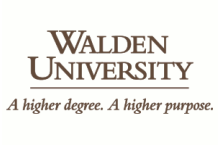

2019

Exploring Data Security Management Strategies for Preventing Data Breaches

Michael Samuel Ofori-Duodu
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Michael Samuel Ofori-Duodu

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. Steven Case, Committee Chairperson, Information Technology Faculty
Dr. Jodine Burchell, Committee Member, Information Technology Faculty
Dr. Charlie Shao, University Reviewer, Information Technology Faculty

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

Walden University
2019

Abstract

Exploring Data Security Management Strategies for Preventing Data Breaches

by

Michael Samuel Ofori-Duodu

MS, Walden University, 2018

BS, American Public University, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2019

Abstract

Insider threat continues to pose a risk to organizations, and in some cases, the country at large. Data breach events continue to show the insider threat risk has not subsided. This qualitative case study sought to explore the data security management strategies used by database and system administrators to prevent data breaches by malicious insiders. The study population consisted of database administrators and system administrators from a government contracting agency in the northeastern region of the United States. The general systems theory, developed by Von Bertalanffy, was used as the conceptual framework for the research study. The data collection process involved interviewing database and system administrators (n = 8), organizational documents and processes (n = 6), and direct observation of a training meeting (n = 3). By using methodological triangulation and by member checking with interviews and direct observation, efforts were taken to enhance the validity of the findings of this study. Through thematic analysis, 4 major themes emerged from the study: enforcement of organizational security policy through training, use of multifaceted identity and access management techniques, use of security frameworks, and use of strong technical control operations mechanisms. The findings of this study may benefit database and system administrators by enhancing their data security management strategies to prevent data breaches by malicious insiders. Enhanced data security management strategies may contribute to social change by protecting organizational and customer data from malicious insiders that could potentially lead to espionage, identity theft, trade secrets exposure, and cyber extortion.

Exploring Data Security Management Strategies for Preventing Data Breaches

by

Michael Samuel Ofori-Duodu

MS, Walden University, 2018

BS, American Public University, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2019

Dedication

This research study is dedicated to my wife, Tiffany, daughter, Victoria, and son, Isaiah, as well as my father, Seth, and belated mom, Victoria, family members, and friends. I would also like to dedicate this study to all IT practitioners, especially those working in the field of data security management, who day in and out fight to protect and safeguard information from reaching the hands of adversaries, and ultimately for the good of society. May we continue to strive for what is best and push through to preserve information confidentiality, integrity, and availability.

Acknowledgments

First, I want to give thanks to God for giving me the opportunity to pursue this degree and making all this possible. Secondly, without the support of my wife, Tiffany, daughter, Victoria, and son, Isaiah, this journey would be unimaginable; therefore, I would like to express my sincere appreciation for all their encouragement, sacrifice, and support. I would like to thank my father, Seth, for laying the foundation for me by stressing the importance of education, and my family members and friends for their continuous support and words of encouragement. You have all played a part in making this accomplishment possible.

I would also like to say a big thank you to my mentor and committee chair, Dr. Steven Case. I also want to thank my second committee member, Dr. Jodine Burchell, as well as my University Research Reviewer, Dr. Charlie Shao, and supporting staff, for their time and dedication in reviewing my work to ensure the highest quality of work is delivered. With your abundant guidance and support, this doctoral study has come to completion. Thank you.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

In the field of information technology (IT), humans and security are two entities which work together to ensure the safe and smooth operation of a system. Any shift in either component will offset this balance and cause disruption. One of those changes, on the human side of the scale, is an insider threat. Insider threats cost the average American firm $15.4 million per year (U.S. Department of Justice, 2015). A National Institute of Standards and Technology (NIST) survey revealed 20% of data breaches result from insider threats (NIST, 2011). Insider threats pose a serious problem to the organization by exploiting trusted relationships between humans and data.

Data exfiltration is one of the byproducts of insider threats. Per Schlicher, MacIntyre, and Abercrombie (2016), data exfiltration involves transporting data from within an organization to an entity outside of the organization. Additionally, partners and vendors are additional factors due to the collaborative nature of IT architecture today. As echoed by Quigley (2002), these relationships of organizations enable access to internal systems for suppliers and partners alike.

Recent research studies conducted on insider threat and how that relates to data breaches focus more on the reactive side of the fence, versus proactive. Liu, Shu, Yao, and Butt (2015) emphasized the importance of ensuring data transmitted and stored, especially in cloud solutions and is protected from data leaks. The technique involved a scan of the data in a target cloud solution using optimized algorithms to detect data leaks. Once a leak is detected using big data technology, encapsulation is performed by

transforming the leaked data identified to ensure information about the detected leak in itself does not become a risk. Lamba, Glazier, Schmerl, Pfeffer, and Garlan (2015) sought to create a clustering algorithm that combines contextual information and current data exfiltration events to determine if a data breach has occurred. The deficiency of this is the lack of strategies presented from the lack thereof of solutions to deter and prevent insider threats. More so, the idea will be to potentially use the findings of this study to contribute to the exploration of a solution that may be usable as a standardized framework in the IT industry.

Problem Statement

There is a lack of strategies for securing data from unauthorized trusted insiders. Researchers have found that a majority of small-scale IT government contracting firms do not place appropriate emphasis and investment in securing data from unauthorized trusted insiders (Densham, 2015). A large share of the $4.63 billion losses incurred by victim companies, attributes to data breaches by malicious insiders (Internet Crime Complaint Center, 2016). The perpetuation of this type of crime continues to ravage organizations of all sizes and sectors, causing security and economic concerns for companies and clients due to the dangers of sensitive information leakage. The general IT problem is that data breaches caused by malicious insiders are still prevalent due to the lack of data security management strategies. The specific IT problem is that some database and system administrators lack data security management strategies to prevent data breaches by malicious insiders in small-scale IT government contracting firms.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the data security management strategies that database and system administrators use to prevent data breaches by malicious insiders in small-scale IT government contracting agencies. The targeted population is database and system administrators of three small-scale IT government contracting agencies along the northeast region of the United States that have data security management strategies. The implication for positive social change is that by reducing data breaches, the unauthorized disclosure of consumers' sensitive information may subside, thereby preventing cases of identity theft and securing and preserving business secrets and reputation.

Nature of the Study

After considering the three methods of research, qualitative, quantitative, and mixed methods, I selected qualitative research methodology for the research study. The qualitative approach helps to gather information and obtain an understanding of human behavior and perspectives (Houghton, Murphy, Shaw, & Casey, 2015). This study explored the human behavior and perspectives of database and system administrators, and the data security management strategies they use to prevent data breaches by malicious insiders in small-scale IT government contracting agencies; therefore, the qualitative method is appropriate for this study. Quantitative research gathers quantifiable data needed for statistical analysis through the evaluation of relationships between variables, and the validation or invalidation of hypotheses (Gray, 2013). Because my study does not attempt to validate a hypothesis, I chose not to use a quantitative method. Mixed methods

research includes both qualitative and quantitative research elements (Mayoh & Onwuegbuzie, 2015). I did not choose the mixed method because I eliminated the quantitative approach. Therefore, I determined that the qualitative approach best suited my study.

Four qualitative research designs: case study, phenomenology, ethnography, and narrative were considered as the research design for this study. The case study research design was considered and chosen as the most suitable design for this study. Researchers use case study research design to conduct probing research by asking how and why questions to gain a deeper understanding of real-life situations in their naturally occurring setting (Bölte, 2014). Because the intent of this study is to understand and describe strategies used by database and system administrators to prevent data breaches by malicious insiders, the case study research design, specifically, a multiple case study research design, was the most appropriate to inform this study. Another research design considered was phenomenology. Sousa (2014) explained that phenomenology focuses on how research participants experience, live through, or infer the research study topic. Because the focus of the study is not on how the participants lived through the experience, phenomenology design is not the chosen research design. Ethnography was another research design considered. Ethnography design focuses on context or culture-based research of a specific group and targets the shared patterns of a particular culture (Small, Maher, & Kerr, 2014). The intent of this study is not to study any culture, ethnicity, geographical location, or group; therefore, using ethnography will not meet the goal of this research study. The narrative research design was another viable option

within the qualitative methodology. The narrative research design intends to create meaning through interview responses and concluding them with a story that broadens life's meaning (Grbich, 2015). However, the intent of this study is not to qualify life, but to focus on the data security management strategies used by database and system administrators to prevent data breaches by malicious insiders. Therefore, the narrative research design is not the choice for the study.

