did not choose a quantitative study because this research did not intend to understand the relationship between variables or validate the research hypothesis. According to Steils (2021), the quantitative research method uses statistical analysis, surveys, or polls to evaluate the relationship between variables.

This study aimed to understand the collected data from the various participants based on their experiences and perspectives. Because this study did not intend to test theories or utilize numerical measures, I did not use quantitative methods. Quantitative research methods use numerical functions to analyze a research outcome (Côté-Boileau et

al., 2020). Quantitative research was not appropriate for my study because I did not collect numerical data. The mixed methods combine qualitative and quantitative methods. The combination of both qualitative and quantitative methods results in hypothesis formation with minimal theorizing features (Mukumbang, 2023). I did not choose a mixed-method approach because it involves the combination of both qualitative and quantitative methods. For this study, I used data from the participants and rely on their experiences rather than using a combination of statistical data analysis, finite measures, and users' viewpoints. Therefore, the qualitative method was considered the most appropriate for this study.

The data collection technique for this study was based on the participants' responses to the interview questions and the various organizational documents that was provided. Also, qualitative research best uses oral responses from transcribed audio interview outputs, written field notes and other non-verbal sources to explore research phenomena. Therefore, a quantitative research approach would not deliver an in-depth evaluation of the problem statement since I did not use any hypothesis for this research study. The mixed method would also not be suitable for this study because it combines both qualitative and quantitative methods, which would be time-consuming for this research study. Mixed-method research involves the data collection, analysis and integration of qualitative studies and quantitative studies (Guetterman et al., 2019). Because this research study intended to have an in-depth exploration of the problem statement, both quantitative methods and mixed methods was not suitable for this study.

Research Design

This study used a pragmatic inquiry study as a research design. The researcher can evaluate a problem more extensively within its environment when using pragmatic inquiry (Kerins et al., 2019a). A pragmatic qualitative inquiry allowed the researcher to collect data from multiple sources to proffer solutions to the problem. The choice of a pragmatic qualitative inquiry study supported my investigation of different security strategies used by IT security managers in the banking industry and their experiences in implementing the strategies. A pragmatic qualitative inquiry effectively explores phenomena from different participants and analyses real-life scenarios (Agrawal, 2021). The qualitative pragmatic inquiry design was appropriate for this study because it helped to explore and understand the security strategies used by IT security managers to prevent data breaches that could be caused by employees and contractors who have access to banking resources, facilities, and customer data.

IT security managers in the banks were the best participants to help understand the experience and strategies they used in preventing data breaches due to insider threats in the industry. Using the pragmatic qualitative inquiry provided an in-depth understanding of the organization's security strategies, roadmaps, and overall experience from the IT security managers. Pagnini et al. (2021) argued that pragmatic qualitative inquiry provides the opportunity to use multiple approaches when collecting and documenting the participants' experience of specific phenomena. Because the study was validated across various banks, the pragmatic inquiry showed the study's outcome to be transferable within the banking industry.

One of the alternatives considered was a phenomenological and ethnographic research approach. Ethnographic design is dependent on the researcher's ability to understand the culture and social orientation of the people, which can be overwhelming (Ravindran et al., 2020). Also, Côté-Boileau et al. (2020) explained that Ethnography research may require that the researcher observes and understands the research subjects by living or experiencing the participants' environment. This method may itemize areas of strength that can be improved from the participant's experience (Hagues, 2019). Because my research work intends to explore the security strategies used by my participants and not intervene in their situation, I think this approach may not be appropriate for my study. Researchers use the phenomenological approach when trying to understand the perspective and experience of the target population instead of explaining a phenomenon from the participants' experience. Allowing the participants to interpret and attribute meanings to a phenomenon based on their experiences (Frechette et al., 2020). Therefore, this approach was not appropriate for this study. This study aimed to explore and learn from the successful implementation of strategies from the participants' experience and not go over the transition with them.

Another alternative research design considered was narrative. Researchers use this approach to gain insight into the meaning of life through stories (Parks, 2023). However, my research focused on exploring the participants' strategies, so I think this was not appropriate for my study. The descriptive design is suitable for mixed methods or for investigative analysis when gathering data, and there is a need to present a description of a phenomenon (Turale, 2020). The descriptive design was not appropriate for this study

because this research was not to describe events or provide background information about any geographical boundaries but to explore the security strategies used in financial institutions to prevent breaches due to insider threats.

To ensure data validity for this research, I ensured data saturation was achieved. Data saturation is vital in a research study because it ensures that all necessary information is collected and there are no new data that could be important to provide a new theme within the study (Eakin & Gladstone, 2020). I collected data until there was no new available data to achieve data saturation. Achieving data saturation ensured that all essential data elements for the study had been collected and that nothing was left out that are critical to answering the research question (Eakin & Gladstone, 2020). This study ensured data saturation by ensuring that all interview questions were answered by multiple interviewees and that other data sources covered all the possible themes identified in the literature review.

According to Santana-Cordero and Szabó (2019), a researcher must integrate document analysis with interview protocols during exploratory qualitative research. Also, I reviewed field notes to identify if there were concerns raised during the interview. Using multiple data collection tools increases the chance of achieving saturation because the amount of data collected from various perspectives increases (Mwita, 2022). By analyzing the contents of the field notes, the researcher can weigh the benefits and concerns of the research study (Jain, 2021).

Population and Sampling

The population of my study included IT security managers, security architects and security administrators in the banking industry in Toronto, Canada. The selected population for the study had knowledge and experience with information security management strategies. These managers had developed and used security strategies to secure customers' and banks' data from breaches due to insider threats. The participants in this pragmatic qualitative inquiry study were from southeastern Canada. I used purposive sampling to select the research participants because their experience and knowledge were critical to the research study. To deliver the research objective, the researcher must consider the participants' knowledge and skillset using purposive sampling during selection (Walsh et al., 2020). Also, Tuthill et al. (2020) explained that participants' experiences in a phenomenon must be factored in during selection in qualitative research. Using purposive sampling is suitable and helped focus on the banks that had implemented strategies to prevent insider threats which helped answer the research questions for this study.

This study sample population was at least six participants who were solution architects, IT security managers and security administrators. The sample size is essential to ensure the study's validity (Glenton & Carlsen, 2019). All participants met the criteria of six years of minimum experience and knowledge of security management strategies and had worked in the bank for a minimum of three years. According to Etz et al. (2019), adopting expert sampling ensures that subject matter experts are used, which improves triangulation and the study's validity. The selected criteria helped me collect the data

required to answer my research question: What data security and management strategies do IT security managers use to prevent breaches due to insider threats?

I ensured data saturation by comparing the outcomes of the individual interview sessions and document analysis until further data collection was no longer required due to any new data. The same interview questions were used for all the participants to ensure data saturation. Xu and Zammit (2020) emphasized that data saturation is a pivotal aspect of qualitative research. Explaining that the same set of data would be returned to the collection as there would longer be any new data necessary for the research study. Also, I ensured that member checking was done to further ensure the credibility of the study. Researchers in qualitative studies must emphasize on the credibility of the study (Eldh et al., 2020). The data collection, triangulation, all relevant documents, and the number of participants helped ensure data saturation for my study. This study ensured that the interview questions were consistent and the same for all the participants to attain data saturation. Farley (2020) emphasized that researchers may sometimes reach data saturation with the selected sample size. My sample size for this study was at least six participants.

The interview location and mode may affect the quality of the interview and the collected data. Given this, the interviews were set up with each participant via an agreed medium. Arquilla and Guzdial (2020) explained that using virtual conferencing with participants is highly recommended as it convenient. The plan was to interview all participants face to face or via online communication media such as Skype, Zoom or MS Teams. Each interview session took about 30 minutes to 1 hour. If the interview was to

take longer, I ensured the participants take a break to be comfortable. Also, I ensured I conduct a follow-up interview with the participants to achieve member checking. Pessoa et al. (2019) explained that conducting interviews help to understand the participants' viewpoint and experiences on the research questions. Previous participants were interviewed to understand their experiences of the entire process (Bremner, 2020).

Ethical Research

Research ethics is an essential part of any study. Not considering this could result in potential physical, psychological, and social-economic harm to the participants and the researcher (Gelling, 2019). The ethical expectations of a research study are the researcher's responsibility (Cumyn et al., 2019). Ethics is essential to protect the privacy of all the research participants. I have completed the required CITI doctoral training on ethics and protecting human research participants. This helped me conduct the research ethically to prevent harm to the participants from any harm to the privacy and confidentiality of their information (see Appendix A).

I emailed participants a consent form to obtain their informed consent before the interview. A researcher should inform the participants of the procedures and other risks involved in the research study (Tolich, 2019). The informed consent form can be found in Appendix B. In the form, I informed the participants on the process, their roles in the study, the study objectives and how the outcome of the study would be used. The participants were given full disclosure to voluntarily indicate their absolute willingness to participate in the research study based on these conditions. I also informed the

participants in writing and verbally that they could withdraw their consent and willingness to participate or continue in the research at any time.

The consent form clearly stated the research topic, the participant's right to withdraw, the interview process, and any incentives disclosure. I ensured that the participants understand that participating in the research was valuable and can benefit the development of security strategies in the banking industry. Also, I communicated both in writing and verbally to the participants that their participation in this study did not include any financial incentives. Noting that financial rewards could compensate for the participants' time and efforts, it could also be seen as creating an undue influence or coercion (Zapata-Barrero & Yalaz, 2020).

I assured the participants of the privacy and confidentiality of any information they provide or were collected during the research, including names and other data. Privacy protection was ensured in the interview protocol. The participants were in a location, preferably away from their office, where their communication was not overheard or interrupted by anyone. Trust is built when the participants are assured that their information would be preserved and confidential (Gelling, 2019). Assuring the participants of the confidentiality of their information could guarantee the authenticity of the participants' statements (Surmiak et al., 2022). As a result, participants' information was protected using anonymization. The anonymization process was done by representing participants' information with some codes so they cannot be used to identify any participants. Unauthorized access to participants' personal information could significantly impact their reputation and ability to move on (Brimblecombe, 2020).

In addition, all the data collected from the participants was encrypted using the Bitdefender full-disk encryption solution. All files and data were stored in the cloud and would be destroyed after five years.

Data Collection

Instruments

This study aims to explore the strategies used by IT security managers to prevent breaches that can be caused by employees and contractors that have access to customers' and banks' sensitive data. I am the primary data collection instrument for this qualitative research. As the primary data collection instrument, I used an interview protocol with semi-structured in-person interviews using open-ended questions, field notes, industry documents, security archival records and other publicly available security documents. Using a traditional structured interview does not give the participants the opportunity to tell all the story from their experiences (Goopy & Kassan, 2019). Interviews are considered an essential data collection instrument for the researcher to collect comprehensive information about the experience and skill set of the participants (Jones et al., 2019). I conducted a semi-structured interview as specified in the interview protocol in Appendix C. The data collected from the interview, field notes and industry documents were kept confidential using the NVivo coding approach.

The interview duration was 30 to 60 minutes at a time convenient and agreed upon by the participants. I supported the interview data with field notes and evaluation of at least 10 security-related documents and archival records in the organization. The researcher combines interview protocol with observations to answer the research

questions (Roberts, 2020). Also, a semi-structured interview allows the researcher to ask follow-up questions to better under the participant's experience (Macias & Contreras, 2019). I ensured that the participants consent and know that the interview session would be recorded before the interview. This allowed the review of the recorded script to understand the discussion better.

Researchers use multiple data sources for triangulation to increase the study's validity, credibility, and reliability (Lemon & Hayes, 2020). This approach helped mitigate all biases to increase the validity of the study's outcome. Also, researchers may use semi-structured interviews and probing to understand the participants' perspectives and experiences (Brawn & Clarke, 2019). The interview strategy was to gain the participants' trust using open-ended questions. Each participant was to answer 13 open-ended questions freely. By using open-ended questions, the researcher built a rapport with the respondents, which helped expand their responses and provided a more helpful understanding of the research questions.

Member checking was done by following up with the individual participants and having them verify all information collected during the interview to ensure data accuracy. Member checking is essential in a study to provide credibility and validity (Candela, 2019). Member checking ensures the integrity of the research process by sharing the data collected during interviews with the participants to ensure it resonates with their experiences (Brear, 2019). Internal information security documents were reviewed as the secondary data source. These documents include policies and procedures, archival

records, and other publicly available documents. The secondary data supported the data validation of the primary data collected during research and ensured its triangulation.

Data Collection Technique

The data collection entails conducting semi-structured interviews, using field notes, and analyzing documents. This process included the participants' identification and selection, sending out the informed consent form, performing the interview, member checking and ensuring triangulation in the study. Using an interview protocol allows the researcher to collect meaningful information and participant experiences regarding the research problem (Naeem & Ozuem, 2021). I commenced the data collection phase for this research after obtaining the Walden University Institutional Review Board (IRB) approval. IRB approval is a requirement for all research that involves human and animal participants (DiGiacinto, 2019). The primary data collection for this research was from the interview I conducted with the participating security managers, architects and CISOs from various financial institutions. I formally invited the prospective participants by email (See Appendix D). The interviews helped to have a deeper understanding of the experiences of the IT security managers and other participants. The participants were expected to answer the research question as they reflected on their experience and skill (Hamilton & Finley, 2019). A semi-structured interview was used, and the interview discussions were recorded using the audacity application. Before the interview sessions, the participants received a consent form via email to help them provide their consent and understand that they could withdraw at any time during the research.

On the interview day, I arrived early to test the audacity application for audio quality and to see if the application would function as expected. The interview was conducted for each participant at their convenient time and location or via Skype, Zoom, Teams or Google Meet. The data that was collected was transcribed after the interview. Also, I took field notes as part of the data collection process. I used the field notes to confirm what was discussed during the interview session and asked the participants for clarity should there be any deviation. I conducted member checking to ensure the consistency and accuracy of the interview transcripts. Member checking ensures that the researcher follows up with the participants to validate the data collected (Caretta & Perez, 2019).

I contacted the participants to collect industry policy documents, archival records, and other operational documents related to the research study. The documents were reviewed as part of the data analysis process. I collected additional documents from public websites such as banks, government websites and other regulators' websites and ensure they were reviewed before and after the interview.

Data Organization Techniques

Researchers use various approaches during the data organization stage to organize the identified materials from the field (Champagne-Poirier et al., 2021). Files from each organization were stored in electronic format in separate folders to allow for easy identification. Also, the audio files, transcript and soft copies of other secondary data collected were included in the folders. Hardcopy documents that were scanned due to various constraints were kept safely in individual document files and labelled according

to the organization. The document files were securely locked in a safe and would be returned to the participants after completing the research. Researchers must develop techniques to provide a detailed outcome that would account for missing data within a specific data set (Chan et al., 2020). As a result, I ensured that I accounted for every question the participants did not answer due to nondisclosure or information sensitivity. I assessed the impact level of every missing data within the study.

Managing data in research is essential for the success of the research and must be kept securely for the entire period and disposed of afterwards (Kavitha et al., 2022). Chauvette et al. (2019) explained that the current technological advancement has made it convenient and possible to store and reuse data and other digital content over a period. Organizing qualitative data in a single repository is essential for proper coding, labelling, theming, and data categorization within the same platform (Al-Eisawi, 2022). The data collected for this study were encrypted with the Bitdefender full-disk encryption solution. The data collected would be retained for a maximum of 5years in a locked file cabinet, after which they would be destroyed. I used a logbook to record the research process, analyzed and organized the collected data. Also, I stored all the recorded audio interviews, field notes, internal documents and other data collected. The recorded audio script was transcribed to produce the verbatim text. Also, the memo was used for adding notes and other comments during the study.

Themes were documented in the research logs to keep track of the understanding and patterns during the interview. The interview protocol, as a form of participant observation, provided insight into the participants' perspectives and experiences,

generating the appropriate themes for the study (Adekoya & Guse, 2020). The collected themes were mapped to emerging strategies. The emerging strategies IT security managers used to prevent breaches due to insider threats were documented as they increased. The thematic analysis provided the similarities in the various responses from the participants.

Data Analysis Technique

Researchers in qualitative studies emphasize the importance of the data collected and how they are analyzed and interpreted (Williamson et al., 2020). Researchers use data analysis to transform the collected data to provide more insight and value (Jahja et al., 2021). Data analysis should include compilation, categorization, re-organization based on the entire theme, and data translation to describe the emerging themes (Abram et al., 2020). I adopted this approach to develop the research themes from the data. The outcome of thematic analysis provided the basis for deeper insight into some specialized analysis (Lester et al., 2020). Also, I used methodological triangulation to provide a deeper understanding of all the emerging themes from the study. The use of data triangulation for data collection from multiple sources enhances the analysis process from various perspectives to validate the data (Beresford et al., 2020). Researchers use thematic analysis to label, categorize and interpret the theme from the collected data set (Brower et al., 2019). Given this, I used thematic analysis to label, categorize and interpret the themes from the various data set.

Researchers use thematic analysis to deepen the understanding and discover hidden themes within the various data sets by identifying patterns which are reported as the study

themes (Lochmiller, 2021). The basis for identifying the themes was to identify and analyze the data. I used a thematic analysis approach to ascribe meaning to the recorded audio interview transcript, the field notes, and other industry documents. During the first phase of the data analysis, I obtained a transcript of the recorded audio interview, the field notes, and the interview questions in Microsoft Word. Then, I became familiar with the interview from the audio recording and the field notes to identify and eliminate data irrelevant to the research.

More so, I used coding to classify the data for comparison with other aspects of the collected data. Coding with the aid of software helps to identify and categorize data for comparison with components of the data set (Gilmore et al., 2019). I used the NVivo software for coding, categorization, and thematic identification for accurate data interpretation. The NVivo tool is an essential data management tool that provides thematic analysis to help the researcher make informed decisions (Sezgin et al., 2019). In addition, I took notes of the discussions to check for misconceptions from the participant's understanding or interpretation of the interview questions. Researchers use the coding process to identify additional codes that may emerge using common patterns, themes and other categorizations related to the research question (Locke et al., 2022). I used the data matching approach to identify common themes during the data analysis.

The identified themes helped compare the findings of previous studies and their relationship with the literature review and the conceptual framework for this study. The theme categorization helped present the results, recommendations for future research, and research study conclusions.

Reliability and Validity

The reliability and validity of a study are essential for ensuring that the study's outcome produces quality and transferable knowledge. A researcher must understand the reliability conditions and criteria for the validity of the study's outcome (Yadav, 2022). Also, Mwita (2022) explained that qualitative research must ensure reliability and validity to produce credible and transferable knowledge.

Reliability

Reliability shows the degree of trustworthiness of the findings of a research study. The study's findings' consistency ensures the industry's constant research dependency. For this study, I ensured the findings are reliable by using multiple data sources and addressing all dependencies by member checking during the interview to ensure data saturation. Member checking and data saturation enhance the research findings' trustworthiness (Guest et al., 2020). According to Yonas et al. (2023), member checking ensures that interpreted data is verified to improve its reliability. I ensured the participants reviewed the interpreted information for clarity and to improve its trustworthiness. I ensured that I described the context of the study in detail so it can be transferable or always produce the same result under the same conditions.

Validity

The validity of qualitative research shows consistency in the data verification and findings (Schweinsberg et al., 2023). Also, the validity of the research depicts the effectiveness of the research instruments used for the findings (Coleman, 2022). To ensure the validity of this study, I ensured that the participants reviewed the interpreted

data and the findings to provide clarification or corrections if there was an error. I also used numerous questions to help analyze the participants' responses. Antonietti et al. (2023) explained that validity could be achieved when the researcher uses numerous options to explore any concerns about the study's validity. I ensured that data saturation was achieved by collecting data to the point that no additional information obtained from additional data collected. Four parts are required to validate a qualitative study – credibility, transferability, dependability, and conformability (Moukhah et al., 2023).

Dependability

Interview protocol was used in addition to industry documents and research journals to create audit trails that provided the dependability and confirmability of the study. Conforming to a research protocol during data collection would eliminate bias in a study (Ivey, 2020). The researcher must have an audit trail that records all the procedures and happenings throughout the study (Dasaklis et al., 2022). The audit trails help prospective researchers to understand the occurrence during previous research. The dependability of a research study greatly depends on the audit trail created during the study (Campbell et al., 2020). Also, I ensured the study's dependability by using the interview recording, transcripts, and follow-up interviews through member checking. Member checking ensures the dependability of a study through follow-up interviews and deep data analysis (Kusuma et al., 2023). I described and documented this study's processes, methods, and designs.

Credibility

The credibility of research can be reached when the collected data is adequately peer-reviewed and enough to support the study's outcome using appropriate evidence and member checking Ningi (2022). I used member checking to validate that the interview details conform with the perspectives shared by the participants. Dyar (2022) argued that researchers validate the credibility of qualitative research when the findings conform with the shared views of the participants. The study's credibility becomes questionable when the respondent's perspective does not conform with the study's outcome.