Research Question

What data security management strategies do database and system administrators use to prevent data breaches caused by malicious insiders?

Interview Questions

I conducted semi structured interviews with the participants of my study to explore data security management strategies they use to prevent data breaches by malicious insiders. The interview questions are open-ended to allow the researcher to capture as much information from each participant as possible. Appendix A contains the 12 interview questions I asked each participant of my doctoral study.

Conceptual Framework

I selected the general systems theory (GST) as the conceptual framework for the study. In 1937, Von Bertalanffy (1972) introduced the GST. Later in 1949 and 1972, Von Bertalanffy developed the theory further and revamped it, respectively. The GST focuses on the study of the interdependence of modules rather than the models working in isolation. Over the decades, Von Bertalanffy's GST has contributed significantly to many disciplinary fields, including philosophical, and extensible to the complete set of sciences

(Pouvreau, 2014). The GST approach provides a robust framework for security (Young & Leveson, 2014). Drack and Schwarz (2010) noted that key constitutes of the GST include function, structure, and process, which are the critical constructs to help inform this research study. Function pertains to the order of processes within the system and relates to how system components interact. Structure refers to a system component that is thoughtfully instituted, such as a business enterprise, or order of the various parts of an organization, among others. The process relates to the activities and dynamics that go on within the system to preserve it or cause a change.

As related to this study, the key constructs comprise a system, that is small-case IT contracting firms. Within the system, input functions include data security management strategies used by database and system administrators. This is a process that secures data from data breaches by a malicious insider and *output functions* or the prevention of data breaches by malicious insiders due to more secure systems. From a structure point of view, a cross-sectional analysis of participant organizations structures could help inform the study by identifying areas of improvement from one institution to the other. Processes implemented from one organization to another may help detect key data security management strategies. This may help to close gaps that allow malicious insiders to exploit. GST aligns with this study exploring data security management strategies to secure data that may result in reducing data breaches, and the unauthorized disclosure of consumers' sensitive information will subside; thereby preventing cases of identity theft, securing business secrets and preserving the reputation of an organization.

Definition of Terms

Anomalies: Anomalies are states of behavior that are unusual and deviate from the expected or norm (Goldberg, Young, Memory, & Senator, 2016).

Computer-readable extracts: Computer-readable extracts (CREs) are exports of data from information systems that hold some level of classified data (U.S. Department of Homeland Security, 2012).

Cybercriminals: Cybercriminals are individuals who use information and communications technology (ICT) to commit a crime, usually for personal gain, and are responsible for data breach incidents targeting organizations (Li, Yin, & Chen, 2016).

Data breaches: Data breaches are incidents that result from unauthorized access to data, compromising data confidentiality, integrity, and availability (Sen & Borle, 2015).

Database administrator: The database administrator or DBA role comprises the use of specialized software to organize and store data and ensures that data are available to authorized users and secured from unauthorized access (U.S. Department of Labor, 2018a). For the purposes of this study, the database administrator role encompasses personnel with job titles such as but not limited to database management specialist, database specialist, database architect, manager of database administration, database manager, database designer, database analyst, data administrator, data center support specialist, data quality manager, database engineer, and informaticist, among others.

Insider threats: Insider threats are current or former employees, contractors, and other interactors of the system with privileged access, and can circumvent security

mechanisms in place, steal valuable information, and cause damage (Jingguo, Gupta, & Rao, 2015).

Malicious insiders: Malicious insiders are current or former users of a system who has or has authorized access and has intentionally or accidentally violated system policy that adversely affected the confidentiality, integrity, or availability of a system (Nostro, Ceccarelli, Bondavalli, & Brancati, 2013).

Personally identifiable information: Personally identifiable information (PII) is any piece of information that is used solely or in conjunction with other information to identify an individual by direct or indirect inference (U.S. Department of Homeland Security, 2012).

System administrator: The system administrator or sysadmin role ensures the day-to-day operation and management of the computer systems of an organization (U.S. Department of Labor, 2018b). For this study, the system administrator role encompasses personnel with job titles such as but not limited to network systems administrator, security systems administrator, application administrator, system architect, and systems engineer, among others.

Trusted partners: Trusted partners are any business partners that have authorized access to a system (Caruso, 2003).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are unconscious, socially-shared beliefs, knowledge, and conventions believed to be accurate but may not be real (Atkinson, 2017). For my

doctoral study, I made some assumptions. I assumed that an efficient way to retrieve the data needed to answer my research question is to use the qualitative research method. I expected that my participants would understand the interview questions and responded honestly based on their knowledge and experience. Also, I assumed the number of participants would be enough to reach data saturation and reflect an accurate representation of the population sample. I ensured the knowledge and experience of my study to the best of my ability when collecting their participant eligibility information before the interviewing phase. I used open-ended questions in the semistructured interviews to allow participants to provide a considerable assessment with their responses rather than yes-or-no answers.

Limitations

Limitations in research studies allow researchers to communicate problems of their research study, and provide awareness of those problems to research reviewers, as well as discuss how to address those problems in the study (Allen, 2017). Limitations to research studies may not be intentional. The study did not include large-scale organizations; instead, I explored data security management strategies used by database and system administrators at small-scale government contracting firms. Data security management strategies of small-scale government contracting forms may differ from that of larger firms. Another limitation of my study was that the sample population of database and system administrators encompassed those who have experience and knowledge on questions I asked during the semistructured interviews around data security management strategies. The lack of experience in or around a specific subject

merited no data collected on those themes and topics. Also, I anticipated that the use of qualitative research methodology might introduce bias on my part, or by my participants.

Delimitations

Delimitations refer to the confines and context of the research study that is within the control of the researcher (Carson, Gilmore, Perry, & Gronhaug, 2001). The chosen geographical location for my research is the northeastern region of the United States; therefore, I only interviewed participants in this specific geographic area. Thus, the geographic location is a boundary set for this study. The constraints placed in my study isolated it to a particular population of the sample. The data collection may, therefore, not be a general representation of all cases in larger firms or other nongovernment contracting firms. Additionally, the nature of the chosen research design, a multiple case study, would not lend itself to ensuring external validity as case studies are restraining to the specific environments wherein the event occurred.

Significance of the Study

Contribution to Information Technology Practice

The significance of this research study will reside in the effort to explore data security management strategies whereby database and system administrators of small-scale IT government contracting firms can implement to prevent data breaches by malicious insiders. The response cost invested by database and system administrators to react to data breaches by malicious insiders are expensive (Posey, Roberts, & Lowry, 2015). Furthermore, the findings of the study might assist database and system administrators in preventing and addressing gaps in data security management strategies

to prevent data breaches by malicious insiders. Data from this study might assist database and system administrators in identifying best practices to avoid data breaches proactively, giving back time and peace of mind, while helping their organizations to save on cost incurred from reacting to data breaches.

Implications for Social Change

The implication for social change is that by reducing data breaches, the unauthorized disclosure of consumers' sensitive information may subside, thereby preventing cases of identity theft, and securing and preserving business secrets and reputation, respectively. The results of the study might contribute to social change by shedding light on data security management strategies which when implemented especially in small or large scale government information systems, may prevent data breaches by malicious insiders that could potentially lead to espionage, identity theft, trade secrets exposure, and cyber extortion, among others. Securing data is a cost-effective solution, and a must for organizations to prevent or reduce the risk of impact from breaches caused by insiders, which is more severe than that by outsiders as insiders have considerable knowledge of the data stored (Ho-Jae, Min-Woo, Jung-Ho, & Tai-Myoung, 2015). The damage caused by data breaches could ruin the reputation of an organization and incur legal ramifications.

A Review of the Professional and Academic Literature

Data breach incidents continue to cripple organizations of all sizes due to a variety of reasons, such as the lack of data security management strategies to prevent malicious insiders from perpetuating data breaches. The reason for this continuous trend

is due to the value of data today. Claycomb (2015) argued IT practitioners must recognize current trends as an important aspect of ensuring systems remain secure. Therefore, like keeping up with trends in the field of IT, defenders of information systems need to keep abreast of new capabilities, which could be exploitable by malicious insiders. Data is the fundamental and crucial element in systems used by IT enterprises. Therefore, my doctoral study research topic focuses specifically on safeguarding data, and not network browsing, or file access activities. In my review of the professional and academic literature, I discuss the GST, as well as establish grounds to use as a foundation for conducting my study (Liang, Biros, & Luse, 2016). Additionally, I relate these concepts to the research question of my study: What data security management strategies do database and system administrators use to prevent data breaches caused by malicious insiders?

From the literature reviewed, I discovered a variety of data management security strategies are already at the disposal and in reach of database and system administrators, although each implementation is different. I also noticed from reviewing the literature over and over that these four themes were reoccurring (a) the impact of data breaches to companies, consumers, society, and nation; (b) data security management administrative strategies; (c) data security management technical strategies; and (d) professionals' view on data security management. Therefore, the literature review for my study is based on these four themes.

The literature review spans across multiple years, that is, literature published within five years of my anticipated graduation date (2019), and are relevant to the

research topic, to encompass growth and trends in this doctoral study. I ensured the articles are peer-reviewed by using Ulrich's Periodicals Directory. The primary sources for my journal articles include the following research databases: Association for Computing Machinery (ACM) Digital Library, EBSCOhost Computers, and Applied Sciences Complete, IEEE Xplore Digital Library, ProQuest database, and Google Scholar. From the review of the literature, I found there was a gap in literature covering the use of a holistic data security management strategy that encompasses both technical and administrative data security management strategies. The prior literature contains technical or administrative strategy and not both; therefore, it does not portray a holistic strategy. In addition, some literature discussed strategies from a proactive stance and others from a reactive posture, but none of them addressed a combination of both. In summary, of the 12 papers relevant to this study, none of them sufficiently addressed data security management strategies in use by database and system administrators to prevent data breaches by malicious insiders.

As compared to other forms of cyber-attacks on the rise, the exponential growth of data breaches has a significant impact on organizations, and malicious insiders are the perpetrators to a sizable portion of these data breach accounts. In a review of the causes of data breaches, I observed that there are various manifestations and motivation factors of malicious insiders who perpetrate this crime. As suggested by Posey et al. (2015), some of these motivation factors are discoverable late. However, the proactive mechanism may be put in place to prevent or minimize breaches altogether, such as the use of proactive administrative and technical controls (Korpela, 2015; Padayachee,

2015). Both administrative and technical data security management controls complement each other and bring to a full cycle the three components of organizations: people, process, and technology.

Large volumes of research efforts are underway to gain a better understanding of some of the motivational factors of malicious insiders, but that is not the focus of this study. Burns, Posey, Roberts, and Lowry (2017) predicted behaviors of malicious insiders. Cates (2015) discussed the motivations of malicious insiders, which includes financial gains from the sale of financial information, personally identifiable information, and critical intellectual property. Both Cates and Burns et al. addressed the human aspect of the triad but may not be enough to prevent data breaches by malicious insiders; therefore, a combination of strategies that satisfy all three elements of an organization may be vital. To predict the risk to organizations from a data breach attack, additional components such as the use of the Bayesian belief network are introduced (Sticha & Axelrad, 2016). Having considered the inevitable, data breaches are bound to occur (Cho & Lee, 2016); therefore, the focus of this study is to gain a better understanding of data security management strategies implemented by organizations to prevent data breaches by malicious insiders.

The General Systems Theory

The purpose of this qualitative multiple case study is to explore data security management strategies that database and system administrators use to prevent data breaches by malicious insiders. In my literature review, I discussed GST as the conceptual framework as it related to the focus of my literature review. The research

question was: What data security management strategies do database and system administrators use to prevent data breaches caused by malicious insiders?

To explore the research and assess my discoveries through foundational content, past and current research, and trends and innovations in information security, I used the GST as the conceptual framework for the study. Von Bertalanffy (1972) developed the GST from which the system theory originates from. The GST focuses on the nature of complex systems and is a framework researchers use to explore or describe the interdependence of objects working together to yield some result rather than the objects working in isolation. Fundamental tenets of the systems theory include (a) objects or variables within the system, (b) system and object attributes, (c) the interrelationships existing between objects within the system, and (d) the presence of the system within an environment. The GST approach provides a robust framework for understanding the complexities of a system (Schneider, Wickert, & Marti, 2017); hence, it will support exploring data security management strategies used by database and system administrators to prevent data breaches caused by malicious insiders.

The GST is applicable to this doctoral study. The constructs align well with information systems within organizations, and the data stored in these systems. Data security management strategies align with attributes of the information system. Another attribute alignment is the movement of data into, from, or within the system. The presence of data consumers indicates the use of information systems within an environment. From a structural perspective, systems theory provides a lens from which to

explore the relationship between data security management strategy, provisioned by database and system administrators to secure organizational data.

The Evolution of the General Systems Theory

The GST explains that systems are comprised of individual subsystems that work together as a whole. In the use of the analogy of the system theory as a premise, a car is a system; however, the separate car parts do not define the car as a system on their own. The various parts assembled and working units make up the car system. Therefore, Von Bertalanffy (1972) asserted in the definition of a system, the individual subsystems should not be used to describe the system, but a comprehensive approach should be used.

Over the years, there have been significant contributions to the systems theory. Kast and Rosenzweig (1972) discussed the need to review the study the complexity of systems in both science and technology rather than the analysis of a system. In a study of the generations of complexity theories, Alhadeff-Jones (2008) pointed out contributions made by Morin in 1977 and 1980, as well as Moignein 1990, that challenged the inherent nature of the system theory to be linear, and hierarchical, among other epistemological legitimacy facets. Ceric (2015) described systems theory as a method that enables the holistic understanding of the interdependencies between the elements of a system, which is critical to evaluate and manage the target system successfully. An application of the system theory is a derivative of it called the general technical system theory in which a system plays a specific role in the general functions within an environment such as performing a function of transferring human inputs, materials, energy or signals to the output of humans, materials, energy or signals (Wang, Zhang, & Wang, 2016).

Supporting Theories

Multiple theories could be used from different viewpoints to perform a research study on data security management strategies to prevent data breaches. Theories such as the soft systems methodology (SSM), open systems theory (OST), and theory of planned behavior (TPB) have been used as the conceptual framework in other researches on data breaches in organizations caused by malicious insiders. The supporting theories noted depict their purposes and how they can be used as the lenses to explore the research question for my study, although I did not choose them as the conceptual framework for this study. I chose the GST to explore data security management strategies in use by database and system administrators to prevent data breaches caused by malicious insiders.

SSM is one supporting theory of GST. The SSM is described as a technique used to solve complex and unclear problems (Fitroh & Utama, 2017). SSM was developed by Checkland and involves the use of a series of stages to evaluate a phenomenon to obtain a holistic view. Four various kinds of activity are used in the SSM model, including finding out the problematical situation, making purposeful activity models relevant to the situation, using the models to question the situation, and defining or acting to improve the situation. A mnemonic often associated with SSM is CATWOE, which stands for customers, actors, transformation process, Weltanschauung, owners, and environmental constraints. SSM supports GST as it focuses on the impact of an action or lack of thereof of actors within a system and how the existing association between entities in the system are affected.

OST is a supporting theory of GST and was developed after the second world war. In a study to explore the interconnection of the GST and OST in 2015, Norman determined the use of the GST allowed the identification of the components of the phenomenon under study, whereas the use of the OST helped to understand how the system influences system-related entities. Malecic (2017) argued that it is vital for researchers to understand systemness as a characteristic of GST and identify where to find it in life applications. Understanding the inputs, internal process, and outputs of a system allow researchers to grasp an in-depth understanding of the phenomena under study. OST supports GST as it posits that systems are strongly under the influence of their environment.

The TPB is another supporting theory of GST. TPB was instituted and revisited by Icek Ajzen in 1988 and 1991, respectively (Ajzen, 2004), to help understand how to change the behavior of people. Researchers use theories to allow the exploring of a phenomenon or answer a research question from the perspective of the theory using that as the lens through which to view a phenomenon (Hasking & Schofield, 2015). TPB posits that the outcome of a specific behavior is based on the intentions of that behavior resulting from subjective norms, attitudes, and behavioral control perceived. TPB allows researchers to link the belief and behavior of a phenomenon through predictability. Sutton and White (2016), used TPB as the lens to predict sun-protective intentions and behaviors. TPB supports GST as it focuses on investigating factors associated with an entity based on what is believed.