Transferability

Transferability is the degree to which research findings can be transferred or applied to other contexts (Moukhah et al., 2023). The transferability of the research outcome can be defined when the context of the findings is enumerated (Younas et al., 2023). I documented the study's limitations, delimitations, and assumptions so that other IT security managers would make more informed decisions when using the research outcome. Also, I ensured that external parties reviewed the research findings with relevant and similar experiences with the participants. Research outcomes are considered transferable if it resonates with external parties with similar experience, especially if they did not participate in the research (Klem et al., 2022). I provided a detailed interview procedure and used the interview protocols to support the transferability of the research outcomes.

Confirmability

Confirmability shows the degree to which the researcher demonstrates that the study's outcome represents the participants' perspective without bias or the researcher's viewpoint (Manouchehri et al., 2022). Also, a researcher can ensure confirmability when the focus is on the data collected and the interpreted data is based on the participant's perspective without prejudice (Korstjens & Moser, 2018). Although the participant's perspective is critical for determining confirmability, triangulation and multiple data sources would help maintain credibility (Adler, 2022). I maintained a detailed field note and sought the perspective of other professionals to ensure that I achieved confirmability for this study.

Transition and Summary

The aim of this pragmatic qualitative inquiry study was to explore data security strategies that IT security managers used in the banking industry to prevent insider threats. I ensured I kept all data collected from participants' interviews confidential using the NVivo coding software. I used the interview protocol (see Appendix C) to mitigate bias in this study. Also, I used semi-structured interviews. I explored strategies used by IT security managers in banking industries to prevent insider threats. I used online industry documents, security archival records, banking industry website documents and other publicly available security documents. I used six participants as a sample size. I got the approval of the Walden University Institutional Review Board (IRB) before I started data collection for this study. I ensured that all the participants received an informed consent form (see Appendix B) and the interview protocol (see Appendix C) before

interviews. I used Zoom for the video interview with each of the participants. I used industry documents to complete the triangulation. I imported all data collected from participants to NVivo 14 for data organization, analysis, and themes identification. Section 2 included an overview of the purpose statement, my role as the researcher, population and sampling, data collection, data organization techniques, data analysis, reliability and validity, and the research methodology.

Section 3 includes presentations of research findings, applications to the IT field, and implications for social change. I also address potential areas for future study, reflections, and conclusions.

Section 3 Application to Professional Practice and Implication for Change

The purpose of this qualitative pragmatic inquiry study was to explore the effectiveness of security strategies that IT security managers use in the banking industry to implement secure procedures in order to protect customer and organizational data from breaches due to insider threats. The population was IT security managers in the banking industry in southeastern Canada who were aiming to improve their data security strategies.

Presentation of Findings

I used Zoom interviews for the data collection from IT security managers, working in the banking industry for at least 5 years. Also, I reviewed 25 documents collected from banks and regulator websites, government organizations, and other related online sources for standards and security frameworks such as NIST and ISO.

I interviewed six IT security managers in the banking industry using Zoom communication software. After the introduction and proper permission, I recorded interviews and took necessary notes. I also included industry documents on security as part of data collection. I used NVivo 14 for data organization, analysis, and coding of the recorded interviews. Conclusions and reflection of this study are presented at the end of this section. The following themes resulted from the data analysis stage: security standards, procedures, and policies, information security education and training, organizational security culture, asset management, identity and access management, and data security.

All participants were assigned unique identification number (IP-1, IP-2, IP-3, IP-4, IP-5, and IP-6) to protect their privacy. Industry documents include National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO/IEC), Payment Card Industry Data Security Standard (PCI DSS), and cybersecurity maturity model certification documents.

Table 1

Themes

Themes	NVivo Data Analysis Tool Word Count	Participants' Count	Document Count
The need for administrative controls	30	6	8
The need for information security education and training	64	6	8
The importance of organizational security culture	34	6	8
The importance of asset management	61	6	8
The importance of identity and access management	73	6	8
The importance of data encryption	61	6	8

Table 2 involves information about the six participants regarding their years of experience in the banking industry and current geographic location.

Table 2

Naming Convention for Participants

Participants	Geographic Location
IP-1	Southeastern, Canada
IP-2	Southeastern, Canada
IP-3	Southeastern, Canada
IP-4	Southeastern, Canada
IP-5	Southeastern, Canada
IP-6	Southeastern, Canada

According to Boto-García (2023), cybersecurity risk has become a great concern to IT security managers due to the rise in the use of technologies. Organizations that provide consistent and adequate information security awareness training to their employees are less likely to suffer breaches due to unhealthy security practices (Yao et al., 2019). The NVivo tool plays a vital role in data analysis and helps the researcher deduce themes in qualitative research (Robins & Eisen, 2017). The themes from this study aligned with the purpose of the study and the literature review. The outcome of the findings also aligned with the ANT. All identified themes were reviewed as they related to the ANT.

Theme 1: Administrative Controls

Administrative controls in the banking industry to prevent breaches due to insider threats were a theme according to participant interviews. This category has subthemes, including security frameworks, policies, security procedures, and security standards.

Table 3

Administrative Controls

Data	Security frameworks	Security policies	Security procedures	Security standards
Participants	6	6	6	6
Documents	8	8	8	8

Table 4 includes a list of documents used for the data triangulation and downloaded from public and government websites.

Table 3 shows that six IT security managers participated in the interview that generated the following subthemes: security frameworks, security policies, security procedures, and security standards (see Table 4).

Table 4

List of Documents

Documents	Participants	Document Page Count
NIST SP 800-53	All	14 - 16
NIST Special Publication 800-100	All	16- 20
PCI DSS v4.0 Quick Reference Guide	All	15 - 22

Payment Card Industry (PCI) Software Security Framework	All	23
ISO/IEC STANDARD 27001	IP-4, IP-6	9 - 24
Cybersecurity Maturity Model Certification Version 2.0	IP-1, IP-4	1 - 6
ISO/IEC TS SPECIFICATION 27008	All	7 - 13
Personal Information Protection and Electronic Documents Act (PIPEDA)	All	60

Participants validated the need for security frameworks in the security program and that the NIST framework was adopted in the banking industry as part of the strategies used to prevent breaches due to insider threats. The Payment Card Industry Data Security Standard (PCI-DSS) for card data security, were adopted as part of the strategies for preventing breaches due to insider threats. The participants confirmed that the ISO 27001 certification provided the security standards used in building an effective and robust security management system for data protection as part of the strategy to prevent breaches due to insider threats.

Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian privacy regulation that provides guidelines for protecting the rights and privacy of consumers in Canada. The law provides guidelines to all private organizations,

including banks, on collecting, using, and distributing consumer data. Participants confirmed the need to protect consumer data and that the PIPEDA regulation helped in developing the banks' security program and strategies to prevent breaches due to insider threats. Participants implemented the following subthemes:

Security Framework

Frameworks provide the means for standardizing service delivery to improve the efficiency of the organization's security program. Frameworks are often implemented to provide a common language and understanding between organizations and their clients. Cybersecurity frameworks provide standards, guidelines, and industry's best practice approach to managing organizational risks. Using a cybersecurity framework, an organization can prioritize a repeatable and cost-effective means to promote data security and resilience within the business. A bank's ability to operate and do business is based on the condition that it shows its adoption of specific standards and the maturity of its information security program (Pollmeier et al., 2023). Participants mentioned that their organizations developed security programs around the NIST SP 800-53 Risk Management Framework. Participants IP-4 explained that the Risk Management framework allows the bank to integrate its data security, privacy, and other risks associated with third-party management into the overall organizational security strategy. Emphasizing that the effectiveness of the security program is dependent on how well the bank can manage its organizational risk.

According to IP-5, organizational risks can be caused due to activities of both internal and external individuals, such as employees, contractors, and third-party

vendors that constitute specific insiders. The NIST SP 800-53 provides a risk-based approach to security controls selection and specifications that provide an effective security program for an organization. Participants emphasized the need for consumer privacy and that their security strategies are tailored to meet the requirements for PIPEDA. Security policies are developed to help banks meet their PCI DSS compliance obligations and strengthen their strategies for data security in preventing breaches due to insider threats. Participants IP-1 and IP-4 mentioned that their security strategies combine various frameworks, including the CIS Cybersecurity Maturity Model, the ISO 27001, and the NIST framework. Stating that using this combination of frameworks and standards provides a comprehensive list of controls and policies that help improve the security posture for the banks in preventing breaches due to insider threats.

Using the ANT framework, all the participants explained how they achieved data security in the banking industry from interactions created between people, security policies, and technology. According to Lee (2023), data security is achieved when data confidentiality, integrity, and availability is achieved from the interaction of people, policies, and tools. According to IP-5, the security frameworks are essential to help the banks improve their security posture and establish effective security practices while achieving compliance with regulations. In addition, IP-1 mentioned that the primary objective of cybersecurity in the banking industry is to protect critical assets, including business and customer data. IP-2 mentioned that the security framework helps banks develop policies and procedures that can help establish and maintain security controls for preventing breaches due to insider threats. The outcome of this study aligns with the

conceptual framework as it demonstrated the interaction between the people and the security policies and procedures to achieve data security to prevent breaches due to insider threats.

Security Policies

Writing an effective security policy is essential for banks. Financial institutions are exposed to a variety of risks which include but are not limited to operational and transactional risks. Information security policies provide a set of rules or statements that guide the employee's behavior concerning their responsibilities to the organization, data handling, and acceptable use of critical and noncritical assets. The security policy defines employees' desired behavior and contributes to the organization's security posture. A security policy noncompliance can be very damaging to an organization. Organizations must invest in tools to detect policy noncompliance and potential breaches (Li & Hoffman, 2023).

All the participants confirmed that they had implemented security policies aligned with the business objectives. Participant IP-3 confirmed that the information security policy should include an acceptable use policy that defines how an employee must handle company data and assets. Also, IP-4 commented that employees must understand their responsibility to protect the organization's critical assets as defined in the information security policy. IP-3 discussed the need to punish employees if they violate the organization's information security policy. Stating that policy enforcement is essential to improving the organization's overall security posture. The use of technology cannot

provide absolute security assurance without a properly developed and enforced information security policy (Li & Hoffman, 2023).

IP-3 commented that banks must be deliberate in enforcing security policies and that procedures should be laid down to assess policy effectiveness and ensure periodic reviews and corrections. IP-1 emphasized the importance of security policies in protecting the business's physical and digital assets. IP-2 stated that security policies must define the roles and responsibilities of the individuals and that business leadership must drive security. Stating that business leadership must understand the importance of information security and its effects on the business. Also, IP-2 mentioned that security policies must include data classification and handling processes to categorize data depending on sensitivity and value to the business. The severity of data would determine the level of security controls that must be applied to it. IP-5 also reiterated the need to assign data owners after identifying critical assets and data elements.

Security policies must ensure appropriate data governance to help banks identify, detect, and protect critical assets. All participants mentioned that security policies must include security awareness training for all new and existing employees. Security awareness trainings must have sufficient instructions on security best practices, potential security threats such as ransomware, phishing attacks, password policies, and security industry best practices approach to preventing breaches. The outcome of this study aligns with the ANT framework as it defines the interaction between the employees and the security policies to create security awareness that could help prevent breaches due to insider threats.

Security Procedures

Security procedures provide the activities required to perform specific security functions or tasks. Procedures define the series of steps that an implementer needs to follow consistently or repetitively to achieve an expected outcome. When banks implement effective security procedures, it provides some expected actions that can support the business processes when conducting security functions. All participants commented that banks must have clearly defined security procedures that must be communicated appropriately. IP-2 suggested that when security procedures are implemented, it promotes process improvement and employee training.

Procedures drive the implementation of consistency required to decrease variation in the organization's security processes (Fay & Patterson, 2018). IP-3 emphasized the need for all employees to understand the organization's security procedures as this increases performance and improve process quality. When the variations in the security processes are minimized, organizations can increase security controls within the business (Fay & Patterson, 2018). All participants explained that lack of clear procedures or its implementation and enforcement could result in organizational inefficiency in its security program.

According to IP-4, the absence of clear procedures is the primary cause of security negligence among employees, which could result in insider threats. IP-3 commented that banks need a matured security program that details its security procedures to structure employees' behaviors and create a security-conscious culture. Effective information security procedures inform better understanding and influence employees' security

behaviors (Ogbanufe & Ge, 2023). All participants agreed that security procedures must be designed to help banks meet their business needs. Also, security procedures should provide banks with the framework that influences their architectural design, implementation, and management. The outcome of this study aligned with the ANT framework as it defines the interaction between staff and business strategies in creating security procedures by collecting information from the organization and staff.

Security Standards

Security standards provide guidelines and industry best practices that banks can implement to improve the overall security posture. Information security standards are integral to business operations within banks and other financial institutions. Information security programs governed by industry standards help protect business digital assets from malicious insiders and external threat actors. All participants commented that a robust security program with industry standards would reduce the risk of security breaches within the banks. IP-2 commented that security controls with industry standards would prevent unauthorized access to an organization's critical assets.

All participants commented that cybersecurity standards can help banks to identify and develop measures to protect business-critical assets from cyber-attacks. IP-3 commented that security standards provide necessary guidance on responding to threats and recovering from security incidents. IP-4 commented that implementing the ISO/IEC 27001 provides the banks with the frameworks for managing business-sensitive data. IP-6 commented that the ISO/IEC 27001 provided the requirement for implementing security controls and performing risk assessments for banks.

All participants commented on the importance of the NIST framework as it provides a set of standards used for managing security risks within the banks. According to IP-6, the NIST frameworks help banks to identify and manage security risks in a structured manner. IP-4 commented that implementing the NIST framework helped the bank establish security baselines to improve security posture and identify security risks. All the participants commented that banks must develop and implement security processes based on industry standards to identify and resolve security incidents. All participants commented that the NIST cloud security framework (NIST CSF) could be implemented with ISO 27001 as they have similar principles, including business leadership support, continuous improvement, and risk management approach.

IP-3 commented that implementing appropriate security standards would help banks put necessary plans in place and change its security practices to build an organization-wide security culture. The outcome of this study aligned with the ANT framework because as the banks develop and implement security standards, it changes the security practices and improves the interactions between the employees and these standards to build a security-conscious culture within the bank.

Theme 2: Need for Information Security Education and Training

According to all the participants, security education and training are very important in preventing breaches due to insider threats. IP-2 commented that an effective security program improves the behavior of employees by driving a positive behavioral change that supports the security objectives. IP-3 also mentioned that security awareness training improves the employees' knowledge of security procedures and drives behavioral

changes and beliefs that create a more security-aware culture for the bank. All the participants mentioned that banks need security education and training for employees to create awareness of security threats and provide the required knowledge and skills for security policy compliance. IP-4 mentioned that security awareness and training could be critical in improving the banks' security posture as most employees may need to be aware of the various security risks. In developing strategies to prevent breaches due to insider threats, all the participants mentioned that effective security education and training can minimize the risks of losing sensitive business and customer data. IP 5 emphasized an effective security program helped the employees see the importance of security and that it is everyone's responsibility. IP-6 mentioned that it is vital for employees to understand the business and the various security risks around it. All the participants stressed the need for the Human Resource Management team to include mandatory security training for new and existing employees. Stating that employees should be made to participate in mandatory security awareness training at least annually. Security must be driven by senior leadership and built into all bank policies and processes to instill a security-aware culture.

Table 5

Responsibilities and Components of an effective Security Awareness Training program

	Subthemes
Human Resources Process	Background Checks
	New Hire Onboarding

Mandatory Security Trainings/ Phishing Campaigns

Leadership Involvement

HR Process

The HR department is a fundamental part of an organization. They work with everyone and every unit in a broader reach than any other department within the bank. Because of this level of visibility, the HR department can support banks to improve its security posture by creating awareness and ensuring employees have the necessary level of security training before and after the hiring process. The interaction with new hires at the beginning of the hiring process is an opportunity to set the foundation for a culture of security awareness. All participants mentioned that HR departments should include security risk awareness training in the new hire onboarding process to improve the bank's security posture. IP-3 mentioned that HR department should also include consequences in its processes for noncompliance with the security awareness training, as this would improve compliance and build an overall security culture within the organization. IP-4 mentioned that although security awareness training is being developed and introduced by the IT and security department, bringing HR department into this process may help improve compliance and enhance the security posture for banks.

According to IP-3, HR department should introduce penalties for poor data handling, whether it leads to a security breach or not. The HR department should be

involved in enforcing organization policies around acceptable use, data handling process, and any other actions of an employee that may result in security risk. All participants mentioned that employees' acts of omission or commission toward data protection significantly impacts the bank's overall security. IP-3 mentioned that although the human element is considered the weakest link in the cyber chain, it can also be perceived as the most critical aspect in preventing breaches due to insider threats as security starts with people. Human resources provide employees with improved job-related knowledge and skills, including security awareness and training. In alignment with the ANT framework, the HR department can collect relevant data about employees' behaviors that can be used for user analysis to prevent breaches due to insider threats. Also, the HR department may collaborate with employees to provide awareness training and develop policies and procedures to improve their interactions with security strategies and programs to prevent security breaches due to insider threats.

Background Checks

Background checks as an employment process help organizations understand the holistic picture of the candidate they intend to hire. Apart from ensuring that the most qualified persons are hired, this process can be used to understand the behaviors of the intended hire, which can help prevent theft and other criminal activities. IP-3 mentioned that background checks are necessary to protect the bank's assets, reputation, and employees. All participants commented that banks must validate a prospective employee's character before hiring. The HR department can identify some questionable

behaviors during a background check that could help detect the possibility of maliciousness. All participants commented that banks must conduct adequate background checks to understand the new hire and know if any behavioral red flags can be detected at the early stage of preemployment.

New Hire Onboarding

The business hiring process must ensure a new hire has a smooth onboarding. Although most of these activities are administrative and taken care of by the HR department, some security-related tasks should be identified because they could cause organizational risks. All participants commented that the HR onboarding process should include IT checklists that the IT department would be prepared in advance for the employee. The following are some of the IT checklist and their security benefits to the banks: Department for the new hire: This would help the IT department determine the user access scope on the network. Services and applications the new hire need to access within their job role: This helps the IT department provision role-based access control based on the principles of need-to-know and least privilege. The new hire manager or supervisor: This would help in creating the workflow for approval and escalations. Account creation: The new hire account creation must meet the requirements as set out in the security policies.

All participants mentioned that new hire access must be based on the principles of least privilege, and access must only be given to what the employee needs to do their

jobs. Participants IP-2, IP-3, IP-4, IP-5, and IP-6 confirmed that user access must be continuously monitored, and alerts created for noncompliance or data exfiltration attempts. All participants confirmed that they had implemented Identity and Access Management solutions that restricted user access to only what they need to do their jobs.

IP-1 confirmed that strong and continuous authentication to critical assets was implemented for banks to prevent breaches due to insider threats. IP-1 and IP-2 confirmed that they had implemented strategies to monitor and control any access combinations considered toxic pairs. All the participants commented that user access must be monitored and profiled to detect any behavior anomaly or change. IP-2 and IP-5 confirmed that they had implemented strategies to monitor privileged access within the network to prevent breaches due to insider threats. The outcome of this study aligns with the ANT framework in that creating interactions between new hires and the security strategies of the bank helps create awareness and improve security practices that can help prevent breaches due to insider threats.

Mandatory Security Training and Phishing Campaigns

Security awareness training provides employees with the education to identify security risks and understand best practices. All participants reported that security awareness training is essential for banks to reduce security risks that could result in data breaches. IP-3 and IP-5 mentioned that effective security awareness training would help employees identify phishing attempts and other techniques used by attackers that could lead to data breaches. IP-2 mentioned a need to reduce the risk of loss of PII and other business-critical data by enforcing security awareness training to help the employees

understand how these assets can be protected. All participants confirmed that well-developed and implemented security awareness training improves compliance with password security policies and reduces the chance of employees falling for phishing attempts within the organization. All participants commented that security awareness training teaches employees good cyber hygiene habits and how to identify risks to the business. Effective security training helps employees to identify phishing attempts, malware infections, and insecure websites. IP-3 mentioned that when there is enough security awareness, the employees understand their responsibilities and the expectations of the business as it relates to protecting critical assets.

Strong security awareness training protects the customers, employees, and the business. It must protect everyone and ensure security is a priority for the business. IP-6 mentioned that employees must have requisite training to understand the policies and procedures for protecting the business's digital assets. IP-3 mentioned that all employees must be made to acknowledge the security policies and understand the acceptable use of the business assets. All the participants reported that they have developed and implemented mandatory security awareness training that must be delivered at least annually to all employees. IP-2 commented that security awareness training must have email security protocols, password security policy, and malware identification and avoidance elements. According to all the participants, effective security awareness training provides employees with the knowledge required to identify, report, and prevent incidents that could result in security breaches. Also, all the participants mentioned that security awareness training must be mandatory and conducted more frequently to keep

employees updated on how to identify threats and respond accordingly. The outcome of this study aligned with the ANT conceptual framework because it showed the interactions between the employees and the security awareness training to prevent security incidents from an insider that could result in a data breach.