Another supporting theory of GST is the critical systems thinking theory. Critical systems thinking theory is known to have roots in soft systems theory. Critical components of the systems thinking approach are its critical stance against inclusion and exclusion factors constituting the problem settings under review, and utilization of various systems methods based on the characteristics of the situation encountered (Flood, 1990). Critical systems thinking theory comprises the integration of critical theory and practice in systems that may be diverse and advises how best to use such systems.

Contrasting Theories

Grey systems theory is a contrasting model to the GST. The grey systems theory, established by Julong Den in 1982, operates under four models: even grey model, original difference grey model, even difference grey model, and discrete grey model (Liu & Lin, 2010). Liu, Yang, Xie, and Forrest (2016) suggested that researchers use grey systems theory, especially in situations where available information is incomplete, and the data collected lacks accuracy. The aim of grey systems and its application is to link social science and natural science and may also be used to determine the probability of occurrence of incidents, due to the difficulty in making that determination with certainty (Omidvari, Abootorabi, & Mehrno, 2016). Unlike the GST, where elements of a system are known, grey systems lack information, such as behavior document, structure message, and operation mechanism. The differences between the grey systems theory and systems theory are substantial that the two theories are in contrast.

General Systems Theory Applied to Data Security Management

Von Bertalanffy (1972) described systems theory as the study of the interdependence of modules within a system rather than the models working in isolation. The systems theory is a central theory used in the investigation of systems not only in a modular fashion but as a whole due to the interaction of the individual components that make up the system (Bridgen, 2017). System theory views a system in its completeness and the relationships between the various subsystems constituting the whole system (Von Bertalanffy, 1968). In a study of modeling to deter insider threats, Casey, Morales, Wright, Zhu, and Mishra (2016) found that the in-depth look at the interaction between senders and receivers in a system presents great insight into the static or dynamic nature of information with which an organization can build simulations and parameters to learn insider behavior. Similarly, this study intends to explore the interactions within a system to obtain insight into the effects of the various components on each other, as well as on the system as a whole.

The critical components of the systems theory are (a) objects within the system, (b) attributes of the objects within the system, (c) the relationship between the system objects, and(d) the presence of the system inside an environment (Von Bertalanffy, 1968). As this related to my doctoral study topic, (a) the organization and the information systems are objects, (b) data security management strategies are attributes, (c) data residing within information systems connected to the network of the organization represents relationships, and (d) information systems containing data within the organization depicts the presence of a system inside an environment.

I chose the systems theory as the lenses for my doctoral study to explore data security management strategies used by database and system administrators within an organization, the threats of malicious insiders to cause data breaches, and the outcomes of implementing the specific strategies to deter and prevent data breaches. To understand and explore the relationship between the components of my study: database and system administrators, information systems, data, malicious insiders, and data breaches, in the context of my study, a relationship exists between all four components.

Like managing any shop, taking an inventory of and defining what is in stock is the right place to start. Likewise, information systems hold a variety of data, including personal data, confidential data, geographical data, images, and financial data, among others. Performing this type of planning activity provides visibility into data areas that may not have been transparent and well understood, leading to the development of a holistic data security management strategy that encompasses all data areas. The laws and regulations that govern organizations have an influence on the type of data classification in use. Zhurin (2015) asserted a variety of regulatory documents at the disposal of organizations could be used as part of their strategy to prevent insider threats. Some of the laws and regulations implemented are a result of threats and impacts from the international community (Atkinson, 2016). Compliance with such laws fosters international relationships, meaning international help is accessible in times of need.

The process of defining organizational assets, especially data around personnel, process, and technology, it is vital to determine the resources that require protection, the value, and classification based on priority. Attributes such as the location of the data

element, the type of asset associated with that piece of data, the classification level such as whether the data is personally identifiable information (PII), sensitive PII (SPII), or protected health information (PHI), among others, needs consideration, while keeping in mind the cost and effort value. Also, Bakar and Selamat (2016) asserted it is crucial to consider how data is used primarily in crowdsourcing information systems to preserve data confidentiality.

Performing the act of determining risk levels and classification of data will ensure the appropriate classification of data and risk level, to ensure association of the right level of emphasis on data that has little to no impact on the organization should there be a compromise. Kenney (2015) suggested another side of the coin to this aspect of data risk assessment and classification is the importance of gaining an understanding of the diverse types of potential threats to organizational data. Setiawan and Sastrosubroto (2016) found that in circumstances where a layered security strategy is in use, organizations stood a higher chance of deterring and preventing data breaches by malicious insiders. Alongside planning and classification of the risk of data, if compromised, it is vital for organizations to assess the impact and threats that may come with their data.

Data Security Management Explained

The information security triad: confidentiality, integrity, and availability play a vital role in the establishment of a data security management strategy within an organization. As suggested by Moghaddasi, Sajjadi, and Kamkarhaghighi (2016), data security management ensures the identity of the source or sender of data, the integrity of the data, and the identity of the destination or receiver. The assurance and control

afforded by data security management allow for flexibility and expansion with the evolution of ICT, ensuring new features or areas are brought under the umbrella of an organization's data security management strategy. Data stored in systems come in a variety of forms. For instance, in the study performed by Razaque and Rizvi (2016), the data is stored in a cloud storage system, whereas the data reviewed in the study by Shalev, Keidar, Moatti, and Weinsberg (2016), reflect the use of security controls to protect data stored on-premise; however, despite the location of the data storage, the level of damage of a breach is the same. Establishing a mechanism to monitor and detect insider threats by malicious users, accessing data, and combining this information with other established insider threat solutions, may provide an organization with a more revealing insight into the posture of the security policies and controls around the security of their data.

Data Security Management Conceptual Model

From a technical strategy point of view, based on the reviewed literature, the aspect of the IT industry focusing on data security management continues to make long strides to enhance the strategies used by database and system administrators to prevent data breaches by malicious insiders. For instance, in both government and private sectors, smart cards are in use by personnel to increase the authentication factor level of privileged users. Despite known vulnerabilities with smart card and password authentication are exploitable through an attack known as privileged insider attack, where obtained private key credentials could be used to impersonate access to a system, two-factor authentication in general provides added protection to the authentication of

personnel (Wang, D., Wang, N., Wang, P., & Qing, 2015). Authentication plays a key role in the protective mechanisms that an organization can use to prevent data breaches by malicious insiders. Also, personnel background checks are more intense, and at more detail than ever before, to ascertain new hires and employee personnel clearance renewals are adequately performed before entrusting them with classified information.

Another observation made during my review of the literature related to my research topic is that most of the researchers leveraged the general system theoretical framework. Also, most of the researchers conducted their work using case studies, and data provided to them by a partner or some form of collaboration with a more extensive IT establishment or entity. For instance, the research conducted by Shalev et al. (2016) involved gaining access to the database of the IBM Research IT department.

Aspects of the topic that have been researched include (a) the setup of an auditing mechanism to monitor privileged user behavior and isolating any anomalies for further review; (b) the identification and establishment of a baseline either by previous behavior, canned roles, or peers; and (c) the proactive detection of insider threat based on a specific policy, or the behavioral pattern of a known insider threat (Agrafiotis, Erola, Goldsmith, & Creese, 2016).

Aspects of the topic that needs to be researched further, according to the reviewed articles include (a) the implementation of the identified solutions in a large-scale environment, (b) the elevation of a role by nonprivileged users through collusion, (c) the lack of a cross-platform solution for enterprises with a hybrid architecture of operating

systems (Lamba et al., 2015), and (d) the lack of an automated mechanism to temporarily disable infringing accounts.

Based on the literature review, held assumptions existing within the field include the general notion that only privileged users can pose insider threats to organizations. Also, there is a vague notion that users of systems are security savvy, and educating personnel on security awareness is not a priority. Education on other aspects of security is prevalent today. However, education specifically on the topic of the insider threat is lacking. Educating users about early indicators of insider threat and providing information on the communication channels to use for reporting suspicious malicious insider behavior confidentially, could help reduce the likelihood of insider threat occurring.

Insider Threats Explained

From the literature review conducted, a held assumption that exists in some IT organizations is the general notion that only malicious privileged users could become insider threats, ignoring the need to train and educate the nonprivileged personnel, making them more vulnerable to vectors such as social engineering, whereby malicious staff could collude with them or take advantage of them. The lack of education and training of users on how to handle and report suspicious activity could also contribute to factors leading to data breaches.

Insider threats could take a variety of forms, resulting in varying magnitudes of a threat to companies. Per Legg, Buckley, Goldsmith, and Creese (2015), three main categories of insider threats include the following: IT sabotage, theft of intellectual

property, and data fraud. Each of these categories affects the victim organization in a significant way, for some at a higher magnitude than others. Irrespective of the class, Zaytsev, Malyuk, and Miloslavskaya (2017) suggested insider threat can be subsided with the use of strategies, including behavioral models that develop a taxonomy for insiders, attacks, countermeasures, the study of organizational threats with the development of forecasting models, and, early detection techniques. The latter is made possible via the use of technical tools.

Insider Threat Attack Schemes

The threat of malicious insider activity may stem from current employees, previous employees, contractors, or third parties, including organizational partners and vendors. Each of these entities interacting with or within the organization can cause devastation to the organization. The root cause of insider threats is either accidental or malicious. Some organizations find it challenging to secure their enterprise data from cybercriminals. Continuous monitoring and auditing mechanisms are implemented to help detect and report activities by cybercriminals. While these measures have proven to be effective in protecting data from external intruders, some organizations continue to face challenges such as unauthorized access and use of data by insiders, such as altering data through unapproved means (Sallam & Bertino, 2017), and the unauthorized use of CREs. Cheng, Liu, and Yao (2017) concluded that the effect of the data breach, whether intentional or accidental could pose a severe threat to an organization, including reputational damage and financial losses, among others. The focus of my study is on the latter; that is, preventing data breaches resulting from malicious insiders by exploring

data security management strategies are in use to prevent malicious insiders from causing data breaches.

The Impact of Data Breaches on Companies, Consumers, Society, and Nation

The dependency on data in today's information age is high compared to previous eras. Data collection is in amass, from organizations capturing information about their clients to national security information, which, if compromised, can cause irreversible damage to a nation. Knowledge of the impact and threats of data breaches to organizational data may help prioritize the areas of focus when planning for countermeasures to apply for a defense-in-depth strategy. Gaining an understanding of the type of architecture and infrastructure in use will allow the database and system administrators to make an informed decision on the security strategies to implement to secure organizational data. The use of a risk matrix, organizations would be able to assess the probability and impact the breach of a specific classification of data could have not only on the organization but also in the case of stolen PII or PHI, clients whose information was compromised.

Phillips, Mazzuchi, and Sarkani (2018) studied the risk of vulnerabilities and defects in context is minimizable by ensuring security and resiliency of the system architecture, including software, hardware, and other components. Also, a business impact analysis based on the data from the prior data risk assessment and classification would provide insight into the impact a data breach would have on the organization and clients. Rao and Selvamani (2015) concluded it is imperative for organizations to assess the impact an environment may have on their organizational assets prior to use. The

information gathered and assembled from the planning would serve as input in the devising of a layered strategy to protect organizational resources.

Data Security Management Technical Strategies

Technical controls are one of two classes of countermeasures that may be in use by firms to deter and prevent data breaches by malicious insiders. Technical controls alone may not be enough to combat data breaches by malicious insiders but may serve as a layer of defense. One of the more recent technical controls leveraged by firms is the use of virtualization. Some threats may be more challenging to implement countermeasures for, such as zero-day vulnerabilities; however, Last (2016) suggested developing a plan with vendors or system providers to react to such attacks quickly will benefit organizations. In cases where commercial-off-the-shelf software is in use by an organization, ensuring the software is patched will not only prevent vulnerabilities from being exploited but also will provide software warranty and license agreements are maintained.

About virtualization, some organizations move their infrastructure and operations to use cloud technology despite the known risks of privacy and integrity (Sulochana & Dubey, 2015). Cloud solutions are known to offer more flexibility when it comes to data availability (Dieye, Zhani, & Elbiaze, 2017); however, they are also known to have tenets on the security of users' data being the highest priority as well as a concern (Chang & Ramachandran, 2016). Trends software-as-a-service (SaaS) is a type of cloud technology that affords organizations the capability to move entire enterprise resource planning (ERP) systems to the cloud (Saa, Moscoso-Zea, Costales, & Lujan-Mora, 2017).

Outsourcing of data storage and management is another similar strategy used by some organizations to save on cost. In such situations, data travels across physical geographical boundaries are now flat due to virtualization and globalization.

The use of encryption is a strategy some organizations use to minimize the threat of sensitive information at rest and in transit reaching the hands of adversaries. Malicious insiders can exploit vulnerabilities on a network without having direct access to the data stored in the systems; hence, the need to secure data, not only at rest but also in transit (Jung, Valero, Bourgeois, & Beyah, 2015). Encrypting data stored in database systems alone does not as incorporate a holistic solution without securing data in transit as well. However, along with some encryption techniques comes issues with performance and key management. Kumar, Meena, Singh, and Vardhan (2015) concluded the strength of the encryption strategy is as effective as the management of the key; weak key management means an elevated risk of compromise. Some encryption solutions incorporate a block indexing strategy to overcome the issue of performance resulting from the negative impact of encryption on performance (Yuan et al., 2017). In some encryption solutions, detecting and minimizing data breaches by trusted insiders is achievable via the use of a use-once key encryption model (Blasco, Tapiador, Peris-Lopez, & Suarez-Tangil, 2015). The model entails the use of a key to encrypt sensitive files and disallow retrieval of files without prior access to other related files. The approach forces the insider to extract more data than what is needed and, therefore, takes the insider a longer time and increases the effort required by the insiders. In some cases, the frustration resulting from the length of time taken to extract information may be too concerning for malicious insiders and may

deter them. Encryption techniques shield the data from unauthorized access and enforce data confidentiality, and in some cases, nonrepudiation.

In most cases, technical controls are effective in protecting external entities from protruding the network boundary of an organization. The use of devices includes firewalls, load balancers, intrusion detection devices, intrusion prevention devices, honeypots, antivirus, proxy servers, and change detection tools such as tripwire, among others. The detection of malicious insider activity is known to be challenging to detect using technical controls. Countless techniques are under consideration to use by some organizations to help detect malicious insider activity. One such method is the use of a combination of anomaly detection and signature-based techniques to identify potential security breaches (Chae, Katenka, & Dipippo, 2016). A combination of techniques offense a defense-in-depth strategy, offering a more resilient strategy for preventing data breaches. The addition of administrative strategies to an existing technical strategy offers more robust solutions to combat malicious insider activity.

Data Security Management Administrative Strategies

Administrative countermeasures are known to be the most effective when it comes to dealing with threats related to humans, who are also known to be the weakest link in the information security chain. Andersson and Caporuscio (2016) described administrative controls as security controls that can do without technical controls and do not rely on technical or technology controls. Humans or personnel within an organization may become malicious due to several reasons, including (a) retaliation for culture change due to being irate, (b) becoming disgruntled due to unresolved organization-related

issues, (c) financial burden, (d) rewards from corporate espionage, and (e) pride in whistleblowing or sale of trade secrets.

Nostro et al. (2013) described malicious insiders as previous or current users of a system who has authorized access to the target system and has purposely violated the organizational policy, leading to an adverse impact on that target system by compromising the confidentiality, integrity, or availability of the system. Knowing the traits of malicious insiders is key to developing strategies to deter and prevent them from carrying out their activities. Known characteristics of malicious insiders include (a) the unauthorized use of work resources such as the Internet, email, and instant messaging for personal correspondence, (b) unauthorized upload of proprietary organizational information to an external drive or a covert storage locally or in the cloud, (c) tailgating in unauthorized secure areas, (d) working during unofficial hours and unusually transferring large volumes of data, (e) using social engineering techniques against peers to gain unauthorized information, (f) conducting phishing attacks, shoulder surfing, and dumpster diving, and (g) planting logic and time bombs in applications, or creating unauthorized back doors, among others.

Asset management is a vital strategy an organization may use to protect their assets. Knowledge of the hardware, software, and devices on the network allows organizations to detect any deviations from the captured baseline quickly. Having an executable routine in place on a regular schedule and maintained will provide an organization with insight into any changes to their infrastructure should any rogue nodes be set up on their network.