Leadership Involvement

Information security leaders must understand that though technology enables the business, security transcends technology. Cybersecurity provides overall protection for business operations. All the participants commented that security leaders should integrate the people, processes, and tools to ensure a consistent security posture for the banks. IP-2 mentioned that security leaders must view security as a business problem and understand security management related to the business objectives. Also, IP-3 and IP-6 reported that they had implemented strategies to integrate people, processes, and security technologies to secure the bank's critical assets. IP-1 mentioned that the business must invest in security solutions that would support the business objectives and have a horizontal perception of security values. In other words, the business must perceive security as a bridge builder across other departments and skill sets.

Given this, IP-2 mentioned that security should be driven from the top down and across every department. Also, IP-4 reported that security should be everyone's responsibility and not just the business of IT. Also, IP-2 mentioned that security leaders should ensure the business adopts a security-conscious culture across the organization. IP-2 and IP-3 reported that as security leaders, they had developed an effective strategy with other decision-makers within the business. Also, IP-5 and IP-6 mentioned that they

have implemented a security assessment program that identifies risks and helps the business understands its threats and vulnerabilities. They reported that this program helped the banks assess their security posture, measure the progress of new security programs, and require countermeasures to protect against insider threats.

According to IP-3, the IT leadership should drive security initiatives by creating and implementing data security strategies and developing policies and procedures to help achieve the business objectives. This approach gives management an overall view of the individual departments and their organizational risk levels. In other words, business management can get every department to work together to achieve business security objectives. All the participants commented that when security is driven from the top down, the business can demonstrate its commitment to security and prioritize it. When security is prioritized, remediation efforts are more effective because senior leadership is involved. All the participants commented that data security is prioritized when security is driven from the top down. According to IP-3, building a security culture becomes more accessible and effective when senior management is involved. As a result, senior management can set clear objectives and expectations for the business.

Improving the interaction between people and the expected security strategies could help protect data and prevent breaches due to insider threats. According to IP-3, it is important to create a security-aware culture where every employee sees security as their responsibility rather than the business of IT department. All the participants reported that security should be everyone's responsibility, and this can only be possible with the involvement of the business management. Also, IP-5 commented that security needs to be

adequately funded by top management to enable the IT department to perform its functions more optimally. The outcome of this study aligned with the ANT framework because senior management's involvement can improve the interaction between people and the security strategy that could create a security-conscious culture among the people. Creating a security-conscious culture improves employees' commitment and awareness of data security to prevent breaches due to insider threats.

Theme 3: Importance of Organizational Security Culture

When employees think and act with more security awareness, the risks of incidents and other causes of data breaches would be greatly minimized, and employees are more likely to detect and report policy noncompliance and behaviors that could result in data breaches. According to IP-3, employees feel a greater responsibility to protect the business's sensitive data when there is an organizational security culture. All participants reported that employees are more involved, and security can be significantly enhanced even with minimal expenditure from the bank. As a result, this can raise the bank's security maturity and compliance with proactive security controls. IP-1 reported that security-conscious ideals, customs, and interactions should be a priority for banks as this could influence the overall security posture of the bank.

Also, all participants commented that building a security culture provides the platform for its ability to detect and protect customer data, employees, and other business-sensitive information. All participants reported that they had developed and implemented strategies that helped improve employees' attitudes, behaviors, cognition, compliance, communication, and norms to create a security-aware culture within the

bank. IP-3 also mentioned that an effective communication channel provides a sense of responsibility and helps in all security-related incident reporting within the bank. IP-2 mentioned that the bank must promote employees' knowledge and adherence to security policies and procedures. IP-1 reported that he had implemented strategies that helped improve employees' behaviors toward data protection.

All participants reported creating simple, transparent, easy-to-understand security policies, procedures, and guidelines to build an influential organizational security culture. IP-6 mentioned that the banks must prioritize information security and increase their investment to promote a security-conscious environment. Adding that most breaches in recent times are due to the need to be more willing to increase security investment. IP-3 mentioned that employees should be rewarded when contributing to a positive security culture within the bank. All participants mentioned that building an influential security culture depends on positive reinforcement and how well employees are encouraged to adhere to positive security practices. Secure behaviors can be rewarded in various ways, such as recognition and internal security communications, such as intranet or newsletters, to recognize employees for reporting phishing links or vulnerabilities.

In addition, all the participants reported that they had created security strategies that provide employees with adequate awareness and education to identify and report security incidents to prevent breaches due to insider threats - stating that a lack of security awareness creates the majority of the security incidents within the banks. The outcome of this study aligns with the ANT framework as it shows the interactions among

employees and the security strategies that create the culture within the bank for protecting data and preventing breaches due to insider threats.

Theme 4: Importance of Asset Management

Asset management is essential for managing an investment portfolio while mitigating security risks within the organization. All the participants reported that effective asset management solution helps the bank account for all its critical assets. IP-6 mentioned that she had implemented strategies that helped the bank identify, classify, and assign owners to its critical assets. IP-2 mentioned that only when the value of an asset is known can security controls be applied effectively. IP-1 implemented asset management solutions that enforced proper authorization controls in making effective business decisions. When the banks track their assets, it can streamline compliance standards, operations, and reporting efforts. According to IP-5, Asset management would allow the banks to understand better the location of their critical assets and what level of security controls should be implemented.

All the participants reported that asset management would allow the banks to maximize their assets' value better while reducing risk and optimizing the business process. Also, defining data classification and assigning owners to data provide better data handling and security. The data owner determines the security controls that should be applied to the data. IP-1 reported had implemented security strategies around data access management to prevent unauthorized access to data that could result in data breaches due to insider threats. IP-4 reported that an effective asset management process would help the banks ensure regulatory compliance. Also, IP-2 commented that he had

implemented an asset management strategy to track assets and enforce policies to prevent data theft and loss. Stating that tagging assets would allow the bank to effectively track its assets and optimize the use of critical assets. IP-5 mentioned that the bank could only secure an asset that is known and can be located.

All the participants reported that they had implemented asset management strategies that helped the banks identify assets and the associated risks with these assets. As a result, the banks understood the security risks and how they could be mitigated to prevent data breaches. According to all the participants, every device on the network could have associated risks and vulnerabilities that could be exploited, which may result in a data breach. Also, all the participants reported that they had implemented asset management to provide the needed visibility for building a comprehensive security strategy for the bank. IP-4 commented that an effective asset management strategy would help the banks proactively detect threats before they can be exploited or become a significant problem. By continuously monitoring data during a continuous development process, the team would be able to detect and identify risks early in the process.

IP-4 reported that even if a breach occurs, an effective asset management strategies would provide the IT security team with asset inventory and the associated risks to understand the context of the attack. Asset management strategies place the banks in a position to quickly identify and respond to security risks that could result in incidents. IP-5 mentioned that although asset management is only an aspect of the overall security strategy, executing a proactive security operation with a proper asset management strategy is possible. A lack of asset management can introduce more risks to

the business and challenges to security operations. Poor asset management practices could increase the risk of business disruptions and cause data unavailability impacting business operations and reputation.

Also, IP-4 reported that understanding data locations would help the banks implement necessary security controls and respond to possible security incidents. Automating security processes becomes problematic when there is a lack of understanding of data residency and the associated risks. The security team can quickly respond to security incidents by identifying endpoints and performing vulnerability assessments on each of them. Active vulnerabilities can be detected and addressed with a security asset management strategy.

Also, during an incident investigation, asset management provides the security team with the necessary information for root cause analysis and remediation. Security asset management provides visibility into cloud services by identifying vulnerable resources due to a lack of access control and insecure software. According to IP-5, assigning asset owner role increases employee sense of responsibility for data security. All the participants reported that with an effective asset management process in place, the IT assets are identified, inventoried, monitored, and maintained throughout their lifecycle. As a result, performance optimization and asset availability are enhanced with an asset management strategy in place. In policy noncompliance, a security asset management strategy enables quick asset discovery and issue remediation. Participant IP-1 commented that he had implemented an asset management strategy that provided the bank with more visibility into its environment and, as a result, enabled effective threat

detection and prevention.

According to IP-4, understanding the asset inventory, location, owners, configuration settings and level of vulnerabilities would help the bank to identify risks and prioritize its control objectives. All the participants reported that policies and patches can be applied consistently when an effective asset management strategy is in place. According to IP-5, the bank can monitor and audit its assets for any policy noncompliance, malicious activities, and an indication of compromise when an asset management strategy is in place. IP-2 mentioned implemented an asset management strategy that helped the bank effectively respond to security incidents and ensured regulatory compliance. All the participants reported that the banks must define clear policies, procedures, and processes with well-defined and communicated roles and responsibilities when implementing asset management strategy.

All the participants reported that the banks must ensure their employees have adequate security awareness and education to understand the benefits of asset security and their responsibilities to ensure the security of critical business and customer assets. The outcome of this study aligns with the conceptual framework because it shows the interaction between the employees and the asset management strategy to detect and prevent risks that could result in a data breach caused by insider threats.

Table 6

Benefits of Security Asset Management Strategy

Security Asset Management Strategy		
Asset Inventory	Security Controls	Risk Management
Data Residency	Patch Management	Incident Management
Data Ownership	Vulnerability Management	Regulatory Compliance
Monitoring	Policy Enforcement	Licensing Management

Theme 5: Identity and Access Management

Identity and access management is a critical function in an organization. It helps the business organize all levels of user, applications, and privilege access to enhance security and better control systems. This provides controls for mitigating data breaches, identity theft, and other unauthorized access to sensitive business data. IP-1 reported that he had developed an IAM security strategy and integrated it into the business operations, which helped the bank achieve its compliance and regulatory requirement. Stating that integrating IAM controls within databases would enhance data security and unauthorized access to sensitive business data.

All the participants reported that they had implemented the IAM strategy, which helped reduce human errors that could occur due to manual permission entries. They all reported that when IAM is fully automated, it reduces operational cost and enhance business efficiency. Also, the automated IAM process reduces human errors that could lead to data breaches due to insider threats. IP-2 commented that IAM is essential in providing confidentiality for the business. Stating that IAM tools provide restrictions to sensitive data and can only allow selected individuals that require such access. According to IP-1, the IAM solution can provide a streamlined workload for the business. When the IT workloads are streamlined, the number of support tickets for password reset is significantly reduced for the IT department. With a streamlined workload, the IT department can roll out single updates across the organization that can change everyone's access privilege at the same time. The following subthemes were implemented by all the participants in developing IAM strategies for preventing breaches due to insider threats.

Principles of Least Privilege

The principle of least privilege means that an employee is only given sufficient access level to carry out a task or required for a purpose. All the participants reported that employees should only be given privilege levels that are as high as they require. According to IP-1, employees or applications should only have access to specific datasets, services, or applications required to complete a task. IP-2 commented that the principle of least privilege could prevent lateral movement or malware spread in the event of a breach. Participant IP-1 stated that this principle would help the business prevent data loss and exfiltration of sensitive business data. Mentioning that employee

access should be limited to job responsibilities and must be continuously monitored. Participant IP-4 mentioned that implementing the IAM strategy with the least privilege principles would help the banks minimize their attack surface and prevent breaches. Apart from security, all the participants reported that the principle of least privilege could provide system stability by limiting unauthorized system changes.

All the participants reported that they had implemented IAM strategies with least privilege principles that helped streamline user and entity access to only what is required to perform a task as a control for preventing breaches due to insider threats. IP-2 stated that user access must constantly be monitored for changes to its privileges to avoid possibilities of escalation and to prevent data breaches. The outcome of this study aligns with the conceptual framework such that it creates an interaction between users and the IAM security strategy to prevent data breaches due to unauthorized changes by an insider. According to all the participants, they had implemented the principles of least privilege as a mitigation strategy to prevent privilege escalation and abuse. They commented that this strategy helped the banks to prevent attackers from escalating their privileges to perform lateral movement to gain access to sensitive business data.

IP-4 reported that he had implemented a data classification and handling strategy for sensitive data, which helped safeguard business-critical data with the principles of least privilege. All the participants reported that roles and responsibilities are essential when implementing the PoLP because it works with role-based access control (RBAC). RBAC ensures that employees' access to data or applications is limited to their role. IP-1 mentioned that PoLP would help banks mitigate identity theft and other identity-related

risks. To effectively implement the PoLP, all the participants reported that good data sanitation practice is critical and should be practiced by removing duplicate and redundant accounts or data. Stating that hackers can exploit redundant accounts and use them to perform malicious acts that could result in data breaches in the organization. IP-2 mentioned that privilege access monitoring is critical to provide visibility and create baselines for normal user behaviors. Mentioning that least privilege access should be case-specific or one-time basis and limited to only when needed with strict oversight. The output of this study aligned with the ANT conceptual framework as it demonstrated how users and other applications interacted with the PoLP strategy to prevent data breaches due to unauthorized access and other forms of privilege escalation by an insider.

Principles of Separation of Duties

The principle of separation of duties (PoSD) is an integral part of the security strategy for every organization as it involves assigning tasks to more than one person such that no individual can solely execute an action without the support of another person. IP-1 mentioned that PoSD would help the banks enforce proper authorization controls on critical databases. All participants reported that no individual should have enough privilege to misuse data or systems within the organization. IP-1 and IP-6 mentioned that they had implemented strategies that applied the PoSD, and a proper access control mechanism was implemented. All participants reported that implementing the PoSD would help the banks reduce errors and collusions that could lead to fraud or data theft. IP-1 and IP-2 mentioned that although PoSD is very important, the banks must ensure it monitors user access for possible toxic pair combinations. Toxic pair

combinations are access combinations either from one person or a group of users that can be used to commit a crime or perform any data breach within the organization.

According to all the participants, the PoSD is critical for banks as it enhances organizational security and compliance. Stating that it helps reduce human errors that could lead to data breaches. Also, IP-6 mentioned that establishing a streamlined access monitoring structure helps the security team understand activities within the organization. IP-2 mentioned that he had implemented security strategies that clearly defined policies and processes that enhanced the separation of duties concept for the bank. Implementing clear policies and processes is critical for successfully implementing the IAM strategy. IP-2 mentioned that incidents of fraud would be inevitable when there is a lack of separation of duties in the banks. All the participants reported a need for collaboration between IT and HR to ensure that roles are adequately defined to help appropriately define security controls that would provide adequate separation of duties. They stated that roles and responsibilities should be defined and separated to reduce the possibility of collusion or misuse of business assets.

According to IP-3, the principles of separation of duties can be more effective when there is a collaboration between HR. and IT to ensure that no individual role is involved in more than one function within the bank. This means that the head of each department or unit must be involved in establishing and maintaining this internal control. Also, IP-2 reported that he had implemented the PoSD in his security strategy, which helped the bank prevent many issues around financial fraud and data loss. In alignment

with the ANT framework, the outcome of this study demonstrates human interactions with security policies to prevent breaches due to insider threats.

Theme 6: Data Encryption

Securing business and customer data is very important to banks because the implications of data leakage could be detrimental. Whether the bank's business data or customers' information, data security is critical to preventing data loss and other security threats. All participants reported that more than traditional security measures such as detection and network firewalls may be required to protect organizations from cyber threats. IP-1 mentioned that data encryption at rest, in transit, and use protects the bank from external threats and malicious insiders. IP-6 stressed that the bank remains vulnerable if its sensitive data are not Encrypted. IP-4 reported that he had implemented a data security strategy to help his organization safeguard sensitive data and achieve compliance objectives. All participants reported that they implemented a security strategy that helped the banks achieve their PCI-DSS recertification, as data encryption is crucial.

They mentioned that data is most vulnerable when it is in transit, so the banks must implement security controls to protect sensitive data when transmitting from one point to another. IP-2 reported that the most common tactic for hackers is to exploit data vulnerabilities and encrypt it for ransom. He mentioned that encrypting data would ensure data integrity and protect it from tampering by malicious individuals. Due to the rise in the use of personal and mobile devices, all the participants reported that they had implemented data security strategies that helped the banks ensure their data is fully

protected on all devices across its locations. IP-1 mentioned that device authentication is essential to mitigating the risks of unauthorized access to data.

Protecting Data at Rest

Data at rest is data in storage or disk. Data encryption when in storage, protects the integrity and prevents unauthorized access to the data. This provides controls that would prevent attackers from accessing unencrypted business or customer data and making unauthorized changes to the data. All the participants reported that sensitive data such as credit card information, business information, customer identifiable information any other business or customer-sensitive data must be encrypted in storage or disk. IP-1 mentioned that he had implemented a data security strategy for data at rest as part of the bank's overall cybersecurity strategy to support the business objectives. Stating that access and authorization controls were integrated into the encrypted database such that only authorized employees could make authorized changes to the data.

According to IP-1, this approach improved the bank's security posture and enhanced data integrity for the bank. Also, participant IP-1 stated that the data was labelled and cataloged as part of the strategy before encrypting the data at rest. According to IP-1, data labelling, and cataloging provide an effective classification and handling process for the bank. IP-4 mentioned that he highly recommends data encryption and that the banks should prioritize it because of the nature of the data they handle and process. IP-2 and IP-3 mentioned that data encryption at rest is required by the bank's need for regulatory compliance and data governance efforts. They mentioned that data encryption

is a significant requirement for the PCI DSS certification, which all banks have obliged to have.

All the participants reported that they had implemented data encryption at rest as part of the strategy to enhance the defense-in-depth approach to security for the banks. According to IP-5, data residency is an issue for most organizations, especially with cloud computing. Adding that data encryption at rest provides the security assurance these organizations need for data stored in various locations. IP-1 mentioned that when data is encrypted at rest, it becomes easy to dispose of it by secure erasing at the end of its lifecycle with little or no risk of data misuse. All the participants reported that they had implemented data encryption at rest as part of the data security strategies for the banks to enhance security against Advanced Persistent Threats. They mentioned that this approach provided an additional layer of control between the attacker and the sensitive business data that could have been stolen.

According to IP-2, a secure-in-depth approach is highly recommended for all organizations. He mentioned that effective data encryption at rest and other security controls such as access control, DLP agents, and SIEM would help the banks reduce their attack surface and prevent breaches due to insider threats. IP-5 mentioned that banks and other financial organizations should spend more on securing critical data Additionally, organizations would benefit from effective data governance with encryption of data-at-rest to enhance the overall control objectives for the business. In alignment with the ANT framework, the outcome of this study demonstrated the interaction of employees with the

data security strategies for encryption of data-at-rest to prevent breaches due to unauthorized access and modifications of data by an insider.

Protecting Data in Transit

Data encryption while in transit protects the data during transmission, especially after a connection has been established and authenticated. This approach reduces the attack surface and eliminates the need to trust third-party security controls on the other end. All the participants reported that data encryption in transit is highly recommended due to the sensitive nature of the data handled by the banks. IP-4 reported that he had implemented a security strategy that enforced data encryption in transit that helped the organization achieve its security objectives, business objectives, and regulatory compliance. IP-2 mentioned that business data must be encrypted in transit in case of interception and compromise because, with encryption, the data becomes unreadable if intercepted.

All the participants reported that they had helped the organization identify its critical assets, assign data ownership, and worked with these owners to assign appropriate security controls as part of the data security strategies. They recommended that sensitive business data be encrypted when transmitted across external or internal networks. This may include application-level data encryption or, at the minimum, using protected channels such as TLS or HTTPS. The use of encrypted VPN tunnels or Generic Routing Encapsulation (GRE) with proper access and authorization controls may also be an option for remote data access. All the participants reported that data confidentiality can easily be

compromised when data is transmitted in clear text over an unencrypted network. As a result, attackers can intercept and monitor the plaintext data when in transit.

According to Participant IP-1, data is in its most vulnerable state when it is transmitted from one point to another. When sensitive data and the channel are encrypted, it provides controls and protects data confidentiality at every point during transmission. IP-3 mentioned that secure communication protocols such as SSL/TLS are essential for ensuring data confidentiality, integrity, and authenticity in transit. IP-2 mentioned that he had implemented security strategies that provided data encryption in transit to protect the business-sensitive data transmitted across external and internal networks. All the participants reported that when data is encrypted in transit, it becomes difficult for malicious insiders and other attackers to sniff or intercept the traffic as they are transmitted across the networks. The outcome of this study aligns with the conceptual framework because it demonstrates the interaction between the data security strategy and the employees to ensure data is protected as it travels across the network to prevent unauthorized interception or modification due to insider threats.

Protecting Data in Use

Sensitive data should be protected throughout its entire lifecycle. According to all the participants, when data in use is encrypted, it prevents data loss even when the system is breached. IP-1 reported that applying effective access control to databases would provide additional control for data in use. Also, IP-2 commented that when data is encrypted in use, it gives the bank the privilege to use, share and transact with data securely without fear of exploitation. All the participants agreed that when in-use data is

encrypted, all data fields within an application would be subjected to the organization's encryption standard. IP-6 mentioned that data governance would provide a centralized platform for data management when data is encrypted in use.

All the participants reported that they had implemented a security strategy that provided data encryption for in-use data. They mentioned that data encryption in use does not only provide protection for underlying data but filters and analyses all requests and blocks any anomaly. All the participants reported that encryption of data in use would help the banks achieve compliance objectives faster while streamlining data storage. Also, they mentioned that data sharing between partners and customers becomes more secure and convenient. IP-1 reported that he had implemented a security strategy that protects sensitive data by enforcing encryption of data in use. He mentioned that this approach helped the bank prevent sniffers from intercepting and reading plaintext data.

When sensitive data is in clear text, the risk to the business is high because of the evolving threats landscape and the sophisticated tools that could be used to read data and exploit common data vulnerabilities. Attackers have devised techniques that can be used to exploit weaknesses in systems which include unencrypted data in use. All the participants reported that data is in its most vulnerable state when it is stored unencrypted in memory for the period of its usage. All the participants commented that encrypting in-use data provides the best defense against ransomware attacks and unauthorized modification and access to sensitive data. With the development of homomorphic encryption techniques, data can be used and processed in its encrypted form, making it possible to process data while ensuring it is protected. In alignment with the ANT

framework, the output of this study showed how employees can interact with security strategies for in-use data encryption to prevent breaches due to insider threats.

Applications to Professional Practice

This study explored the security strategies used by IT security managers in the banking industries in southeastern Canada to implement secure procedures to prevent breaches due to insider threats. The outcome of the study is suitable for Chief Information Security Officers (CISO), Business Information Security Officers (BISO), and IT security managers working in the banking industries to use security strategies to protect business and customer sensitive data from data breaches due to insider threats in the banking industry in southeastern Canada. The participants believed that their participation could have an impact on the development and implementation of security strategies to protect business and customer-sensitive data to prevent breaches due to insider threats.

Developing policies, standards, frameworks, and procedures provide a foundation for developing security strategies to protect sensitive data. Information security policies and procedures increase the security postures for the banks, improve compliance with data protection regulations and help employees maintain a culture and reputation that promotes the security of sensitive data. Tejay and Mohammed (2023) argued that when an organization develops a culture of security, its security posture is improved as a result. Also, employees become critical members of the security chain as they are seen as the front line of defense for the organization. Information security awareness is also improved when people's behaviors are understood regarding security. Security cultures

create human interactions with information assets and strategies to influence user behaviors to improve or preserve the organization's information security (Tejay & Mohammed, 2023). An effective security culture must support organizational policies and procedures. Also, Tejay and Mohammed (2023) commented that the success of any organization is related to how well the culture can be changed to a more security aware one.

The need for security awareness and the role of the human element in security is becoming more critical for organizations. Practical security awareness training and education impacts human behaviors, knowledge, and skills to create security conscious environment (Khan et al., 2023). Security education and training provide the required knowledge and skills that users need to protect business and customer data from threats and prevent common mistakes from phishing and other social engineering attacks. Recent studies show that security awareness training improves learning and knowledge of phishing attacks while reducing employees' susceptibility to the attack (Khan et al., 2023). Dincelli and Chengalur-Smith (2020) argued that security awareness training improves employees' perception and knowledge of unauthorized information disclosure, improving the organization's overall security posture. Security awareness improves employees' interactions with one another and with the security policies to help protect the business's sensitive data from insider threats. Security awareness training also helps employees understand their role as the first line of defense in protecting sensitive data. In addition, banks may implement the asset management strategy proposed in this study to help discover critical business assets and data to improve customers' data interaction and

overall banking experience. With the asset management strategy, banks can innovate and modernize data utilization to provide a secure operation, reduce risks, and help achieve compliance objectives.

The outcome of this study may help the banks and financial industry in southeastern Canada to develop and implement secure procedures to protect businesses and customer-sensitive data from breaches due to insider threats. The banking industry can adopt the strategy identified in the study to build a security-conscious banking environment that would interact with secure procedures to protect sensitive data from breaches. The distinct security strategy around administrative controls would help the banks integrate industry best practices into the organizational culture to create security awareness that would help protect sensitive data and reduce the risk of cyber threats. The identified strategies can help the banks understand their critical asset residency, assign owners, and the appropriate level of controls that must be applied to prevent breaches. The data encryption strategy identified in this study can help IT security managers implement secure procedures to protect business-sensitive data at rest, in transit, and in use.

The outcome of this study offered strategies for the banking industry to integrate people, processes, and tools to provide a holistic security control for sensitive data. The study's outcome demonstrates the interaction between the people, the processes, and the security tools to help the banks identify and mitigate security risks within the organization. IT security managers in the banks can implement secure procedures to protect data and prevent breaches due to insider threats by creating a security-conscious

environment where people understand their roles in protecting business-sensitive data. The IT security managers can reduce the risk of cyber-attacks by implementing the strategies identified in the outcome of this study.

Implications for Social Change

Implementing a security strategy to protect data from security breaches, IT security managers in the banking industry can implement a secure procedure to ensure that business and customer-sensitive data are protected from data breaches due to insider threats. The strategies identified in this study may help IT security managers create awareness and reduce employee ignorance and maliciousness while ensuring compliance with standards and procedures to prevent breaches which may improve customers' confidence in banking and other related benefits of safe banking activities. A security-aware banking environment allows IT security managers to implement policies and procedures to protect business and customers' data to prevent breaches and improve banking integrity.

Effective security awareness improves employees' sense of responsibility and commitment to handling and protecting data. The organizational cultural influence resulting of implementing secure procedures can also be considered an implication for social change. IT leadership can use the outcome of a security culture improvement to enhance weak aspects of the business strategies for cohesiveness, work ethics, and professional codes (Tejay & Mohammed, 2023). When management innovatively communicates security policy, the security posture is improved while compliance objectives can be achieved (Omoyiola & Mckeeby, 2023). Management's involvement in

communicating an innovative security strategy to create a secure organizational culture is a positive social change. Omoyiola and Mckeeby (2023) explained the need for business leadership's support for an effective security culture, as security should be everyone's responsibility.

Security culture supports guidelines and procedures for data protection and influences human behaviors, perceptions, and interactions with the data and the security strategy. Security culture creates interactions among employees and helps them understand security best practices to easily identify any behavioral anomaly that could result in a data breach. This interaction creates security awareness and policy compliance can be another implication for social change. A secure organizational culture supports the security procedures and industry best practices and integrates secure behaviors as part of the daily employee interactions with one another (Tejay & Mohammed, 2023). Also, another implication for social change can be seen in the interactions between business leadership and employees when creating a security-conscious culture which demonstrates open communication in the organization and employees' commitment to their job. As a result, this improves morale and lowers employee turnover and overall unemployment.

The outcome of this study and the interactions between IT security managers, employees, security strategy, and business management in creating a secure culture to enhance asset management, data security, and handling, and the overall security posture to help banking industries in other parts of the world prevent data breaches due to insider threats. The result of this study may help other banks and financial industries protect business and customer-sensitive data from insider threats which may improve customers'

confidence in banking and other related benefits of safe banking activities as a positive social change in the community.

Recommendations for Action

This study explores the strategies IT security managers use in the banking industries in Southeastern Canada to prevent breaches due to insider threats. My first recommendation to the banking industry's IT security managers, Chief Information Security Officers, or Business Information Security Officers is to identify its critical assets and ensure that the security operation team understands them to provide appropriate security controls. The critical assets must be within a protected segment with restricted access and authorization controls. Such access controls must leverage the principles of least privilege with defense-in-depth.

Secondly, I recommend that the banking industry develop and enforce security policies aligning with the business's strategic objectives. The organization must ensure that every employee reads and understands the objectives and content of the security policies. Employees must abide by these policies to understand their responsibilities and how they can help protect the business and customers' sensitive data.

Thirdly, I recommend that the banking industry invest in tools that can be used to improve visibility within the organization. These tools must be able to monitor and track user activities and telemetry within the network to help analyze user behaviors. Identified metrics can be used to establish security baselines and identify control gaps. Communication among siloed tools must be improved for faster data ingestion to

improve visibility. Also, implement a robust ticketing or case management solution for the security operation team to manage visibility.

My fourth recommendation is that the banking industry build a security-aware culture with regular security-awareness training exercises for employees, contractors, and other vendors. The banking industry must ensure that all departments collaborate effectively to boost employee morale and on-the-job satisfaction. Because the threat landscape is evolving, and the number of threats is on the rise with the security tools receiving a high number of events per second (EPS) or alerts per day, there is a need to speed up the response time to give the security analyst enough time to triage events relating to insider threats faster.

Given this, my fifth recommendation is that the banking industry improve its incident management plan and automate its security processes. The banks must implement solutions that automatically trigger workflows through the detection, investigation, and response phases. This process should only alert the security team if human intervention is needed. Security automation would allow banks to prevent the never-ending security alerts that make it almost impossible to stay ahead of cyber threats.

My sixth recommendation is that the banking industry must implement a centralized alerting/case and ticketing management system. When all alerts relating to insider threats and other security alerts are centralized, the security operation team would have the correct information to understand the environments to prepare and defend against threats. In addition, the team would be prepared to understand new threats and indications of compromises within the organization. As part of centralized management,

the banking industry must integrate its security toolsets to provide the team with the necessary information to detect and prevent insider threats.

The world is becoming more connected and data-driven. Therefore, insider threat detection is now critical to organizations. Reducing the mean time to resolution (MTTR) is essential to minimizing the damages that insider threats could cause. This would help the banking industry. When the MTTR is reduced, organizations can detect and prevent insider threats from causing damage. Finally, I recommend that the banking industry develops a strategy to integrate people, processes, and technology. By integrating these elements, the security systems provide a single pane of glass to enhance monitoring and control effectiveness to prevent breaches due to insider threats.

The study's outcome would be published via ProQuest Dissertations and Theses Global and made available to the banking industry's IT security managers, CISO, BISO, and other IT security professionals working in the banking industry in the southeastern Canada, and worldwide.

Recommendation for Further Study

Findings showed that I interviewed IT security managers in the banking industry in southeastern Canada. Firstly, I recommend that further study should expand the geographical scope to include other locations in Canada as this would help the research to be more generalizable. My second recommendation is to expand the study to include payment processors that manage transactions between the banks and other customers to study the secure procedures for card data and other customer information and how they can prevent breaches due to insider threats. This qualitative pragmatic inquiry study

aimed to explore the strategies used by IT security managers in the banking industry to implement secure procedures to protect business and customer data and prevent breaches due to insider threats.

Finally, I recommend that future studies use a mixed-method design approach which combines qualitative and quantitative research methods. A combination of design methods may broaden the scope, involve more participants, and provide more data for analysis. Further research is recommended in banks in other parts of Canada. This study was conducted in the southeastern part of Canada and further study may be conducted in other parts of the country that could produce a different or more diversified outcome for preventing breaches due to insider threats. The sharing of the outcome of this study can help IT security managers in other parts of Canada to perform further studies.

Reflections

I started my journey for the Doctor of IT program in the year 2020. When I started the program, I was curious to know how rigorous and time-consuming it would be. I was unsure of my research topics and struggled to combine the study with work and family life. However, in the learning process, I conceived ideas around either robotic process automation research or insider threats in the banking industry. Because of my experience in the financial industry, I have always wanted to research on how to improve security within the industry, which would contribute to the development of the banking industry. Also, considering the rise in cyber threats globally and the enormous impacts on banks and other financial institutions, I settled on developing strategies to prevent breaches due to insider threats in the banking industry. Developing secure procedures for the banking

industry to prevent breaches due to insider threats would contribute to positive social change for the industry, especially in southeastern Canada.

After I selected the topic and got approval from Walden University IRB, I was faced with the challenge of getting my study participants because only a few employees of banks were willing to participate for fear of disclosing sensitive information. Also, financial industry employees would want to keep their security strategies private from outsiders. I had to build a working relationship with some employees by connecting with them via emails and social media platforms such as LinkedIn. I also developed relationships with other people related to these banking industry employees to facilitate my relationship with them. Creating such a relationship was essential for the success of my research study as it accelerated the response, willingness, and interview sessions.

A significant milestone for me in this journey was receiving the approval for my proposal. I was overwhelmed with joy. I appreciate my current chair for all the tremendous feedback and directions that helped me meet the requirements for the doctoral proposal. Before my current chair, I needed proper guidance, communication, and directions from my previous chair for my study, which was very frustrating for me. However, my current chair came in, and I achieved my most significant milestone in less than a month. I am glad for all I have achieved with my current chair as I saw more lights at the end of the tunnel. I imagined the joy I felt walking down the stage to receive my degree.

Overall, I enjoyed my journey throughout the Doctor of IT program. My growth was evident as a researcher and IT professional from the beginning of my program until

completion. I appreciate the opportunity I had to research strategies that would help the banking industry develop secure procedures to prevent breaches due to insider threats and increase security awareness for employees and contractors within the banks to help protect sensitive business and customer data.

Conclusions

This qualitative pragmatic inquiry study aimed to explore the effectiveness of the security strategy that IT security managers use in the banking industry to implement secure procedures to protect customer and organizational data from breaches due to insider threats. I purposefully selected 6 IT security managers in the banking industry in southeastern Canada, aiming to improve their data security strategies. I used interview protocols, field notes and reviewed industry security documents for the data collection for this study. The 6 themes emergent from the data analysis were this qualitative pragmatic study: (a) the need for security standards, procedures, and policies, (b) the need for information security education and training, (c) the importance of organizational security culture, (d) the importance of asset management, (e) the importance of identity and access management, and (f) the importance of data security. The outcome of this study indicates the need for business leadership involvement in security, building a culture of security in the banks where employees and contractors have adequate security awareness and education.

As data becomes a critical asset for organizations, banks, and other financial institutions have derived values from this for innovation and operational modernization. As a result, the need for data security and governance has become an integral part of

banking operations. The banks are obligated to their customers and regulatory bodies to ensure that business and customer-sensitive data have appropriate security controls to prevent breaches. The IT security managers should understand the business strategy and tailor the security strategy by integrating the people, processes, and technology to help the business achieves its objectives.

The IT security managers should understand the need to identify and protect business-critical assets, the need for identity and access management, the need for data encryption, the need for security awareness for employees, the importance of security policies, standards, procedures, and frameworks that can help protect sensitive organizational data. Also, the business leadership must be involved in promoting a security-aware culture in the organization. The IT security managers in the banking industry should subscribe to security intelligence feeds and groups for information sharing and to get threat intelligence and industry best practices for security in the banking industry.

IT leaders in the banking industry can adopt the strategy in the outcome of this study to create positive social change by improving its security controls and developing secure procedures to protect sensitive business and customer data to create a safe banking experience and build customer confidence in the banks.

References

Abaid, Z., Saadat, A., & Mirza, B. M. (2023). The insider threat landscape and the fintech sector: Attacks, defenses, and emerging challenges. *In Handbook of research on cybersecurity issues and challenges for business and fintech applications* (pp. 65-90). IGI.

Abboubi, M. E., Pinnington, A. H., Clegg, S. R., & Nicolopoulou, K. (2022). Involving, countering, and overlooking stakeholder networks in soft regulation: Case study of a small-to-medium-sized enterprise's implementation of SA8000. *Business & Society*, 61(6), 1594-1630.

Abram, M. D., Mancini, K. T., & Parker, R. D. (2020). Methods to integrate natural language processing into qualitative research. *International Journal of Qualitative Methods*, 19, 1- 6. https://doi.org/10.1177/1609406920984608

Abulencia, J. (2021). Insider attacks: Human-factors attacks and mitigation. *Computer Fraud & Security,* 2021(5), 14-17. https://doi.org/10.1016/S1361-3723(21)00054-3

Adekoya, A. A., & Guse, L. (2020). Walking interviews and wandering behavior: Ethical insights and methodological outcomes while exploring the perspectives of older adults living with dementia. *International Journal of Qualitative Methods*,19, 1-6. https://doi.org/10.1177/1609406920920135

Adler, R. H. (2022). Trustworthiness in qualitative research. *Journal of Human Lactation*, 38(4), 598-602.

Afzaal, H., & Zafar, N. (2016). Formal analysis of subnet-based failure recovery algorithm in wireless sensor and actor and network. *Complex Adaptive Systems*

Modeling, 4(1), 1–27. https://doi.org/10.1186/s40294-016-0037-4

Agrawal, N. (2021). Telephone network and internet penetration in India: A pragmatic study using data analytics. *Global Journal of Enterprise Information System*, 13(1), 42–47. https://doi.org/10.18311/gjeis/2021

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. (2020). Situation awareness in incident response: An in-depth case study and process model. *ICIS 2020 Proceedings*, 1. https://aisel.aisnet.org/icis2020/cyber_security_privacy/cyber_security_privacy/1

Aka, G. K. (2019). Actor-network theory to understand, track and succeed in a sustainable innovation development process. *Journal of Cleaner Production, 225,* 524-540. https://doi.org/10.1016/j.jclepro.2019.03.351

Alase, A. (2017). The interpretative phenomenological analysis: A guide to a good qualitative research approach. *International Journal of Education and Literacy Studies*, 5(2), 9–19. https://doi.org/10.7575/aiac.ijels.v.5n.2p.9

Aldbis, A., Naal, H., Kishawi, T., Wazni, R., & Abbara, A. (2023). The lived experience of patients with conflict associated injuries whose wounds are affected by antimicrobial resistant organisms: A qualitative study from northwest Syria. *Conflict and Health,* 17(1), 1-12.

Al-Eisawi, D. (2022). A design framework for novice using grounded theory methodology and coding in qualitative research: Organizational absorptive capacity and knowledge management. *International Journal of Qualitative Methods*, 21.

Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Abdulkareem, K. H., Mohammed, M. A., Gupta, D., & Shankar, K. (2022). A new intelligent multilayer framework for insider threat detection, *Computers & Electrical Engineering*. https://doi.org/10.1016/j.compeleceng.2021.107597.

AlSlaiman, M., Salman, M. I., Saleh, M. M., & Wang, B. (2023). Enhancing false negative and positive rates for efficient insider threat detection, *Computers & Security*, 126. https://doi.org/10.1016/j.cose.2022.103066.

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organization. *Computer & Security*, 100,. https://doi.org/10.1016/j.cose.2020.102090

Alison, J. C., Bell, M., Rogers, 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

Altaf, K., Ayub, H., Shabbir, M. S., & Usman, M. (2022). Do operational risk and corporate governance affect the banking industry of Pakistan? *Review of Economics and Political Science*, 7(2), 108-123.

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), https://doi.org/10.1016/j.heliyon.2021.e06016

Andress, J. (2014). The Basics of Information Security (Second Edition), *Syngress,*

https://doi.org/10.1016/B978-0-12-800744-0.00008-7.

Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Cyber security skills gap: Using tabletop exercises to solve the CSSG crisis, serious games. *Security and Privacy*, 3(6), 117–131. https://doi.org/10.1002/spy2.126

Antonietti, C., Schmitz, M. L., Consoli, T., Cattaneo, A., Gonon, P., & Petko, D. (2023). Development and validation of the ICAP Technology Scale to measure how teachers integrate technology into learning activities. *Computers & Education*, 192, 104648.

Arquilla, J., & Guzdial, M. (2020). Transitioning to distance learning and virtual conferencing. https://doi.org/10.1145/3398386

Asha, S., Shanmugapriya, D., & Padmavathi, G. (2023). Malicious insider threat detection using variation of sampling methods for anomaly detection in cloud environment, *Computers and Electrical Engineering.* https://doi.org/10.1016/j.compeleceng.2022.108519.

Atakav, E., Jarvis, L., & Marsden, L. (2020). Researching British [Muslim] values: Vernacular politics, digital storytelling, and participant researchers. *International Journal of Qualitative Methods*, 19, 1-11. https://doi.org/10.1177/1609406920938281

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and privacy: Concerned, confused, and feeling lack of control over their personal information. *Pew Research Center*. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-

of-control-over-their-personal-information/

Ayaburi, E. W. (2023). Understanding online information disclosure: examination of data breach victimization experience effect. *Information Technology & People*, 36(1), 95-114. https://doi.org/10.1108/ITP-04-2021-0262

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Bella, G., Biondi, P., & Bognanni, S. (2022). Multi-service threats: Attacking and protecting network printers and VoIP phones alike, *Internet of Things*. https://doi.org/10.1016/j.iot.2022.100507.