Another countermeasure database and system administrators may include in their data security management policy is collaborating with the human resources department to develop profiles on employees that show traits of malicious intent. In a study of design and validation of the information security culture framework in 2015, AlHogail determined the need for organizations to establish an organizational culture rich in information security to impact the security behavior and perceptions of employees. The use of the structured STOPE (strategy, technology, organization, people, and environment) framework in conjunction with another framework known as the human factor diamond, which takes into consideration preparedness, responsibility, management, and society and regulations, could be used to assess the culture of the target organization (AlHogail, 2015). Maasberg, Warren, and Beebe (2015) suggested the use of the Dark Triad personality survey instrument to evaluate new employees, just as the Myers-Briggs Type Indicator (MBTI) assessment and the Adjective Check List (ACL) are in use to identify personality and psychological traits, this way organizations can have a closer view of what goes on in the minds of malicious insiders. As part of the organizational policy, personnel should retake the Dark Triad personality survey to identify any anomalies or changes that may have occurred over time.

A well-known strategy database and system administrators implement is a proactive administrative strategy to counteract malicious insider activity leading to data breaches is, security education, and training awareness (SETA) programs. Educate administrators on the need to know the type of data their systems hold, their various access mechanisms, and personnel authorized to access the system, could be a good

strategy to start (Urciuoli & Hintsa, 2017). Bauer, Bernroider, and Chudzikowski(2017) concluded organization should focus more attention on the administrative information security controls of their firm and invest in prevention strategies such as SETA programs. Measuring the effectiveness of SETA programs is an activity that should not be taken lightly by organizations. A research study conducted by Hina and Dominic (2016) revealed there is a relationship between security incidents that occur due to negligence and the erratic behavior of the target population resulting in insider threats to the safety of organizational data. On the contrary, a study performed by Hwang and Cha (2018) revealed the opposite, asserting that the stress resulting from SETA programs leads to role stress and technostress, resulting in lower levels of compliance intention regarding organizational information security.

The creation and implementation of an organizational information security policy (ISP) is another strategy in use by database and system administrators to prevent data breaches. Ismail, Widyarto, Ahmad, and Ghani (2017) concluded ISP portrays an organization's stance towards both internal and external information assets needing protection from unauthorized access, disclosure, destruction, and modification. ISPs comprise information about the rules and boundaries of operation within an organization and consequences for violating the rules set forth. Making sure there is a balance and appropriation for the disciplinary action taken due to employee noncompliance will prevent sanctions or related punishments from negatively affecting them (Aurigemma & Mattson, 2017). The method of application of sanctions should be one that promotes a positive work culture.

Also, it is crucial that the ISP is easy to understand and interpret. Buthelezi, Van Der Poll, and Ochola (2016) found that clear ISPs facilitate implementation with no difficulty and avoid misinterpretation and ambiguity, resulting in conformity and uniformity by personnel across an organization. Management support for a zero-tolerance policy is an essential facet to ensuring conformity and compliance to ISPs by all staff; especially, when it comes to cultural elements, and internal processes such as system development life cycle (SDLC), change control, change management, and release management, among others.

Knowledge of the life cycle of the types of data in use by organizations would put them in a better position to ensure adequate strategies are in place to safeguard data entering the information system of the organization, data stored, as it travels internally within and externally from the organization due to vendors and partners, among others. Graves (2017) stated the lack of information about how data flows in, out, and the reasons put organizations at a higher risk for data breaches due to the lack of awareness and ability to apply strategies to critical data flow points, which are exploitable by malicious insiders. It is crucial for database and system administrators to include strategies to routinely audit and measures the effectiveness of data security management strategies implemented throughout the life cycle of organizational data (Ramachandran & Victor, 2016).

About the end-of-life of data in a data life cycle, in situations where third parties are involved in the destruction of information system storage devices, strategies must be set in place to conduct a follow-up check with the vendor to ensure the vendor uses

appropriate storage destruction techniques. Dedicated shredding bins should be allocated to the office space and monitored to ensure unwanted CREs are disposed of correctly. It defeats the purpose of implementing strategies to protect data within information systems but fail to safeguard the same data after it leaves the system. Imran et al. (2017) suggested the use of data provenance to track the origin or last known history of a specific piece of datum. Using such a technique creates an audit trail on data as it moves throughout or outside of the environment, in this case, the organization providing the needed insight organizational personnel could tap into should there be a data breach. In Table 1, I detail the evidence of the reoccurring themes across the literature I reviewed and included an entry at the bottom of the table, indicating the strategic themes I intend to cover in my study.

Table 1

Matrix of Literature Comparison

Author	Theme 1	Theme 2	Theme 3	Theme 4
Ali, O., & Ouda, A. (2016)	Administrative			Reactive
Alihodzic, A., Tuba, E., &Tuba, M. (2017)	Administrative	Technical		Reactive
Aurigemma, S., & Mattson, T. (2017)	Administrative			Reactive
Bauer et al. (2017)	Administrative			Reactive
Buthelezi et al. (2016)	Administrative			Reactive
Chae et al. (2016)		Technical	Proactive	
Chang, V., & Ramachandran, M. (2016)		Technical		Reactive
Dieye et al. (2017)		Technical		Reactive
Forde, E. S. (2017)	Administrative			Reactive
Graves, J. (2017)	Administrative			Reactive
Hina, S., & Dominic, D. D. (2016)	Administrative			Reactive

(continued)

Author	Theme 1	Theme 2	Theme 3	Theme 4
Hwang, I., & Cha, O. (2018)	Administrative			Reactive
Imran et al. (2017)	Administrative			Reactive
Irfan, M., Abbas, H., Sun, Y., Sajid, A., & Pasha, M. (2016).	Administrative			Reactive
Ismail et al. (2017)	Administrative			Reactive
Korpela, K. (2015)	Administrative		Proactive	
Kumar et al. (2015)		Technical	Proactive	
Last, D. (2016)		Technical		Reactive
Maasberg et al. (2015)	Administrative		Proactive	
Phillips et al. (2018)	Administrative			Reactive
Ramachandran, M., & Victor, C. (2016)	Administrative			Reactive
Saa et al. (2017)		Technical		Reactive
Sulochana, M., & Dubey, O. (2015)		Technical		Reactive
Wagner et al. (2017)	Administrative			Reactive
Yuan et al. (2017)		Technical		Reactive

Solutions Implemented by Database and System Administrators

The overall strategies in use by organizations are effective from a general point-of-view; however, that begs the question of how these high-level strategies trickle down and apply to database and system administrators in ensuring the prevention of data breaches. First, technical strategies are as effective as what, when, how, and why specific technics and solutions are used and managed by database and system administrators. In a nutshell, the following are some technical solutions in use by database and system administrators: (a) scaling back excessive privileges, (b) avoiding granting default privileges, (c) securing media exposure (backups) using encryption and expiration, (d) automating auditing and monitoring of administrators' activities, (e) testing patches and releasing in a well-timed maintenance window, (f) balancing administrators' workload, (g) managing and keeping inventory of forgotten databases and backups, (h)

implementing database security controls, (i) enforcing database security plans and policies, (j) conducting incident response activities, (k) removing dormant database users, (l) monitoring access patterns in real-time to detect data leakage and unauthorized transactions, (m) archiving external data and encrypting databases as well as backups, (n) training database and system administrators on risk mitigation, (o) enforcing database management best practices, (p) implementing strict firewall rules, and (q) removing unneeded services to reduce attack surface. In Table 2, I show a classification of the solutions mentioned as administrative or technical controls, and a corresponding column showing the purpose of the solution.