Beresford, M., Jones, J. L., Bausch, J. C., Williams, C. F., Wutich, A., Porter, S., Quimby, B., Eaton, W. M., & Brasier, K. J. (2020). Third-party effects in stakeholder interviews. *International journal of qualitative methods*,19-1-9. https://doi.org/10.1177/1609406920966482

Bergström, E., Lundgren, M., & Ericson, A. (2019). Revisiting information security risk management challenges: A practice perspective. *Information & Computer Security*, 27(3), 358–372. https://doi.org/10.1108/ics-09-2018-0106

Binks, A. (2019). The art of phishing: past, present, and future. *Computer Fraud & Security*, 2019(4), 9–11. https://doi.org/10.1016/S1361-3723(19)30040-5

Birke, F. M., & Knierim, A. (2020). ICT for agriculture extension: Actor-network theory for understanding the establishment of agricultural knowledge centers in South Wollo, Ethiopia. *Information Technology for Development*, 26(3), 591–606.

https://doi.org/10.1080/02681102.2020.1727826

Blank, T. C., Kohlhofer, D. B., & Bonaccorsi, H. (2016). Regulatory monitor. *Investment Lawyer,* 23, 28–30. Retrieved from http://www.aspenpublishers.com

Blažič, B. J. (2021). The cybersecurity labor shortage in Europe: Moving to a new concept for education and training, *Technology in Society*, 67. https://doi.org/10.1016/j.techsoc.2021.101769

Borenius, S., Gopalakrishnan, P., Bertling Tjernberg, L., & Kantola, R. (2022). Expert-Guided Security Risk Assessment of Evolving Power Grids. *Energies*, 15(9), 3237.

Boto-García, D. (2023). Hospitality workers' awareness and training about the risks of online crime and the occurrence of cyberattacks, Journal of Hospitality and Tourism Management, 55, 240-247. https://doi.org/10.1016/j.jhtm.2023.04.010.

Brawn, V., & Clarke, V. (2019). To saturate or not to saturate, questioning data saturation as a useful concept for thematic analysis and sample size-size rationales. Qualitative Research in Sport, Exercise and Health, 13(2). https://doi.org/10.1080/2159676X.2019.1704846

Brear, M. (2019, June). Process and outcomes of a recursive, dialogic member checking approach: A project ethnography. Qualitative Health Research, 29(7), 944–957. https://doi.org/10.1177/1049732318812448

Bremner, N. (2020). Time for timelines: The take-home timeline as a tool for exploring complex life histories. International journal of qualitative methods,19, 1-13. https://doi.org/10.1177/1609406920948978

Brimblecombe, F. (2020). The public interest in deleted personal data? The right to be forgotten's freedom of expression exceptions examined through the lens of Article 10 ECHR. *Journal of Internet Law*, 23(10).

Brower, R. L., Jones, T. B., Osborne-Lampkin, L., Hu, S., & Park-Gaghan, T. J. (2019). Big qual: Defining and debating qualitative inquiry for large data sets. *International Journal of Qualitative Methods*, 18, 1-10. https://doi.org/10.1177/1609406919880692

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.

Brothers, K. B., Rivera, S. M., Cadigan, R. J., Sharp, R. R., & Goldenberg, A. J. (2019). A belmont reboot: Building a normative foundation for human research in the 21st century. *The Journal of Law, Medicine & Ethics*, 47(1), 165-172 https://doi.org/10.1177/1073110519840497

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

Burga, R., & Rezania, D. (2017). Project accountability: An exploratory case study using actor-network theory. *International Journal of Project Management*, 35, 1024-1036. https://doi:10.1016/j.ijproman.2017.05.001

Callon, M., & Law, J. (1997). After the individual in society: Lessons on collectivity from science, technology, and society. *Canadian Journal of Sociology/Cahiers canadiens de sociologie*, 22 (2), 165-182. https://doi.org/10.2307/3341747

Campean, S. (2019). The human factor at the center of a cyber security culture. *International Journal of Information Security & Cybercrime*, 8(1), 51–58. https://doi.org/10.19107/ijisc.2019.01.07

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: Complex or simple? Research case examples. *Journal of Research in Nursing*, 25(8), 652–661. https://doi.org/10.1177/1744987120927206

Candela, A. G. (2019). Exploring the Function of Member Checking. The Qualitative Report, 24(3), 619-628. https://doi.org/10.46743/2160-3715/2019.3726

Caretta, M. A., & Perez, M. A. (2019). When participants do not agree: Member checking and challenges to epistemic authority in participatory research. *Field Methods*, 31(4), 359–374. https://doi.org/10.1177/1525822X19866578

Carmichael, T., & Hadzikadic, M. (2019). The Fundamentals of Complex Adaptive Systems. https://DOI:10.1007/978-3-030-20309-2_1

Catak, F. O., Yazı, A. F., Elezaj, O., & Ahmed, J. (2020). Deep learning based sequential model for malware analysis using windows exe API calls. *PeerJ Computer Science*. https://doi.org/10.7717/peerj-cs.285

Coleman, P. (2022). Validity and reliability within qualitative research for the caring sciences. *International Journal of Caring Sciences*, 14(3), 2041-2045.

Côté-Boileau, E., Gaboury, I., Breton, M., & Denis, J.-L. (2020). Organizational ethnographic case studies: Toward a new generative in-depth qualitative methodology for health care research? *International journal of qualitative methods*,

19, 1-17. https://doi.org/10.1177/1609406920926904

Champagne-Poirier, O., Carignan, M. E., David, M. D., & O'Sullivan, T. (2021). Understanding and quantifying: A mixed-method study on the journalistic coverage of Canadian disasters. *International journal of qualitative methods*, 20, 1-13. https://doi.org/10.1177/1609406921990492

Chan, N. N., Ahrumugam, P., Scheithauer, H., Schultze-Krumbholz, A., & Ooi, P. B. (2020). A descriptive phenomenological study of students' and school counsellors' lived experiences of cyberbullying and bullying. *Computers & Education*, 146, 103755. https://doi.org/10.1016/j.compedu.2019.103755

Chang, D. F. (2014). Increasing the trustworthiness of qualitative research with member checking. In PsycEXTRA Dataset (pp. 109-115). http://doi.org/10.1037/e530492014-001

Chang, S. I., Chang, L. M., & Liao, J. C. (2020). Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach. *Information & Management*, 57(6), 103335. https://doi.org/10.1016/j.im.2020.103335

Chapman, P. (2021). Defending against insider threats with network security's eighth Layer. *Computer Fraud & Security*, 2021 (3), 8 - 13. https://doi.org/10.1016/S1361-3723(21)00029-4.

Chauvette, A., Schick-Makaroff, K., & Molzahn, A. E. (2019). Open data in qualitative research. *International journal of qualitative methods*, 18, 1-6. https://doi.org/10.1177/1609406918823863

Chen, Y., & Wu, S. (2021). An exploration of actor-network theory and social affordance for the development of a tourist attraction: A case study of a Jimmy-related theme park, Taiwan, *Tourism Management,* 82, 104206. https://doi.org/10.1016/j.tourman.2020.104206.

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed? *Journal of Information Systems*, 33(3), 163–182. https://doi.org/10.2308/isys-52410

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: *Taxonomising countermeasures, Computers & Security*, 87, https://doi.org/10.1016/j.cose.2019.101568.

Cornejo, M., Bustamante, J., Del Río, M., De Toro, X., & Latorre, M. S. (2023). Researching with Qualitative Methodologies in the Time of Coronavirus: Clues and Challenges. *International Journal of Qualitative Methods*, 22. https://doi.org/10.1177/16094069221150110

Côté-Boileau, E., Gaboury, I., Breton, M., & Denis, J.-L. (2020). Organizational ethnographic case studies: Toward a new generative in-depth qualitative methodology for health care research? *International journal of qualitative methods*, 19, 1-17. https://doi.org/10.1177/1609406920926904

Cresswell, K. M., Worth, A., & Sheikh, A. (2010). Actor-network theory and its role in understanding the implementation of information technology developments in healthcare. *BMC medical informatics and decision making*, 10, 67-77. https://doi:10.1186/1472-6947-10-67

Cross, C., Parker, M., & Sansom, D. (2019). Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach. *International Review of Victimology*, 25(1), 53-69. https://doi.org/10.1177/0269758017752410

Crowley, M. G., & Johnstone, M. N. (2016). Protecting corporate intellectual property: Legal and technical approaches. *Business Horizons*, 59, 623-633. https://doi:10.1016/j.bushor.2016.08.004

Crumpler, W., & Lewis, J. A. (2019). The Cybersecurity workforce gap. Center for Strategic & International Studies. https://csis-website- prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf

Cumyn, A., Ouellet, K., Côté, A. M., Francoeur, C., & St-Onge, C. (2019). Role of researchers in the ethical conduct of research: A discourse analysis from different stakeholder perspectives. *Ethics & Behavior*, 29(8), 621-636. https://doi.org/10.1080/10508422.2018.1539671

Cybersecurity Maturity Model Certification Version 2.0. *Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov/resources-tools/resources/cybersecurity-maturity-model-certification-20-program.

da Silva, G. M. B. (2022). A study of implementing theory of constraints healthcare services.

Das, M. S., Govardhan, A., & Doddapaneni, V. L. (2021). A Model of Cloud Forensic Application With Assurance of Cloud Log. I*nternational Journal of Digital Crime and Forensics* (IJDCF), 13(5), 114-129. doi: http://10.4018/IJDCF.20210901.oa7

Dasaklis, T. K., Voutsinas, T. G., Tsoulfas, G. T., & Casino, F. (2022). A systematic literature review of blockchain-enabled supply chain traceability implementations. *Sustainability*, 14(4), 2439.

Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S., & Pitner, T. (2023). Addressing insider attacks via forensic-ready risk management, *Journal of Information Security and Applications*. https://doi.org/10.1016/j.jisa.2023.103433.

Dawson, J., & Jöns, H. (2018). Unravelling legacy: A triadic actor-network theory approach to understanding the outcomes of mega events. *Journal of Sport & Tourism*, 22, 43–65. https://doi:10.1080/14775085.2018.1432409

De Buitrago, S. (2019). Risk representations and confrontational actions in the arctic. *Journal of strategic security*, 12(3), 13-36. https://www.jstor.org/stable/26775813

Deason, G., Seekamp, E., & Barbieri, C. (2022). Actor-network theory and organizational resilience to climate change in community-based tourism, *Journal of Outdoor Recreation and Tourism,* https://doi.org/10.1016/j.jort.2021.100483.

Deep, G., Sidhu, J., & Mohana, R. (2022). Insider threat prevention in distributed database as a service cloud environment, *Computers & Industrial Engineering,* 169. https://doi.org/10.1016/j.cie.2022.108278.

Desai, A., Zoccatelli, G., Adams, M., Allen, D., Brearley, S., Rafferty, A. M., & Donetto, S. (2017). Taking data seriously: The value of actor-network theory in rethinking patient experience data. *Journal of Health Services Research & Policy*, 22, 134-136. https://doi.org/10.1177/1355819616685349

Despujol, I., Castañeda, L., Marín, V. I., & Turró, C. (2022). What do we want to know

about MOOCs? Results from a machine learning approach to a systematic literature mapping review. *International Journal of Educational Technology in Higher Education*, 19(1), 1-22.

Dharmawansa, A. D., & Madhuwanthi, R. A. M. (2020). Evaluating the Information Security Awareness (ISA) of employees in the banking sector: A case study.

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. *Sensors*, 23(3), 1151.

Díaz, J., Pérez, J. E., Lopez-Peña, M. A., Mena, G. A., & Yagüe, A. (2019). Self-service cybersecurity monitoring as enabler for DevSecOps. *IEEE Access*, 7, 100283-100295. https://doi.org/10.1109/ACCESS.2019.2930000

DiGiacinto, D. (2019). The Importance of the internal review board for approving proposed research. *Journal of Diagnostic Medical Sonography*, 35(2), 85–86. https://doi.org/10.1177/8756479318817220

Dincelli, E., & Chengalur-Smith, I. (2020). Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems*, 29(6), 669-687.

DLA Piper Intelligence. (2020). Data protection laws of the world: *Definition of personal data.* Retrieved from https://www.dlapiperdataprotection.com/index.html?t=definitions&c=US

do Céu Morais Cláudio, M., & Santos, A. (2023, January). Strategic Alignment of Knowledge Management Systems. In *Technology and Innovation in Learning,*

Teaching and Education: Third International Conference, TECH-EDU 2022, Lisbon, Portugal, August 31–September 2, 2022, Revised Selected Papers (pp. 418-433). Cham: Springer Nature Switzerland.

Dumay, J., & Rooney, J. (2016). Numbers versus narrative: An examination of a controversy. *Financial Accountability & Management*, 32, 202–231. https://doi:10.1111/faam.12086

Dyar, K. L. (2022, January). Qualitative inquiry in nursing: Creating rigor. In *Nursing Forum* (Vol. 57, No. 1, pp. 187-200).

Eakin, J. M., & Gladstone, B. (2020). Value-adding analysis: Doing more with qualitative data. *International journal of qualitative methods*, 19, 1-13. https://doi.org/10.1177/1609406920949333

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

Elder-Vass, D. (2015). Disassembling Actor-network Theory. *Philosophy of the Social Sciences*, 45(1), 100–121. https://doi.org/10.1177/0048393114525858

Eldh, A. C., Årestedt, L., & Berterö, C. (2020). Quotations in qualitative studies: reflections on constituents, custom, and purpose. *International journal of qualitative methods*, 19,1-6. https://doi.org/10.1177/1609406920969268

Elmrabit, N., Yang, S., Yang, L., & Zhou, H. (2020). Insider Threat Risk Prediction based on Bayesian Network, *Computers & Security*, 96. https://doi.org/10.1016/j.cose.2020.101908.

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis, *IEEE Access*, 10, 52319-52335. https://doi10.1109/ACCESS.2022.3171829

Erola, A., Agrafiotis, I., Goldsmith, M., & Creese, S. (2022). Insider-threat detection: Lessons from deploying the CITD tool in three multinational organizations, *Journal of Information Security and Applications.* https://doi.org/10.1016/j.jisa.2022.103167.

Etz, R. S., Gonzalez, M. M., Crabtree, B. F., Reves, S. R., & Stange, K. C. (2019). An innovative three-step method for identifying exemplars. *International journal of qualitative methods*, 18, 1-7. https://doi.org/10.1177/1609406919867794

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2022). Chapter 11 - Development and application of the Information Security Core Human Error Causes (IS-CHEC) technique, *Cybersecurity and Cognitive Science*, https://doi.org/10.1016/B978-0-323-90570-1.00010-3.

Evans, M., He, Y., Maglaras, L., Yevseyeva, I., & Janicke, H. (2019). valuating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector, *International Journal of Medical Informatics*, 127, 109-119, https://doi.org/10.1016/j.ijmedinf.2019.04.019.

Fahlevi, M., Zuhri, S., Parashakti, R., & Ekhsan, M. (2019). Leadership styles of food truck businesses. *Journal of Research in Business, Economics and Management*, 13(2), 2437-2442. https://www.researchgate.net/

Farley, R. (2020). The Importance of Census 2020 and the Challenges of Getting a

Complete Count. Harvard Data Science Review, 2(1), https://doi.org/10.1162/99608f92.8a0cc85c

Farzan, F., Lahiri, S., Kleinberg, M., Gharieh, K., Farzan, F., & Jafari, M. (2013). Microgrids for fun and profit: The economics of installation investments and operations. *IEEE Power and Energy Magazine*, 11, 52–58. https://doi:10.1109/mpe.2013.2258282

Fay, J. J., & Patterson, D. (2018). Chapter 24 - The Importance of Policies and Procedures, *Contemporary Security Management (Fourth Edition),* Butterworth-Heinemann, 495-522, https://doi.org/10.1016/B978-0-12-809278-1.00024-4.

Fei, Z., Wang, X., & Wang, Z. (2021). Event-Based Fault Detection for Unmanned Surface Vehicles Subject to Denial-of-Service Attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 1-11. https://doi:10.1109/tsmc.2021.3064884

Floricel, S., Bonneau, C., Aubry, M., & Sergi, V. (2014). Extending project management research: Insights from social theories. I*nternational Journal of Project Management,* 32, 1091-1107. https://doi:10.1016/j.ijproman.2014.02.008

Fofana, F., Bazeley, P., & Regnault, A. (2020). Applying a mixed methods design to test saturation for qualitative data in health outcomes research. *PLoS ONE* 15(6), 1-12. https://doi.org/10.1371/journal.pone.0234898

Frechette, J., Bitzas, V., Aubry, M., Kilpatrick, K., & Lavoie-Tremblay, M. (2020). Capturing Lived Experience: Methodological Considerations for Interpretive Phenomenological Inquiry. *International journal of qualitative methods*, 19, 1-12.

https://doi.org/10.1177/1609406920907254

Gale, N. K., Heath, G., Cameron, E., Rashid, S., & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology*, 13, 117. http://doi:10.1186/1471-2288-13-117

Ge, M., Cho, J. H., Kim, D., Dixit, G., & Chen, I. R. (2021). Proactive defense for internet-of-things: Moving target defense with Cyber deception. *ACM Transactions on Internet Technology* (TOIT), 22(1), 1-31. https://doi.org/10.1145/3467021

Gelling, L. (2019). Research ethics in real world research, *Journal of Clinical Nursing* 29(7), 1019-1022. https://doi.org/10.1111/jocn.15083

Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. *Authorea Preprints*.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints.*

Gibaldi, J., & Siddiqi, B. (2019, September). Retention strategies for keeping participants engaged: A case study of the Parkinson's progression markers initiative. *Applied Clinical Trials*, 28(9), 20–21. http://www.appliedclinicaltrialsonline.com/

Gilmore, B., McAuliffe, E., Power, J., & Vallières, F. (2019). Data analysis and synthesis within a realist evaluation: toward more transparent methodological approaches. *International journal of qualitative methods*,18, 1-11. https://doi.org/10.1177/1609406919859754

Giraldo, J. A., El Hariri, M., & Parvania, M. (2022). Moving Target Defense for Cyber–

Physical Systems Using IoT-Enabled Data Replication. *IEEE Internet of Things Journal,* 9(15), 13223-13232.

Glenton, C., & Carlsen, B. (2019). When normal becomes normative: A case study of researchers' quotation errors when referring to a focus group sample size study. *International journal of qualitative methods*, 18, 1-6. https://doi.org/10.1177/1609406919841251

Goldratt, E. M., & Cox, J. (1984). The Goal, Croton-on-Hudson. NY: *North River Press Inc.*

Goopy, S., & Kassan, A. (2019). Arts-based engagement ethnography: An approach for making research engaging and knowledge transferable when working with harder-to-reach communities. *International journal of qualitative methods*,18, 1-10. https://doi.org/10.1177/1609406918820424

Govender, I., Watson, B. W. W., & Amra, J. (2021). Global virus lockdown and cybercrime rate trends: a routine activity approach. *Journal of Physics*: Conference Series, 1828. https://doi.org//10.1088/1742-6596/1828/1/012107

Grabowski, L. J., & Mathiassen, L. (2013). Real estate decision-making as actor networks. *Journal of Corporate Real Estate*, 15(2), 136-149. https://doi:10.1108/JCRE-11-2012-0023

Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering, *Procedia Computer Science*, 181, 59-66. https://doi.org/10.1016/j.procs.2021.01.103.

Green, B., Gies, S., Bobnis, A., Piquero, N. L., Piquero, A. R., & Velasquez, E. (2020).

The role of victim services for individuals who have experienced serious identity-based crime. *Victims & Offenders*, 15(6), 720–743. https://doi.org/10.1080/15564886.2020.1743804

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. MIS Quarterly, 37, 337-355. Retrieved from http://www.misq.org/

Griensven, H. V., Moore, A. P., & Hall, V. (2014). Mixed methods research: The best of both worlds? Manual Therapy, 19, 367-371. http://doi:10.1016/j.math.2014.05.005

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. *Frontiers in Big Data*, 2021(4), 1–24. https://doi.org/10.3389/fdata.2021.583723

Guba, E. G., & Lincoln, Y. S. (1989). *Fourth generation evaluation*. Sage Publications.

Guedes, J. A. S., Fonseca, R. D. C., & Strauhs, F. D. R. (2023). Semantic portals from sociotechnical perspective of the actor-network theory. *Perspectivas em Ciência da Informação*, 27, 54-80.

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. PLOS One, 15(5). https://doi.org/10.1371/journal.pone.0232076

Guetterman, T. C., Sakakibara, R. V., Plano Clark, V. L., Luborsky, M., Murray, S. M., Castro, F. G., Creswell, J. W., Deutsch, C., & Gallo, J. J. (2019). Mixed methods grant applications in the health sciences: An analysis of reviewer comments. *Journal PLOS ONE*, https://doi.org/10.1371/journal.pone.0225308

Gunawong, P., & Gao, P. (2017). Understanding e-government failure in the developing country context: A process-oriented study. *Information Technology for Development,* 23, 153-178. https://doi:10.1080/02681102.2016.1269713

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, 34(7), 808–834. https://doi.org/10.1108/maj-09-2018-2004

Hagues, R. (2019). Conducting critical ethnography: Personal reflections on the role of the researcher. *International Social Work*, 64(3), 002087281881973. https://doi.org/10.1177/0020872818819731

Hajli, N., Saeed, U., Tajvidi, M., & Shirazi, F. (2022). Social bots and the spread of disinformation in social media: the challenges of artificial intelligence. *British Journal of Management*, 33(3), 1238-1253.

Hamilton, A. B., & Finley, E. P. (2019). Qualitative methods in implementation research: An introduction. https://DOI: 10.1016/j.psychres.2019.112516

Hanseth, O., Aanestad, M., & Berg, M. (2004). Guest editors' introduction: Actor-network theory and information systems. What's so special? *Information Technology & People*, 17, 116-123. https://doi:10.1108/09593840410542466

Hardy, J., Sass, M., & Fifekova, M. P. (2011). Impacts of horizontal and vertical foreign investment in business services: The experience of Hungary, Slovakia and the Czech Republic. *European Urban and Regional Studies*, 18, 227-243. https://doi:10.1177/0969776411422618

Harms, P. D., Marbut, A., Johnston, A. C., Lester, P., & Fezzey, T. (2022). Exposing the darkness within: A review of dark personality traits, models, and measures and

their relationship to insider threats, J*ournal of Information Security and Applications*, (71), https://doi.org/10.1016/j.jisa.2022.103378.

Harnesk, D., & Lindström, J. (2011). Shaping security behavior through discipline and agility: Implications for information security management. *Information Management & Computer Security*, 19, 262-276. doi:10.1108/09685221111173076

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95. https://doi.org/10.1016/j.cose.2020.101827

Haven, T. L., & Van Grootel, D. L. (2019). Preregistering qualitative research. *Accountability in Research*, 26(3), 229–244. https://doi.org/10.1080/08989621.2019.1580147

Hedstrom, K., Dhillon, G., & Karlsson, F. (2010). Using Actor Network Theory to Understand Information Security Management. *IFIP-Advances-in-Information-and-Communication-Technology*-1868-4238 http://dx.doi.org/10.1007/978-3-642-15257-3_5

Ho, S. M., & Gross, M. (2021). Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness. *Computers & Security* 108 https://doi.org/10.1016/j.cose.2021.102357

Hoang, L. T., Wee, M., & Yang, J. W. (2023). Strategic trading by insiders in the presence of institutional investors, *Journal of Financial Markets*. https://doi.org/10.1016/j.finmar.2022.100802.

Holland, N. (2020). The human-centric cybersecurity stance. Available at: https://www.bankinfosecurity.com/human-centric-cybersecurity-stance-a-13897 (Accessed July 08, 2020). doi:10.1287/2961bfc6-3c5b-481a-ae7c-47edf9c88831

Hostrup M. & Anderson, B. L. (2020). Leading to make a difference for whom? How vision content moderates the relationship between transformational leadership and public service motivation. *International Public Management Journal*, https://doi.org/10.1080/10967494.2020.1795015

Howell, C. J., Burruss, G. W., Maimon, D., & Sahani, S. (2019). Website defacement and routine activities: Considering the importance of hackers' valuations of potential targets. *Journal of Crime and Justice*, 42(5), 536–550. https://doi.org/10.1080/0735648x.2019.1691859

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture* https://doi.org/10.1111/j.1540-5915.2012.00361.x

Hurst, W., Tekinerdogan, B., Alskaif, T., Boddy, A., & Shone, N. (2022). Securing electronic health records against insider-threats: *A supervised machine learning approach, Smart Health,* 26. https://doi.org/10.1016/j.smhl.2022.100354.

Ikeziri, L. M., Souza, F. B. D., Gupta, M. C., & de Camargo Fiorini, P. (2019). Theory of constraints: Review and bibliometric analysis. *International Journal of Production* Research, 57, 5068-5102. https://doi:10.1080/00207543.2018.1518602

Iskanderov1a, Y., & Pautov, M. (2022). Agents and multi-agent systems as actor-networks.

Iskandarova, M. (2017). From the idea of scale to the idea of agency: An actor-network theory perspective on policy development for renewable energy. *Science & Public Policy*, 44, 476-485. https://doi:10.1093/scipol/scw075

Iskanderov, Y., Svistunova, A., Khasanov, D., & Pautov, M. (2023). Using Actor-Network Theory to Understand Intelligent Systems: The Case of Intelligent IS for Logistics. *In Cyber-Physical Systems and Control II*, 381-391. https://doi.org/10.1007/978-3-031-20875-1_35

ISO/IEC 27001 Information security management systems. https://www.iso.org/standard/27001

ISO/IEC TS 27008:2019. Information technology — Security techniques — Guidelines for the assessment of information security controls (second edition). https://www.iso27001security.com/html/27008.

Ivey, J. (2020). Participation and Recruitment. Pediatric Nursing, 46(3), 152–153. https://link.gale.com/apps/doc/A627278456/EAIM?u=minn4020&sid=ebsco&xid=2be27ea5

Iyamu, T., & Mgudlwa, S. (2018). Transformation of healthcare big data through the lens of actor network theory. *International Journal of Healthcare Management*, 11, 182-192. https://doi:10.1080/20479700.2017.1397340

Jaafar, G., Abdullah, S., & Ismail, S. (2019). Review of recent detection methods for http DDoS attack. *Journal of Computer Networks and Communications*, 2019.

https://doi.org/10.1155/2019/1283472

Jackson, S. (2015). Toward an analytical and methodological understanding of actor-network theory. *Journal of Arts & Humanities*, 4(2), 29-44. https://doi:10.18533/journal.v4i2.210

Jahja, A. S., Sri Ramalu, S., & Razimi, M. S. A. (2021). Generic qualitative research in management studies. Journal Riset Akuntansi Dan Bisnis, 7(1), 1–13. https://doi.org/10.38204/jrak.v7i1.523

Jain, N. (2021). Survey versus interviews: Comparing data collection tools for exploratory research. *The Qualitative Report*, 26(2). https://doi.org/10.46743/2160-3715/2021.4492

Janis, I., Alias, M., Zulkipli, M., & Muhammad-Sukki, F. (2020). Using illustrations to make decisions on the most appropriate qualitative research methodology: The industry 4.0 scenario. *International journal of qualitative methods*, 19, 1-16. https://doi.org/10.1177/1609406920907247

Janjua, F., Masood, A., Abbas, H., & Rashid, I. (2020). Handling Insider Threat Through Supervised Machine Learning Techniques, *Procedia Computer Science*, 177, 64-71. https://doi.org/10.1016/j.procs.2020.10.012.

Jeon, J., Park, J. H., & Jeong, Y. (2020). Dynamic analysis for IoT malware detection with convolution neural network model. *IEEE Access*,8,96899-96911. https://doi.org/10.1109/ACCESS.2020.2995887

Jeong, M., & Zo, H. (2021). Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques, *Telematics, and Informatics*.

https://doi.org/10.1016/j.tele.2021.101670.

Jofre, M., Navarro-Llobet, D., Agulló, R., Puig, J., Gonzalez-Granadillo, G., Mora Zamorano, J., & Romeu, R. (2021). Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach. Applied Sciences, 11(15), 6699. doi: https://doi.org/10.3390/app11156699

Johnson, J. L., Adkins, D., & Chauvin, S. (2020). A review of the quality indicators of rigor in qualitative research. *American Journal of Pharmaceutical Education,* 84(1). https://doi.org/10.5688/ajpe7120

Johri, A., & Kumar, S. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. *Human Behavior and Emerging Technologies*, 2023.

Jones, D. (2022, April 27). Ransomware attacks, payouts soared worldwide in 2021: report. Cybersecurity Dive. https://www.cybersecuritydive.com/news/ransomware-attacks-payouts-2021/622784/

Jones, K. R., Gwynn, E. P., & Teeter, A. M. (2019). Quantitative or qualitative: selecting the right methodological approach for credible evidence. *Journal of Human Sciences and Extension,* 7(2), 61– 87. https://www.jhseonline.com/article/view/826

Juniper Research. (2019, August 27). Business losses to cybercrime data breaches to exceed $5 trillion by 2024 [Press release]. https://www.businesswire.com/news/home/20190826005013/en/Business-Losses-

Cybercrime-Data-Breaches-Exceed-5

Kammüller, F., & Kerber, M. (2021). Applying the Isabelle Insider framework to airplane security, *Science of Computer Programming*. https://doi.org/10.1016/j.scico.2021.102623.

Kamravamanesh, M., Kohan, S., Rezavand, N., & Farajzadegan, Z. (2018). A comprehensive postpartum follow-up health care program for women with history of preeclampsia: protocol for mixed methods research. *Reproductive health*, 15(1), 1-8.

Katrakazas, P., Pastiadis, K., Bibas, A., & Koutsoures, D. (2020). A general system theory approach in public hearing health: Lessons learned from a systematic review of general systems theory in healthcare. IEEE Access, 8, 53018-53033. https://ieeexplore.ieee.org/document/9037270

Kaur, S. J., Ali, L., Hassan, M. K., & Al-Emran, M. (2021). Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts. *Journal of Financial Services Marketing*, 26(2). https://doi.org/10.1057/s41264-020- 00082-w

Kavitha, A., Rao, B. S., Akhtar, N., Rafi, S. M., Singh, P., Das, S., & Manikandan, G. (2022). A Novel Algorithm to Secure Data in New Generation Health Care System from Cyber Attacks Using IoT. *International Journal of Electrical and Electronics Research*, 270-275.

Kerins, C., Houghton, C., McHugh, S., Geaney, F., Toomey, E., Hayes, C., Perry, I. J., & Kelly, C. (2019a). Implementation of a calorie menu labeling policy in public

hospitals: Study protocol for pragmatic research. *International journal of qualitative methods,* 18, 1-10. https://doi.org/10.1177/1609406919878339

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. Computers & Security, 125, 103049.

Khattri, V., Nayak, S. K., & Singh, D. K. (2020). Plastic card circumvention an infirmity of authenticity and authorization. *Journal of Financial Crime*, 27(3), 959–975. https://doi.org/10.1108/jfc-03-2020-0034

Kim, J., Park, M., Kim, H., Cho, S., & Kang, P. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. *Applied Sciences*, 9(19), 1–21. https://doi.org/10.3390/app9194018

Klem, N. R., Bunzli, S., Smith, A., & Shields, N. (2022). Demystifying qualitative research for musculoskeletal practitioners part 5: rigor in qualitative research. *Journal of Orthopaedic & Sports Physical Therapy*, 52(2), 60-62.

Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement, and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy & Practice*, 13(5), 66-80. Retrieved from http://www.na-businesspress.com/jmppopen.html

Kok, S. H., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Prevention of crypto-ransomware using a pre-encryption detection algorithm. *Computers*, 8(4). https://doi.org/10.3390/computers8040079

Korać, D., Damjanović, B., & Simić, D. (2021). A model of digital identity for better

information security in E-learning systems. *The Journal of Supercomputing*, 78(3), 3325–3354. https://doi.org/10.1007/s11227-021-03981-4

Koraus, A., Dobrovic, J., Polak, J., & Backa, S. (2019). Aspects of the security use of payment card pin code analyzed by the methods of multidimensional statistics. *Entrepreneurship and Sustainability Issues*, 6(4), 2017–2036. http://doi.org/10.9770/jesi.2019.6.4(33)

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice, 24*(1), 120-124. http://doi.org/0.1080/13814788.2017.1375092

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, 18, 316-327. http://doi:10.1108/09685221011095236

Kuckartz, U., & Radiker, S. (2019). *Documenting and archiving the research process: Analyzing qualitative data with MAXQDA*. Springer. https://doi.org/10.1007/978-3-030-15671-8

Kurokawa, M., Schweber, L., & Hughes, W. (2017). Client engagement and building design: The view from actor–network theory. *Building Research & Information*, 45, 910-925. https://doi:10.1080/09613218.2016.1230692

Kurpjuhn, T. (2019). The guide to ransomware: How businesses can manage the evolving threat. *Computer Fraud & Security 2019*(11). https://doi.org/10.1016/S1361-3723(19)30117-4

Kusuma, G. H., Indarti, N., & Manik, H. F. G. G. (2023). Strategies for Innovation

Among Indonesian Family Firms. In Heritage Entrepreneurship: *Cultural and Creative Pursuits in Business Management* (pp. 55-72). Singapore: Springer Nature Singapore.

Kuzminykh, I., Ghita, B., & Such, J. M. (2022, March). The Challenges with Internet of Things Security for Business. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems: 21st International Conference*, NEW2AN 2021, and 14th Conference, ruSMART 2021, St. Petersburg, Russia, *August 26–27, 2021, Proceedings* (pp. 46-58). Cham: Springer International Publishing.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, 18, 4-13. https://doi:10.1108/09685221011035223

Latour, B. (1997). The trouble with actor-network theory. Philosophia: *tidsskrift for filosofi*, 25(3-4).18.05

Latour, B. (2011). Network theory| networks, societies, spheres: Reflections of an actor-network theorist. *International journal of communication*, 5, 15.

Lamontagne, C., Sénécal, S., Fredette, M., Labonté-LeMoyne, E., & Léger, P. M. (2021). The effect of the segmentation of video tutorials on User's training experience and performance. *Computers in Human Behavior Reports*, 3, 100071. https://doi.org/10.1016/j.chbr.2021.100071

Law, J. (1986). On power and its tactics: A view from the sociology of science. *The Sociological Review*, 34, 1-38. http://doi:10.1111/j.1467-954X.1986.tb02693.x

Law, J. (2008). On sociology and STS. *Sociological Review*, 56, 623-649.

https://doi:10.1111/j.1467-954X.2008.00808.x

Lecocq, T., Harpke, A., Rasmont, P., & Schweiger, O. (2019). Integrating intraspecific differentiation in species distribution models: Consequences on projections of current and future climatically suitable areas of species. *Diversity and Distributions,* 25(7), 1088-1100. https://www.jstor.org/stable/26662607

Lee, I. (2023). Cybersecurity: Risk management framework and investment cost analysis, Business Horizons, 5, 659-671. https://doi.org/10.1016/j.bushor.2021.02.022.

Lehr, W., Clark, D., Bauer, S., Berger, A., & Richter, P. (2019). Whither the public internet? *Journal of Information Policy*, 9, 1- 42. https://doi.org/10.5325/jinfopoli.9.2019.0001

Lehto, M., & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. Information Security Journal: *A Global Perspective*, 30(3), 139-148. https://doi.org/10.1080/19393555.2020.1813851

Lemieux, M. (2015). Cybercrime, governance, and liabilities in the banking and payment industries. *Banking & Finance Law Review*, 31, 113-140. Retrieved from https://www.bu.edu/rbfl/

Lemon, L. L., & Hayes, J. (2020). Enhancing trustworthiness of qualitative findings: Using lexi-mancer for qualitative data analysis triangulation. *Qualitative Report*, 25(3), 604–614. https://nsuworks.nova.edu/tqr/vol25/iss3/

Lessa, L., & Gebrehawariat, D. (2023). Effectiveness of banking card security in the Ethiopian financial sector: PCI-DSS security standard as a lens. *International Journal of Industrial Engineering and Operations Management*.

Lester, J. N., Cho, Y., & Lochmiller, C. R. (2020). Learning to Do Qualitative Data Analysis: *A Starting Point. Human Resource Development Review*, 19(1), 94–106. https://doi.org/10.1177/1534484320903890

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, 4(3), 324. https://doi:10.4103/2249-4863.161306

Levitt, H. M., Morrill, Z., Collins, K. M., & Rizo, J. L. (2021). The methodological integrity of critical qualitative research: Principles to support design and research review. *Journal of Counseling Psychology*, 68(3), 357–370. https://doi.org/10.1037/cou0000523

Li, Y. J., & Hoffman, E. (2023). Designing an incentive mechanism for information security policy compliance: An experiment, *Journal of Economic Behavior & Organization*, 212, 138-159, https://doi.org/10.1016/j.jebo.2023.05.033.

Lin, C., Wittmer, J. L. S., & Luo, X. (2022). Cultivating proactive information security behavior and individual creativity: The role of human relations culture and IT use governance, Information & Management, 59,(6), 2022. https://doi.org/10.1016/j.im.2022.103650.

Liu, S. (2016). How the user liaison's understanding of development processes moderates the effects of user-related and project management risks on IT project performance. Information & Management, 53, 122-134. https://doi:10.1016/j.im.2015.09.004

Liu, S., & Shih, K. (2009). Construction rescheduling based on a manufacturing rescheduling framework. Automation in Construction. 18. 715-723.

https://10.1016/j.autcon.2009.02.002.

Lloyd, I. (2020). Information technology law. *Oxford University Press*, USA.

Lo, F. Y., Rey-Martí, A., & Botella-Carrubi, D. (2020). Research methods in business: Quantitative and qualitative comparative analysis. *Journal of Business Research*, 1 15, 221–224. https://doi.org/10.1016/j.jbusres.2020.05.003

Lochmiller, C. R. (2021). Conducting Thematic Analysis with Qualitative Data. *Qualitative Report*, 26(6).

Locke, K., Feldman, M., & Golden-Biddle, K. (2022). Coding practices and iterativity: Beyond templates for analyzing qualitative data. *Organizational Research Methods*, 25(2), 262-284.

Loss, J., Brew-Sam, N., Metz, B., Strobl, H., Sauter, A., & Tittlbach, S. (2020). Capacity Building in Community Stakeholder Groups for Increasing Physical Activity: Results of a Qualitative Study in Two German Communities. International Journal of Environmental Research and Public Health, 17(7), 2306. https://doi.org/10.3390/ijerph17072306

Love, B., Vetere, A., & Davis, P. (2019). Handling hot potatoes: Ethical, legal, safeguarding, and political quandaries of researching drug-using offenders. *International journal of qualitative methods*, 18, 1-9. https://doi.org/10.1177/1609406919859713

Lupovici, A. (2019). Toward a securitization theory of deterrence. International Studies Quarterly, 63(1), 177–186. https://doi.org/10.1093/isq/sqy045

Macias, C. J. G., & Contreras, T. J. C. (2019). The life story: A social qualitative

research Method and its application in tourism management studies. *Revista Iberoamericana de Turismo- RITUR, Penedo*, 9, 59-77. https://doi: 10.2436/20.8070.01.143

Mackieson, P., Shlonsky, A., & Connolly, M. (2019). Increasing rigor and reducing bias in qualitative research: A document analysis of parliamentary debates using applied thematic analysis. *Qualitative Social Work*, 18(6), 965–980. https://doi.org/10.1177/1473325018786996

Madsen, A. K. (2013). Virtual acts of balance: Virtual technologies of knowledge management as co-produced by social intentions and technical limitations. *Electronic Journal of E-Government*, 11, 183-197. Retrieved from http://www.ejeg.com/main.html

Mähring, M., Holmström, J., Keil, M., & Montealegre, R. (2004). Trojan actor-networks and swift translation: Bringing actor-network theory to IT project escalation studies. *Information Technology & People*, 17, 210-238. https://doi:10.1108/09593840410542510

Manouchehri, E., Taghipour, A., Ebadi, A., Homaei Shandiz, F., & Latifnejad Roudsari, R. (2022). How do I deal with breast cancer: a qualitative inquiry into the coping strategies of Iranian women survivors. *BMC women's health*, 22(1), 1-11.

Manral, B., & Somani, G. (2021). Establishing forensics capabilities in the presence of superuser insider threats, Forensic Science International: *Digital Investigation*, 38. https://doi.org/10.1016/j.fsidi.2021.301263.

Marcon Nora, G. A., Alberton, A., & Ayala, D. H. F. (2023). Stakeholder theory and

actor-network theory: The stakeholder engagement in energy transitions. *Business* Strategy and the Environment, 32(1), 673-685.

Matta, P., Arora, M., & Sharma, D. (2021). A comparative survey on data encryption Techniques: Big data perspective. Materials Today: *Proceedings*, 46(2021), 11035–11039. https://doi.org/10.1016/j.matpr.2021.02.153

Maxwell, J. A. (2021). Why qualitative methods are necessary for generalization. *Qualitative Psychology*, 8(1), 111–118. https://doi.org/10.1037/qup0000173

Mazzarolo, G., & Jurcut, A. D. (2020). Insider threats in cyber security: The enemy within the gates. *European Cybersecurity Journal*, https://arxiv.org/abs/1911.09575

McCracken, J. (2020). Ethics as Obligation: reconciling diverging research practices with marginalized communities. *International journal of qualitative methods*, 19, 1-11. https://doi.org/10.1177/1609406920964336

McCreless, P. (2022, March 22). South Carolina residents lost $42 million to cyber crime in 2021. Government Technology. https://www.govtech.com/security/south-carolina-residents-lost-42m-to-cyber-crime-in-2021

McGarry, O. (2016). Knowing 'how to go on': Structuration theory as an analytical prism in studies of intercultural engagement. *Journal of Ethnic & Migration Studies*, 42, 2067-2085. https://doi:10.1080/1369183X.2016.1148593

McKim, C. (2017). The value of mixed methods research. *Journal of Mixed Methods Research*, 11(2), 202-222. https://doi:10.1177/1558689815607096

Mendez, J. V., Castillo, M. P. L., Sanchez, J. R., Mateus, J. D., & Maldonado, J. C.