Table 2

Classification of Solutions

Solution	Classification	Purpose
Scaling back excessive privileges	Technical	To ensure the least privilege permissions and need-to-know is enforced.
Avoiding granting default privileges	Technical	To prevent privilege escalation and masquerading
Securing media exposure (backups) using encryption and expiration	Technical	To prevent malicious access to backups and enforce appropriate backup set disposal
Automating auditing and monitoring of administrators' activities	Technical	To receive notifications of security incidents close to real-time
Testing patches and releasing in a well-timed maintenance window	Technical	To ensure vulnerabilities are mitigated, and minimal to no risk is introduced to the live production system

(continued)

Solution	Classification	Purpose
Balancing administrators' workload	Administrative	The evenly distributed workload of database and system administrators prevents burnout. In a way, this strategy enforces the separation of duties, which is a role-based access control mechanism. Therefore, balancing of workload reduces the number of permissions to be managed within a system (Ultra & Pancho-Festin, 2017)
Managing and keeping an inventory of forgotten databases and backups	Administrative	To ensure that any form of access and retrieval is accounted for. Unauthorized or out-of-norm behavior, which could be an indication of malicious activity, could be easily identified by reviewing access logs for inventoried databases and backups
Implementing database security controls	Technical	To ensure confidentiality, integrity, and availability of database management systems to ensure the appropriate levels of access and permissions are assigned to application and human accounts that connect to and use database management systems
Enforcing database security plans and policies	Administrative and Technical	To ensure routine checks are performed to uncover any deviations from a documented system baseline such as in a System Security Plan (SSP) are reviewed and justified. Also, enforcing database security policies ensures compliance with regulations that may be governing an organization. Some examples of industry-based controls include Center for Internet Security (CIS) benchmarks, NIST special publication (SP) 800-53 controls, and DoD Defense Information System Agency (DISA) Security Technical Implementations Guidelines (STIGs)
Conducting incident response activities	Administrative and Technical	To ensure that database and system administrators, as well as the incident response team clearly understand their roles and responsibilities, as well as the

Solution	Classification	Purpose
		courses of action to be taken when an incident occurs
Removing dormant database users	Technical	To ensure that users who no longer have the authorization to access, such as terminated employees, or employees whose roles have changed, are accounted for, and restricted accordingly
Monitoring access patterns in real-time to detect data leakage and unauthorized transactions	Technical	To ensure any abnormal access patterns and behaviors are detected quickly and resolved timely
Archiving external data and encrypting databases as well as backups	Technical	To ensure all incoming and outgoing data points are accounted for, and only accessible by the authorized database and system administrators, and third parties, such as vendors and partners
Training database and system administrators on risk mitigation	Administrative	Regular training will ensure compliance with current federal regulations and equip database and system administrators with the knowledge to identify and mitigate threats including those from within such as social engineering, shoulder surfing, phishing, and collusion, among others
Enforcing database management best practices	Administrative and Technical	To ensure best coding practices are followed thus prevent Structured Query Language (SQL) injection, brute-force, unauthorized privilege escalation, and exploitation of unpatched database vulnerabilities
Implementing a strict firewall ruleset	Technical	To ensure only authorized traffic to the database system, and easily identify any attempts to exfiltrate or circumvent access to the database through a backdoor
(table continues)		
Removing unneeded services to reduce the attack surface	Technical	To ensure only the services needed are running; therefore, reducing the chances of attackers using irrelevant services as a hook to reach into the

Solution	Classification	Purpose
		operating system (OS) layer which may lead to greater system compromise

Transition and Summary

The GST by Von Bertalanffy demonstrates the impact of interdependent elements of people, processes, and technology working together in organizations to secure organizational assets rather than each element working in isolation to achieve the same. The GST is applicable to both small and large-scale organizations and focuses on interdependent objects working together in a complex system while considering the impact of external factors on the target system. This theory suits well research related to exploring and describing the impact data security management strategies have on the prevention of data breaches by malicious insiders.

Within this section, I discussed the topic of data security management strategies and the impact of insider threats on this paradigm. By leveraging the GST as the lens for my study, it allowed me to explore data security management strategies and the impact on organizations. The review of the literature centered on explanations of data security management, insider threats, insider threat attack schemes, the impact of data breaches, and data security management technical and administrative strategies.

Based on the literature, there were no areas of discourse, contention, or divergent perspectives. The literature reviewed identified the need for the improvement of insider threat detection, or better yet, the prevention of data breaches caused by a malicious insider altogether. The articles acknowledge that we, humans, are the weakest link in the information security chain. I discovered from the reviewed literature that trust is a

standard theme across all the articles and plays a significant role in any IT enterprise, whether small or large and private or government. The next section, Section 2, discusses further areas of my research study, including the role of the researcher, participants, research methodology, and design I chose for this study, population, and sampling, as well as ethical research. Also, this section presents data collection, organization, and analysis strategies, and addresses the topics of reliability and validity.

Section 2: The Project

In this section, I will provide information on the role of the researcher, potential participants, the criteria for selection of participants, population sampling, and research methodology. Also, in this section, I will address ethical subjects relating to my study and steps I may take to alleviate such factors. Last, I will describe the data collection instruments, data collection approach, data organization techniques, and data analysis, as well as explain issues of reliability and validity in the context of this study. I will then provide a transition and summary, leading to the final phase of my doctoral study.

Purpose Statement

The purpose of this qualitative multiple case study is to explore the data security management strategies that database and system administrators use to prevent data breaches by malicious insiders in small-scale IT government contracting agencies. The targeted population was database and system administrators of three small-scale IT government contracting agencies along the northeast region of the United States that have data security management strategies. The implication for positive social change is that by reducing data breaches, the unauthorized disclosure of consumers' sensitive information may subside, thereby preventing cases of identity theft and securing and preserving business secrets and reputation, respectively.

Role of the Researcher

The researcher was the primary data collection instrument based on the nature of qualitative research (Yin, 1981). In my primary role, as the sole researcher and primary data collection instrument in this research study, I designed and conducted the study,

collected, organized data, as well as analyzed and presented the findings in an unbiased manner. As a human, it was impossible to remove all bias; however, I did the best I can to mitigate bias during the data collection process of my study. During the data collection phase of my study, I leveraged an interview protocol (see Appendix A) and concluded the interviews once data saturation was reached. Other data collection instruments used in this study included semi structured interviews with open-ended questions either in-person or via a remote communication medium such as Skype for Business or Google Hangouts, any documentation furnished by participants, audio recordings, field notes including observations, and transcripts from the interviews. The open-ended interview questions were reviewed by my committee and peers to ensure the questions were free from bias. As suggested by Leedy and Ormrod (2015), qualitative researchers should display comprehensiveness, poise, and equality when analyzing and interpreting collected data. I ensured data collected from my participants were comprehensive, poise, and ensured equality when analyzing and interpreting research data by using the same data collection instruments across all my participants. Using the same data collection instruments ensured uniformity, equality, and would minimize bias.

Securing and working with data has always been a passion of mine; hence, I entered the database and security engineering fields. Through my profession as a database administrator with over 15 years of experience working in the field of study, ensuring only authorized personnel to have access to data is apriority. My role over the years has been that of more of database architecting, development, and operations, versus database security management; hence, I consider myself to be unbiased and proactively

sought to alleviate any form of bias to the data collected was not skewed or tainted. The selection of the topic and use of a multiple case study research design were selected based on my interest to learn more and gain a wealth of understanding about the problem. From an ethical standpoint, I ensured neither the target participants are from places I have previously worked, nor do I know the participants professionally or personally. My relationship to the geographical location of the study was that I worked in the region.

I reviewed the *Belmont Report* provided by the United States Department of Health and Human Services. While conducting research, the *Belmont Report* serves as ethical guidelines and principles for protecting research study participants (U.S. Department of Health & Human Services, 1979). As a researcher, I treated all participants ethically and with respect, and ensured risks are minimized. I have also completed the Protecting Human Research Participants training offered by the National Institutes of Health (NIH) Office of Extramural Research (Certification Number: 2275855) and have enclosed my certificate of completion (see Appendix B). I ensured that all participants were made aware that their names were kept confidential. I was sure to keep all interview interactions confidential to maintain and protect interviewees' identities and uphold confidentiality. I followed the principles outlined in the *Belmont Report*.

I avoided bias in this doctoral study by making sure I did not inject any personal values, subjectivity, and predispositions. Roulston and Shelton (2015) described bias as any distortion or manipulation of data collected that threatens the credibility of research either unintentionally or hidden from the researcher. Also, I recorded all the interviews

with the participants, transcribed the interview data collected, and performed member checking. Member checking ensured that the data collected was accurate and reflected an accurate representation of the participants and was free from bias. The integrity of the data collected was maintained, if not enhanced, by using member checking.

Additionally, I was sure to avoid bias when selecting participants by ensuring they were representative of the population. For this study, I used the GST as the conceptual framework. Per Rule and John (2015), conceptual frameworks that will help with navigating relationships between theories and case studies will be needed.