(2014). A software development for establishing optimal production lots and its application in academic and business environments. *Engineering and Research*, 34, 81-86. https://doi:10.15446/ing.investig.v34n3.41578

Meraz, R. L., Osteen, K., & McGee, J. (2019). Applying multiple methods of systematic evaluation in narrative analysis for greater validity and deeper meaning. *International journal of qualitative methods*, 18, 1-6. https://doi.org/10.1177/1609406919892472

Metselaar, S. (2019). Commentary 1: Informed consent of research participants: The gap between regulations and reality. *Journal of Empirical Research on Human Research Ethics*, 14(5), 433–435. https://doi.org/10.1177/1556264619831589a

Mittal, Y., Roy, D., & Saxena, D. (2010). A knowledge management model to improve information security. *International Journal of Computer Science Issues*, 7(6), 105-108. Retrieved from http://ijcsi.org/

Montano, H. I, Aranda, G., Diaz, R. J, Cardin, M.S., & Diez, T.I. (2022). Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat. *Cluster Comput* 25, 4289–4302 (2022). https://doi.org/10.1007/s10586-022-03668-2

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: *Concerns for psychiatry Current Psychiatry Reports* 23(18). https://doi.org/10.1007/s11920-021-01228-w

Monteiro, E. (2000). Actor-network theory and information infrastructure. In C. U. Ciborra (Ed.). *From control to drift: The dynamics of corporate information*

infrastructure (pp. 71-86). Oxford, United Kingdom: Oxford University Press.

Montenegro, L. M., & Bulgacov, S. (2014). Reflections on actor-network theory, governance networks, and strategic outcomes. *Brazilian Administration Review*, 11(1), 107-124. https://doi:10.1590/S1807-76922014000100007

Montenegro, L. M., & Bulgacov, S. (2015). Governance and strategy of undergraduate business programs in light of the actor-network theory. *Contemporary Administrative Magazine*, 19, 212-231. Retrieved from http://www.scielo.br

Moore, R. (2022). Incident response team: What are the roles and responsibilities? AT&T Cybersecurity. https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/arming-your-incident-response-team

Morgan, D. L., & Nica, A. (2020). Iterative thematic inquiry: A new method for analyzing qualitative data. *International journal of qualitative methods*,19,1-11. https://doi.org/10.1177/1609406920955118

Morse, W., Lowery, D., & Steury, T. (2014). Exploring saturation of themes and spatial locations in qualitative public participation geographic information systems research. *Society & Natural Resources, 27*(5), 557-571. https://doi:10.1080/08941920.2014.888791

Moukhah, S., Ghorbani, B., Behboodi M. Z., Zafardoust, S., Haji P. A., Alinaghi, E., & Moukhah, R. (2023). Perception of Female Identity in Women with Premature Ovarian Insufficiency: A Qualitative Study. *Journal of Reproduction & Infertility*, 24(1), 49-57.

Müller, F. I., & Richmond, M. A. (2023). The technopolitics of security: Agency,

temporality, sovereignty. *Security Dialogue*, 09670106221141373.

Mueller, R. A. (2019). Episodic narrative interview: capturing stories of experience with a methods fusion. *International journal of qualitative methods*,18,1-11. https://doi.org/10.1177/1609406919866044

Mukumbang, F. C. (2023). Retroductive theorizing: a contribution of critical realism to mixed methods research. *Journal of Mixed Methods Research*, 17(1), 93-114.

Murry, L. T., Witry, M. J., & Urmie, J. (2023). Medicare part D plan-selection experience: Qualitative findings from a national cross-sectional survey. *Exploratory Research in Clinical and Social Pharmacy*, 100219.

Mwiraria, D. R., Ngetich, K., & Mwaeke, P. (2022). Factors associated with cybercrime awareness among university students in Egerton university, Njoro campus, Kakuru county, Kenya. *European Journal of Humanities and Social Sciences* 2(3), 63-68. http://dx.doi.org/10.24018/ejsocial.2022.2.3.256

Mwita, K. M. (2022). Factors to consider when choosing data collection methods. *International Journal of Research in Business and Social Science.* 11(5), 532-538

Naeem, M., & Ozuem, W. (2021). The role of social media in internet banking transition during COVID-19 pandemic: Using multiple methods and sources in qualitative research. *Journal of Retailing and Consumer Services*, 30. https://doi.org/10.1016/j.jretconser.2021.102483

Nasser, A. M., Ahmad, R., Abidin, Z., Abdulkareem, K. H., Mohammed, M. A., Gupta, D., & Shankar, K. (2022). A new intelligent multilayer framework for insider threat detection, *Computers & Electrical Engineering,*

https://doi.org/10.1016/j.compeleceng.2021.107597.

Nastasiu, C. (2016). Cybersecurity strategies in the Internet era. Proceedings of the Scientific Conference AFASES, 2, 619-624. doi:10.19062/2247-3173.2016.18.2.19

Narayanan, S. N., Khanna, K., Panigrahi, B. K., Joshi, A. (2019). Security in Smart Cyber-Physical Systems: *A Case Study on Smart Grids and Smart Cars*, 147-163. https://doi.org/10.1016/B978-0-12-815032-0.00011-1.

Ningi, A. I. (2022). Data Presentation in Qualitative Research: The Outcomes of the Pattern of Ideas with the Raw Data. *International Journal of Qualitative Research*, 1(3), 196-200.

Nishio, N., Kondo, M., & Kamoshida, R. (2022). Personnel Scheduling for Logistics Warehouses Based on the Theory of Constraints. *Journal of Advanced Management Science* Vol, 10(3).

NIST SP 800-53. Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Nunfam, V. F. (2021). Mixed methods study into social impacts of work-related heat stress on Ghanaian mining workers: *A pragmatic research approach*, Heliyon, 5 (7). https://doi.org/10.1016/j.heliyon.2021.e06918.

O'Connor, C., & Joffe, H. (2020). Intercoder reliability in qualitative research: debates and practical guidelines. *International journal of qualitative methods*,19,1-13. https://doi.org/10.1177/1609406919899220

Ogbanufe, O. & Ge, L. (2023). A comparative evaluation of behavioral security motives:

Protection, intrinsic, and identity motivations, Computers & Security. https://doi.org/10.1016/j.cose.2023.103136.

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://www.sciencegate.app/document/10.3837/tiis.2019.03.035

O'Kane, P., Smith, A., & Lerman, M. P. (2021). Building Transparency and Trustworthiness in Inductive Research Through Computer-Aided Qualitative Data Analysis Software. *Organizational Research Methods*, 24(1), 104–139. https://doi.org/10.1177/1094428119865016

O'Leary, D. E. (2019). What phishing emails reveal: An exploratory analysis of phishing attempts using text analyzes. *SSRN Electronic Journal*, 33(3), 285–307. https://doi.org/10.2308/isys-52481

Olowolayemo, A., Adewale, N., Zeki, A. M., & Ahmad, Z. (2019). Examining users' understanding of security failures in EMV smart card payment systems. JOIV: *International Journal on Informatics Visualization*, 3(2), 185–191. https://doi.org/10.30630/joiv.3.2.244

Omoyiola, B. O., & Mckeeby, J. (2023). Strategies For Implementing Cybersecurity Policies in Organizations (A Case Study of West African Organizations). *Available at SSRN 4395723*.

Pabian, A., Pabian, B., & Reformat, B. (2020). E-customer security as a social value in the sphere of sustainability. *Sustainability*, 12(24), 1–14.

https://doi.org/10.3390/su122410590

Padayachee, K. (2022). Understanding the effects of situational crime prevention and personality factors on insider compliance, *Journal of Information Security and Applications.* https://doi.org/10.1016/j.jisa.2022.103338.

Parks, P. (2023). Story Circles: A New Method of Narrative Research. *American Journal of Qualitative Research,* 7(1), 58-72.

Parker, E. (2017). An actor-network theory reading of change for children in public care. *British Educational Research Journal*, 43, 151-167. https://doi:10.1002/berj.3257

Payment Card Industry (PCI) Software Security Framework Secure Software Standard https://listings.pcisecuritystandards.org/documents/Secure-Software-Program-Guide-v1.pdf

PCI DSS Quick Reference Guide. *Understanding the Payment Card Industry Data Security Standard version 3.0.* https://listings.pcisecuritystandards.org/documents/PCIDSS_QRGv3.pdf

Perez, M., & Suek, J. (2019). Spotlight: Bank's face growing cybercrime threat. Southwest Economy, Federal Reserve Bank of Dallas, issue Fourth Quarter. https://ideas.repec.org/a/fip/feddse/87589.html

Pessoa, A. S. G., Harper, E., Santos, I. S., & Gracino, M. C. D. S. (2019). Using reflexive https://www.obssr.od.nih.gov/wp-content/uploads/2018/01/Best-Practices-for-Mixed-Methods-Research-in-the-Health-Sciences-2018-01-25.pdf interviewing to foster deep understanding of research participants' perspectives. *International journal of qualitative methods*, 18,1- 9.

https://doi.org/10.1177/1609406918825026

Peterson, J. S. (2019). Presenting a qualitative study: A reviewer's perspective. *Gifted Child Quarterly*, 63(3), 147–158. https://doi.org/10.1177/0016986219844789

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning*, 12(3), 224–232. https://pubmed.ncbi.nlm.nih.gov/30857581/

Pieters, W. (2011). Explanation and trust: What to tell the user in security and AI? *Ethics & Information Technology,* 13(1), 53-64. https://doi:10.1007/s10676-010-9253

Pokorny, H. (2023). Recognition of Prior Learning Translation and Transfer (RPLTT): using Actor-Network-Theory to develop a specialized pedagogy. *Assessment & Evaluation in Higher Education*, 1-13.

Pollack, J., Costello, K., & Sankaran, S. (2013). Applying actor-network theory as sensemaking framework for complex organizational change programs. *International Journal of Project Management*, 31, 1118-1128. https://doi:10.1016/j.ijproman.2012.12.007

Pollack, J., & Clegg, S. (2023). 12. Uncovering the role of non-human actors in projects. *Research Handbook on Complex Project Organizing*, 117.

Pollmeier, S., Bongiovanni, I., & Slapničar, S. (2023). Designing a financial quantification model for cyber risk: *A case study in a bank, Safety Science*. https://doi.org/10.1016/j.ssci.2022.106022.

Poornima, A. S. (2023). Actor Network Theory, Social Networks, Marketing of Mutual Funds. *The Management Accountant Journal,* 58(1), 98-101.

Posey, C., Bennett, J. R., & Roberts, L. T. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, 30, 486–497. https://doi:10.1016/j.cose.2011 .05.002

Prabowo, H. Y. (2020). Reinvigorating the human instrument: An exploratory study on the potential use of CAQDAS in qualitative evaluation of corruption prevention in Indonesia. Journal of Financial Crime, 27(2), 505-530. https://doi.org/10.1108/JFC-01-2019-0004

Pagnini, F., Bonalda, E., Montrasi, E., Toselli, E., & Toselli, A. (2021). Mindfully Reframing the Psychological Impact of the COVID-19 Outbreak Through a Social Media Community for Students: A Pragmatic Study. *Sec. Personality and Social Psychology*. https://doi.org/10.3389/fpsyg.2021.566778

Protudjer, J. L., Batac, A. L. R., Merrill, K. A., Golding, M. A., & Knibb, R. C. (2023). Guidance to enhance participant validity during virtual qualitative interviews and focus groups. Annals of Allergy, Asthma & Immunology.

Puchta, A., Böhm, F., & Pernul, G. (2019). Contributing to Current Challenges in Identity and Access Management with Visual Analytics. 33th IFIP *Annual Conference on Data and Applications Security and Privacy (DBSec), Charleston, SC, United States.* pp.221-239, 10.1007/978-3- 030-22479-0_12 . https://hal.inria.fr/hal-02384584

Rademacher, P., & Wagner, K. (2020). Efficient Bayesian sequential classification under the Markov assumption for various loss functions. *IEEE signal processing letters*,

27, 401-405. https://doi.org/10.1109/LSP.2020.2973854

Rafi, S., Yu, W., Akbar, M. A., Alsanad, A., & Gumaei, A. (2020b). Prioritization based taxonomy of DevOps security challenges using PROMETHEE. IEEE Access,8,105426-105446. https://doi.org/10.1109/ACCESS.2020.2998819

Rahim, N. H. A., Hamid, S., & Kiah, L. M. (2019). Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An assessment. *Malaysian Journal of Computer Science*, 32(3). https://doi.org/10.22452/mjcs.vol32no3.4

Rahimi, F., Hvam, L., & Moller, C. (2014). Alignment between business process governance and IT governance. *Twentieth Americas Conference on Information Systems*, 2, 1-12. Retrieved from http://aisel.aisnet.org

Rakova, O., & Fedorenko, O. (2021). Sticky notes against corporate hierarchies in South Korea: An ethnography of workplace collaboration and design co-creation. *Design Studies,* 76, 101033.

Ramanadhan, S., Revette, A. C., Lee, R. M., & Aveling, E. L. (2021). Pragmatic approaches to analyzing qualitative data for implementation science: an introduction. *Implementation Science Communications*, 2(1), 1-10.

Rand, G. K. (2000). Critical chain: The theory of constraints applied to project management. *International Journal of Project Management*, 18, 173-177. Retrieved from www.elsevier.com/locate/ijproman

Randive, K., Mohan, R., & Sivakrishna, A. M. (2023). An efficient pattern-based approach for insider threat classification using the image-based feature

representation, *Journal of Information Security and Applications*, (73), https://doi.org/10.1016/j.jisa.2023.103434.

Rapport, F., Smith, J., Hutchinson, K., Clay-Williams, R., Churruca, K., Bierbaum, M., & Braithwaite, J. (2022). Too much theory and not enough practice? The challenge of implementation science application in healthcare practice. *Journal of Evaluation in Clinical Practice,* 28(6), 991-1002.

Ravindran, A., Li, J., & Marshall, S. (2020). Learning ethnography through doing ethnography: Two student—researchers' insights. *International journal of qualitative methods*, 19, 1-11. https://doi.org/10.1177/1609406920951295

Redman-Maclaren, M., Mills, J., & Tommbe, R. (2014). Interpretive focus groups: A participatory method for interpreting and extending secondary analysis of qualitative data. *Global Health Action*, 7(4), 44-69. https://doi.org/10.3402/gha.v7.25214

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open*. https://doi.org/10.1177/21582440211000049

Rice, C., & Searle, R. H. (2022). The enabling role of internal organizational communication in insider threat activity–evidence from a high security organization. *Management Communication Quarterly*, 36(3), 467- 495.

Ridgeway, J. L., Albertie, M., Pantoja, E., Prescott, D., Zhu, X., & Breitkopf, C. R. (2019). Understanding diverse perspectives on genetic research through focus group talk. *International Journal of Qualitative Methods*,18, 1-14.

https://doi.org/10.1177/1609406919892476

Roberts, R. E. (2020). Qualitative Interview Questions: Guidance for Novice Researchers. The Qualitative Report, 25(9), 3185-3203. https://www.proquest.com/scholarly-journals/qualitative-interview-questions-guidance-novice/docview/2445581779/se-2

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

Rubio, J. E., Alearaz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers & Security Journal* 87(1). https://doi.org/10.1016/j.cose.2019.06.015

Saathoff, G. B., Nold, T. & Holstege, C.P. (2013). We Have Met the Enemy and They Are Us: Insider Threat and Its Challenge to National Security, 24-35, https://doi.org/10.1016/B978-0-12-407191-9.00003-X.

Safa, N. S., Maple, C., Furnell, S, Azad, M.A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organizations, *Future Generation Computer Systems*, 97, 587-597. https://doi.org/10.1016/j.future.2019.03.024.

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

Saleh, E. A., Lazaridou, F. B., Klapprott, F., Wazaify, M., Heinz, A., & Kluge, U. (2023).

A systematic review of qualitative research on substance uses among refugees. *Addiction,* 118(2), 218 - 253. https://doi.org/10.1111/add.16021

Santana-Cordero, A. M., & Szabó, P. (2019). Exploring qualitative methods of historical ecology and their links with qualitative research. *International journal of qualitative methods*, 18,1-11. https://doi.org/10.1177/1609406919872112

Sayes, E. (2017). Marx and the critique of actor-network theory: Mediation, translation, and explanation. *Distinktion: Journal of Social Theory*, 18, 294-313. https://doi:10.1080/1600910X.2017.1390481

Schiffling, S., Hannibal, C., Tickle, M., & Fan, Y. (2022). The implications of complexity for humanitarian logistics: A complex adaptive systems perspective. Annals of Operations Research, 319(1), 1379-1410.

Schweinsberg, M., Thau, S., & Pillutla, M. (2023). Problem Validity in Primary Research: Precision and Transparency in Characterizing Past Knowledge. *Perspectives on Psychological Science*, 17456916221144990.

Sezgin, D., O'Donovan, M., Cornally, N., Liew, A., & O'Caoimh, R. (2019). Defining frailty for healthcare practice and research: A qualitative systematic review with thematic analysis, *International Journal of Nursing Studies*, 92, 16-26. https://doi.org/10.1016/j.ijnurstu.2018.12.014

Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes Prevention: Promising Organizational practices. *Information Technology & People* 32(5), 1125-1129. https://doi.org/10.1108/ITP-10-2019-564

Shahin, A., Jamkhaneh, B. H., & Cheryani, Z. H. S. (2014). EFQMQual: Evaluating the

implementation of the European quality award based on the concepts of model of service quality gaps and ServQual approach. Measuring Business Excellence, 18, 56-38. https://doi:10.1108/MBE-12-2012-0057

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974.

Silvis, E., & Alexander, P. M. (2014). A study using a graphical syntax for actor-network theory. *Information Technology & People*, 27, 110-128. https://doi:10.1108/ITP-06-2013-0101

Singh, S. K. (2017). Conceptual framework of a cloud-based decision support system for arsenic health risk assessment. *Environment Systems and Decisions*, 37(4), 435-450. https://doi.org/10.1007/s10669-017-9641-x

Skeoch, H. (2022). Expanding the Gordon-Leob model to cyber-insurance. *Computers & Security* 112(6), https://doi.org/10.1016/j.cose.2021.102533

Soh, C., Yu, S., Narayanan, A., Duraisamy, S., & Chen, L. (2019). Employee profiling via aspect-based sentiment and network for insider threats detection, Expert Systems with Applications,135, 351-361. https://doi.org/10.1016/j.eswa.2019.05.043.

Srinivasan, B., & Mukherjee, D. (2018). Agile teams as complex adaptive systems (CAS). *International Journal of Information Technology*. https://10. 10.1007/s41870-018-0122-3.

Steils, N. (2021). Qualitative Experiments for Social Sciences. New trends in qualitative

research. https://doi.org/10.36367/ntqr.6.2021.24-31

Stewart, H., & Gapp, R. (2014). Achieving effective sustainable management: A small medium enterprise case study. *Corporate Social Responsibility and Environmental Management,* 21, 52-64. https://doi:10.1002/csr.1305

Stewart, H., Gapp, R., & Harwood, I. (2017). Exploring the alchemy of qualitative management research: Seeking trustworthiness, credibility and rigor through crystallization. *The Qualitative Report*, 22(1), 1-19. https://doi.org/10.46743/2160-3715/2017.2604

Steyn, H. (2002). Project management applications of the theory of constraints beyond critical chain scheduling. *International Journal of Project Management*, 20, 75-80. https://doi:10.1016/S0263-7863(00)00054-5

Suresh, P. V., & Madhavu, M. L. (2022). Insider threat detection in organization using machine learning. *Journal of Applied Information Science* 10(1), 17-28. http://www.publishingindia.com/jais

Surmiak, A., Bielska, B., & Kalinowska, K. (2022). Social Researchers' Approaches to Research Ethics During the COVID-19 Pandemic: An Exploratory Study. *Journal of Empirical Research on Human Research Ethics*. 17(1-2):213-222. https://doi:10.1177/15562646211055056

Soares, S., & de Oliveira, W. F. (2016). The matrix approach to mental health care: Experiences in Florianopolis, Brazil. *Journal of Health Psychology*, 21, 336-345. https://doi:10.1177/1359105316628752

Smith, J. D., & Hasan, M. (2020). Quantitative approaches for the evaluation of

implementation research studies, *Psychiatry Research*. https://doi.org/10.1016/j.psychres.2019.112521.

Tan, J., Lei, C., Zhang, H., & Cheng, Y. (2019). Optimal strategy selection approach to moving target defense based on Markov robust game, *Computers & Security*, (85), 63-76. https://doi.org/10.1016/j.cose.2019.04.013.

Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective, *Information & Management,* 60(3). https://doi.org/10.1016/j.im.2022.103751.

Terlizzi, M. A., Meirelles, F. S., & Viegas Cortez da Cunha, M. A. (2017). Behavior of Brazilian banks employees on Facebook and the cybersecurity governance. *Journal of Applied Security Research*, 12, 224-252. https://doi:10.1080/19361610.2017.1277886

Thakur, H., & Purandare, P. (2022, October). Comparative study on bibliometric data of cyber-attacks on financial institutions. In *AIP Conference Proceedings* (Vol. 2519, No. 1, p. 030044). AIP Publishing LLC

The Personal Information Protection and Electronic Documents Act (PIPEDA). Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Thelwall, M., & Nevill, T. (2021). Is Research with Qualitative Data More Prevalent and Impactful Now? *Interviews, Case Studies, Focus Groups and Ethnographies. Library & Information Science Research*, 43(2).

https://doi.org/10.1016/j.lisr.2021.101094

Thomas, L. D., & Tee, R. (2022). Generativity: A systematic review and conceptual framework. *International Journal of Management Reviews*, 24(2), 255-278.

Thumlert, K., de Castell, S., & Jenson, J. (2015). Short cuts and extended techniques: Rethinking relations between technology and educational theory. *Educational Philosophy and Theory*, 47, 786-803. https://doi:10.1080/00131857.2014.901163

Tolich, M. (2019). What Qualitative Researchers Must Do When Ethical Assurances Disintegrate? Recognise Internal Confidentiality, Establish Process Consent, Reference Groups, Referrals for Participants and a Safety Plan. *In World Conferences on Qualitative Research* (pp. 22-32). Springer, Cham. https://doi.org/10.1007/978-3-030-31787-4_2

Tortia, E. C., & Sacchetti, S. (2023). Networking, Governance, and Stakeholder Engagement of Financial Cooperatives: Some National Case Studies. In *Humanistic Governance in Democratic Organizations*: The Cooperative Difference (pp. 331-357). Cham: Springer International Publishing.

Turale, S. (2020). A brief introduction to qualitative description: A research design worth using. *Pacific Rim International Journal of Nursing Research*, 24(3), 289-291.

Turner, J. R., & Baker, R. M. (2019). Complexity Theory: An Overview with Potential Applications for the Social Sciences. *Systems*. 2019; 7(1):4. https://doi.org/10.3390/systems7010004

Tuthill, E. L., Maltby, A. E., DiClemente, K., & Pellowski, J. A. (2020). Longitudinal qualitative methods in health behavior and nursing research: assumptions, design,

analysis and lessons learned. *International journal of qualitative methods*,19,1-21. https://doi.org/10.1177/1609406920965799

Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, 89, 101666.

Valdovinos, I. A., Pérez-Díaz, J. A., Choo, K. R., & Botero, J. F. (2021). Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions, *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2021.103093.

Van Brussel, S., Boelens, L., & Lauwers, D. (2016). Unraveling the Flemish mobility orgware: The transition towards a sustainable mobility from an actor-network perspective. *European Planning Studies*, 24, 1336-1356. https://doi:10.1080/09654313.2016.1169248

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector, *Computers & Security*, 105. https://doi.org/10.1016/j.cose.2021.102239.

Varpio, L., Ajjawi, R., Monrouxe, L. V., O'brien, B. C., & Rees, C. E. (2017). Shedding the cobra effect: Problematizing thematic emergence, triangulation, saturation and member checking. *Medical Education, 51*(1), 40-50. http://doi.og/10.1111/medu.13124

Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related

security threats. *Materials Today: Proceedings*, 51, 2172-2175.

Visser, A., du Preez, P., & Simmonds, S. (2019). Reflections on life design narrative inquiry as a methodology for research with child sex trafficking survivors. *International journal of qualitative methods*, 18, 1-12. https://doi.org/10.1177/1609406919857553

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.

Waibel, S., Vargas, I., Aller, M. B., Gusmão, R., Henao, D., & Vázquez, M. L. (2015). The performance of integrated health care networks in the continuity of care: a qualitative pragmatic qualitative inquiry study of COPD patients. *International journal of integrated care*, 15(3). https://doi.org/10.5334/ijic.1527

Walls, D. M. (2015). Access(ing) the coordination of writing networks. *Computers and Composition*, 38, 68-78. https://doi:10.1016/j.compcom.2015.09.004

Walsh, S., Jones, M., Bressington, D., McKenna, L., Brown, E., Terhaag, S., Shrestha, M., Al-Ghareeb, A., & Gray, R. (2020). Adherence to COREQ reporting guidelines for qualitative research: A Scientometric study in nursing social science. *International journal of qualitative methods*, 19, 1-19. https://doi.org/10.1177/1609406920982145

Walsham, G. (1997). Actor-network theory and IS research: Current status and future prospect. In A. Lee, J. Liebenau & J. DeGross (Eds.), *Information systems and qualitative research*. London, England: Chapman & Hall.

Wa-Mbaleka, S. (2020). The Researcher as an Instrument. In: Costa, A., Reis, L., Moreira, A. (eds) Computer Supported Qualitative Research. WCQR 2019. Advances in Intelligent Systems and Computing, vol 1068. *Springer, Cham.* https://doi.org/10.1007/978-3-030-31787-4_3

Wang, Q., & Hannes, K. (2020). Toward a more comprehensive type of analysis in photovoice research: The development and illustration of supportive question matrices for research teams. *International journal of qualitative methods*,19,1-15. https://doi.org/10.1177/1609406920914712

Wasko, S., Rhodes, R. E., Goforth, M., Bos, N., Cowley, H. P., Matthews, G., Leung, A., Iyengar, S., & Kopecky, J. (2021). Using alternate reality games to find a needle in a haystack: An approach for testing insider threat detection methods, *Computers & Security*. https://doi.org/10.1016/j.cose.2021.102314.

Weaver, S. T., Ellen, P. S., & Mathiassen, L. (2015). Contextualist inquiry into organizational citizenship: Promoting recycling across heterogeneous organizational actors. *Journal of Business Ethics*, 129, 13-28. https://doi:10.1007/s10551-014-2165-0

Wei, Y., Chow, K., & Yiu, S. (2021). Insider threat prediction based on unsupervised anomaly detection scheme for proactive forensic investigation, Forensic Science International: *Digital Investigation*. https://doi.org/10.1016/j.fsidi.2021.301126.

Williamson, C., Van Rooyen, A., Shuttleworth, C., Binnekade, C., & Scott, D. (2020). Wuity as a philosophical lens for qualitative data analysis. *International journal of qualitative methods*,19,1-11. https://doi.org/10.1177/1609406920926885

Willan, M. M. (2016). Research approaches for higher education students: A personal experience. *BCES Conference Proceedings*, 14, 247-254. Retrieved from http://bces-conference.org/

Wilson, M., Hash, J. & Bowen, P. (2006). Information Security Handbook: A Guide for Managers. *Recommendations of the National Institute of Standards and Technology*. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-100.pdf

Wodo, W., Blaskiewicz, P., Stygar, D., & Kuzma, N. (2021). Evaluating the security of electronic and mobile banking, *Computer Fraud & Security*, (10) 8-14, https://doi.org/10.1016/S1361-3723(21)00107-X.

Wolgemuth, J., Hicks, T., & Agosto, V. (2017). Unpacking assumptions in research synthesis: A critical construct synthesis Approach. *Educational Researcher*, 46(3), 131-139. https://doi:10.3102/0013189X17703946

Wright, A. L., Gabel, C., Ballantyne, M., Jack, S. M., & Wahoush, O. (2019). Using two-eyed seeing in research with indigenous people: An integrative review. *International journal of qualitative methods*, 18,1-19. https://doi.org/10.1177/1609406919869695

Xu, W., & Zammit, K. (2020). Applying thematic analysis to education: A hybrid approach to interpreting data in practitioner research. *International journal of qualitative methods*,19,1-9. https://doi.org/10.1177/1609406920918810

Yadav, D. (2022). Criteria for good qualitative research: A comprehensive review. *The Asia-Pacific Education Researcher*, 31(6), 679-689.

Yao, S., Wang, X., Yu, H., & Guchait, P. (2019). Effectiveness of error management training in the hospitality industry: Impact on perceived fairness and service recovery performance, International Journal of Hospitality Management, 79, 78-88. https://doi.org/10.1016/j.ijhm.2018.12.009.

Yin, R. K. (2014). Case study research: Design and methods (5th ed.). Thousand Oaks, CA: Sage Publications.

Yin, R. K. (2016). Qualitative Research from Start to Finish (2nd ed.). Guilford Publications.

Yin, R. K. (2018). Case study research: Design and methods. (5th ed.). Sage Publications.

Yonas, V., Rupia, C., & Onyango, D. (2023). Classroom Management Challenges Facing Teachers in Enhancing Students' Academic Achievement in Public Secondary Schools in Tarime District. East African Journal of Education Studies, 6(1), 22-37.

Younas, A., Fàbregues, S., Durante, A., Escalante, E. L., Inayat, S., & Ali, P. (2023). Proposing the "MIRACLE" narrative framework for providing thick description in qualitative research. *International Journal of Qualitative Methods*, 22, 16094069221147162.

Yousef, R., & Jazzar, M. (2021). Measuring the Effectiveness of User and Entity Behavior Analytics for the Prevention of Insider Threats. *Xi'an Jianzhu Keji Daxue Xuebao/Journal of Xi'an University of Architecture & Technology*. XIII. 175-181. https://10.37896/JXAT13.10/313918.

Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review,

challenges and opportunities, *Computers & Security,* https://doi.org/10.1016/j.cose.2021.102221.

Yungaicela-Naula, N. M., Vargas-Rosales, C., Pérez-Díaz, J. A., & Zareei, M. (2022). Towards security automation in Software Defined Networks, *Computer Communications*, (183), 64-82. https://doi.org/10.1016/j.comcom.2021.11.014.

Zainol, Z., Nelson, S. P., & Malami, A. (2012). Internal Human based Threats and Security Controls in Computerized Banking Systems: Evidence from Malaysia, *Procedia – Social and Behavioral Sciences*, 65, 199-204. https://doi.org/10.1016/j.sbspro.2012.11.111.

Zapata-Barrero, R., & Yalaz, E. (2020). Qualitative migration research ethics: a roadmap for migration scholars. *Qualitative Research Journal*, 20(3), 269–279. https://doi.org/10.1108/qrj-02-2020-0013

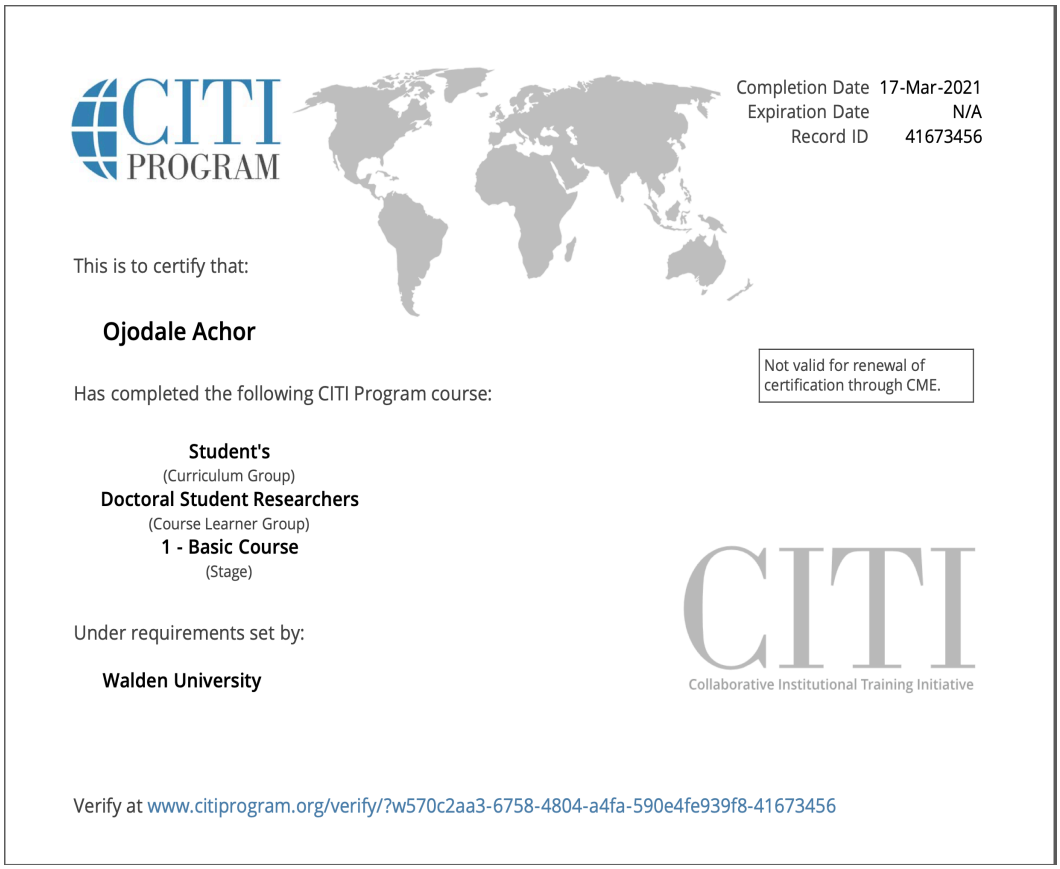
Zare, F., Bazrafkan, K., Irani Behbahani, H., & Mansouri, B. (2023). Actor-Network Theory Methodology in Architectural Co-design Process. *Journal of Architectural Thought.*

Zhu, B., Shum, K. W., Li, H., & Anta, A. F. (2019). On the duality and file size hierarchy of fractional repetition codes. *The Computer journal*, 62(1), 150-160, https://doi.org/10.1093/comjnl/bxy094

Zhuang, R., Bardas, A. G., DeLoach, S. A., & Ou, X. (2015). A theory of cyber-attacks: A step towards analyzing MTD systems. MTD ’15 Proceedings of the second ACM Workshop on Moving Target Defense, USA, 11-20.

https://doi:10.1145/2808475.808478

Appendix A: CITI Doctoral Student Researcher Certificate



CITI PROGRAM

Completion Date 17-Mar-2021
Expiration Date N/A
Record ID 41673456

This is to certify that:

Ojodale Achor

Not valid for renewal of certification through CME.

Has completed the following CITI Program course:

Student's
(Curriculum Group)
Doctoral Student Researchers
(Course Learner Group)
1 - Basic Course
(Stage)

Under requirements set by:

Walden University

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?w570c2aa3-6758-4804-a4fa-590e4fe939f8-41673456

Appendix B: Informed Consent Form

You are invited as participant in a research study about the strategies you implement to prevent security breaches due to insider threats in your organization. The purpose of this study is to explore the strategies used by IT security managers to prevent breaches due to insider threats. The researcher is inviting at least 6 organizational IT security managers that operate within the banking industry in the southeastern part of Canada. The participants must possess the knowledge of information security strategy development and be involved in its implementation. This form is part of a process called "informed consent" which allows you to understand this study prior to deciding whether to participate. This study is being conducted by a researcher named Ojodale Achor, who is doctoral student at Walden University.

Procedures:

If you agree to participate in this study, you would be asked to participate in a 30 to 60-minute audio interview at your convenience. The interview can be performed with the use of video teleconference tools, such as zoom or teams. Any video teleconference tool that is convenient to you can also be used. Please note that the interview would be recorded for transcription purposes. You will review the transcribed interview for accuracy and your consent to use the information in the study, participate in a follow-up interview should additional information is required, and provide me with pertinent documents that portray the implementation of your information security strategy. Electronic copies of these documents would be preferred, but if you are unable to provide copies, then eyes-only viewing would suffice.

Voluntary Nature of the Study:

This study is voluntary. You have the liberty to accept or decline this invitation. No person at your organization would treat you differently if you choose not to participate in the study. If you decide to participate in the study now, you can still change your mind later at any time during the study, and your decision would not impact any previous relationships you may have had with me or any other employee at your organization.

Risks and benefits of participating in the Study:

Participating in this type of study involves some risk of minor inconveniences that may be encountered in daily life, such as taking time out of your busy day to support this study or discussing the implementation of your cybersecurity strategy. Please be informed that your participation in this study would not pose any risk to your safety or well-being. Also, there may be no direct benefits to you, but the identified strategies can be used to enhance information security strategy within the industry.

Payment:

Please be informed that there would be no compensation for participation in this study

Privacy:

All reports and publications as outcome from this study would not show the identities of the individual participants, nor the name of the bank or organization. Any detail that might identify a participant, such as the location of the participant would also not be shared. The researcher would not use your personal information for any other purpose outside of this research studies. All data would be stored secure by replacing

participant information with codes, data files of the participants would be encrypted, and password protected, and the participant's location would not be disclosed in the report. You would not be asked to answer any sensitive/confidential information concerning your organization and you do not have any obligation to do so. If any sensitive/confidential information is accidentally divulged, the information would be deleted from the transcript or masked with a code. Data would be kept for a period of at least five years, then would be deleted/destroyed, as required by the university. All data identifying participant and organizational details would remain confidential throughout and after the study.

Contacts and Questions:

You may ask any questions you have now, or if questions arise later, you may contact the researcher via Ojodale.achor@waldenu.edu. If you want to speak privately regarding your rights as a participant, you may contact the Research Participant Advocate at 183 Walden University at +1 612-312-1210. Walden University's approval number for this study is 05-16-23-1047962 and it expires on May 15, 2024.

Please print or save this consent form for your records.

Obtaining your Consent:

If you feel you understand the study well enough to make an informed decision about it, please indicate your consent by replying to this email with the words, "I CONSENT.".

Appendix C: Interview Protocol

Interview Date: _____Assigned Code Name: _____

Interview Script

Introducing myself to the participant.

Thank the participants for accepting the invitation to participate in the study. Introduce the research topic to the participants. Ask the participant if the organization is currently in the process of any legal actions that relates to the research topic. If yes, the interview process would end immediately with an explanation on avoiding any risks to the organization or the participant. If no, then the researcher would commence with the other aspects of the interview protocol.

A copy of the Informed Consent Form would be provided to the participant and the contents of the form would be review the contents with the participants.

Give the participant the opportunity to ask any questions.

Inform the participant of the interview procedures and that a cell phone would be used as recording device.

Also inform the participants that notes would be taken with pen and paper.

Inform the participants that the interview would be between 30 to 60 minutes and that breaks would be allowed in between the session. Inform the participant of the process that would be used to protect their privacy and how the data captured would be stored and protected. Inform the participant that their participation is voluntary, and they have the right to withdraw from the study or stop the interview if they choose to do so at any time.

Remind the participant of the purpose of the study which is to explore the security strategies used by IT security managers to prevent breaches due to insider threats.

Once the participant understands the purpose of the interview and ready to commence, the audio recording would begin, and the interview process would start with the first interview question. I would ask further probing question(s) if required for clarity. I would allow the participant to be done with each question before proceeding to the next question.

Interview Question

What security strategy do you use to protect data and prevent breaches due to insider threats?

What strategy have you developed to analyze user behaviors to prevent data breaches?

What strategies have you implemented to detect and respond to security incidents that could result in a data breach?

What strategy do you use for risk identification and assessment to detect the possibility of a data breach?

Which data security management strategy best fit your business requirement and why?

What factors within and without your organization determine what security strategies to implement?

What notification approach do you use should a breach occur?

To prevent data breaches, what strategy do you use for third-party and vendor management?

What program do you use to help staff understand their security responsibilities?

What program do you use to keep your security team up to date with current security events?

What strategy do you use to establish security baselines and how often is this baseline reviewed?

What security breach incident have you experienced that was due to an insider threat?

What additional security strategies can you provide as a conclusion for this interview?

Appendix D: Email Invitation

Dear XXX,

This is to cordially invite you to participate in an interview process for ongoing research on the security strategies used to prevent insider threats in banking industries. I looked you up on LinkedIn and saw that you may have the required experience. The interview would take place remotely using zoom or any remote conferencing tool of your choice. Please be informed that your participation in this study is completely voluntary and there would not be any monetary compensation as a result. You may also withdraw your participation at any time within the study. Kindly let me know the most convenient time to reach out to you for this interview. I have attached the consent form to this email. If you feel you understand the study well enough to make an informed decision about it, please indicate your consent by replying to this email with the words, “I CONSENT.”.

Thank you

Ojodale Achor