For this multiple case study, I used a maximum variation (also called heterogeneous) purposive sampling technique, and out of the population interviewed two database administrators and two system administrators from three different participant organizations either in-person or via a remote communication medium such as Skype for Business or Google Hangouts. A heterogeneous purposive sampling technique was chosen because I wanted to capture a wide range of perspectives and experiences around my research topic; therefore, gaining deeper insight and enriching my study. I followed a semistructured interview approach either in-person or via a remote communication medium such as Skype for Business or Google Hangouts and documented field notes and observations during the interviews with participants. The interview questions were aligned with the specific research topic, and I used level 2 questions. Yin (2014) suggested the use of Level 2 questions, to ensure relevance to the research topic, which are questions asked of the individual case. The open-ended type of questions allowed me to ask transitional or follow-up type questions as well. Before finalizing the data

gathered, I presented the data collected to my committee and peers for review and feedback.

Participants

For this study, participant selection will be conducted using the heterogeneous purposive sampling technique. Per Suen, Huang, and Lee (2014), heterogeneous purposive sampling involves the use of specific criteria to select elements from a population and based on the purpose of the study. From three organizations located in the northeastern region of the United States, I will pick participants for my study based on the following criteria: knowledge and experience, years of service at the target organization, and have implemented a data security management strategy. I will choose participants based on their knowledge to assist with my research study. The determination of their knowledge preference will be based on the systems they have worked with and their years of experience. Peticca-Harris, deGama, and Elias (2016) suggested a dynamic, nonlinear process of gaining access broken up into four elements: study design and planning, identifying informants, contacting informants, and interacting with informants during data collection, which is what I plan to achieve in my study.

I will contact the gatekeeper of each organization and discuss the purpose of the research and the data collection process to ensure there are no company policy violations. Next, I will communicate the research purpose, and data collection process, and then provide each gatekeeper the participant screening questionnaires to distribute to potential candidates in the solicitation process. The questionnaire will have content to gather

participant eligibility information, knowledge, experience, and use of data security management strategies. The questionnaire will contain the following:

1. What is your current role and title?
2. How many years of database administration or system administration do you currently possess?
3. How long ago have you implemented a data security management strategy?
4. How many years of experience do you have in this type of role?
5. How many years have you worked at this firm?

After identifying potential participants, I obtained the contact information of each potential participant identified. Next, based on the participant selection criteria, I selected my study participants: two database administrators and two system administrators. From each organization, two database administrators and two system administrators were selected, as a result, data saturation may be reached within each participant organization. Next, I contacted each potential participant and provided an informed consent along with an invitation to participate letter. The informed consent process informs the potential participants of voluntary participation, disclosure, and discuss confidentiality.

After choosing the participants, I worked with the gatekeepers to obtain the emails of my participants to set up interviews with each of them onsite, at a meeting space offsite, or via a remote communication medium such as Skype for Business or Google Hangouts. I worked to build trust and establish a good rapport with the gatekeepers and participants. Building trust and a good rapport was a high priority. I communicated to the participants the importance of the research and assured them their

information would remain confidential and solely for the study. I also informed the participants that the data collected would be retained for five years.

I emailed the participants and briefed them about the interview process, including the use of a recording device, and the creation of a transcript for review, estimated the duration of the interview, among others, before the interview. Prior to the interview, I enhanced the comfort level of my participants and built trust by asking each participant to sign an agreement document that would indicate their role and responsibilities within the organization.

Research Method and Design

This research study examined the lack of data security management strategies in use by database and system administrators to prevent data breaches by malicious insiders. The research method I chose for my study is the qualitative research methodology, and the research design is a multiple case study. The qualitative research method provides me with a deeper understanding of how database administrators and system administrators use data security management strategies to prevent data breaches by malicious insiders. Also, I ensured the research methodology and design I selected are in alignment with the research question for my study.

The research question influences and shapes the research method and design of the study. The type and scope of data collected, as well as the technique used for the collection of data, was also relative to the research question. Therefore, establishing a recursive relationship between research design and data collection sources. Additional themes in the study were derivative of the nature of the information collected from each

participant. At the same time, synthesizing the data collected provided a full picture of the research question. To reach the point where a deeper understanding of the research question was answerable, a methodological triangulation of the various sources of data: questionnaire, semistructured in-person interviews, and company documents, was likely, which in turn yielded emergent themes among participants. As described by Yin (2014), triangulation is the convergence of data collected from a variety of sources, to determine the consistency of a finding. Triangulation ensures that the findings of the case study have been supported by more than a sole source of evidence. Case studies typically solicit level 2 questions, which are questions asked for individual cases, as suggested by Yin (2014). Responses to such questions unraveled a better understanding of the phenomenon under exploration.

It is vital for researchers using a case study research design not to lose sight of the sequence of events due to the individual questions and answers asked of participants. In a case study, the findings of the study are based on the entire organization and not the participants. For instance, in a scenario where a case study is about an organization, interviewing individuals, and collecting data on how and why the organization works, as well as retrieving personnel policies, and organizational outcomes yield an enriched data collection set.

Method

After considering the quantitative, qualitative, and mixed-method research approaches, the research method I chose for my study is the qualitative research

methodology. As Kozleski (2017) suggested, one needs to use the qualitative method to help gather information and obtain an understanding of human behavior and perspectives. I chose a qualitative method because the intent of the study is to explore cases to gain a deeper insight into data security management strategies that database administrators and system administrators use to prevent data breaches. When there is a lack of substantive information on a phenomenon, to gain a deep and rich understanding, researchers prefer to use qualitative research (Houghton et al., 2015). Palinkas et al. (2015) stated the level of depth of information collected theoretically helps to achieve data saturation in qualitative research studies. The landscape of data security management and malicious insiders continue to change and thus presents new challenges to organizations; hence, to enhance my understanding and gather data based on experiences and knowledge of database and system administrators on data security management strategies they use to secure data from malicious insiders, I chose to conduct my study using qualitative research.

I did not choose the quantitative research approach as the intent of the study is not to understand the relationships between variables, or to validate or invalidate hypotheses. Morgan (2015) found that in studies where researchers need to examine variable relationships and test hypotheses, they use the quantitative research methodology. Yin (2014) suggested quantitative research data is quantified for statistical analysis through the evaluation of relationships between variables. Researchers use the quantitative research approach to test hypotheses and examine relationships. In my study, I do not intend to explore relationships or test hypotheses; hence, the quantitative method was not

appropriate for my research study. In a study conducted by Barnham (2015), he concluded that researchers using the quantitative research approach extrapolate meanings of research questions using the same approach for each participant as they assume their study participants will answer questions in the same manner. However, the intent of my study is to gain a deep understanding of the data collected from study participants based on their perspectives.

Even though the mixed-method approach enhances the strengths and minimizes the weaknesses of the other mono-methods, I did not choose to use mixed-method for my study because it contains elements of both qualitative and quantitative methods, which may result in resource constraints, such as time, effort, and is costly. The mixed-method research approach offers researchers a variety of benefits, including triangulation, minimizing bias, increasing validity, enhancing the strengths, and decreasing the weaknesses of the mono-methods of quantitative and qualitative methodologies. After a review of current research, McCusker and Gunaydin (2015) offered the opinion that a researcher needs to weigh the cost involved in researching to identify the most efficient method. Cost and time to complete a mixed-method research study are the reasons some researchers do not pursue a mixed-method study as researchers need to assemble and coordinate expertise across both quantitative and qualitative methodologies, as well as the associated demands to publish the research study findings (Turner, Cardinal, & Burton, 2017). Additionally, my research does not warrant a combination of qualitative and quantitative research methods. Therefore, it was not appropriate for my doctoral study. The quantitative aspect of mixed methods requires the formulation and testing of

hypotheses (Green et al., 2015). However, the intent of my study is to gain a deeper understanding of the research question using semi structured interviews with open-ended questions; therefore, I did not choose the mixed-method research approach.

Research Design

For my research study, I chose the multiple case study qualitative research design to address the research question adequately. Miller and Coutts (2018) concluded that the qualitative multiple case study research design elucidates a variety of ways to answer how and why questions. The multiple case study research design supports the exploration of a phenomenon through various evidence sources and provides a rich description of single or multiple cases within a real-life context (Cousins & Bourgeois, 2014). Multiple case study research design is an ideal approach for identifying common patterns based on historical details (Di Mauro, Fratocchi, Orzes, & Sartor, 2018). Researchers use evidence sources such as documents, observations, artifacts, and interviews in the case study research design. The purpose of semi structured interviews, as well as open-ended questions, would serve me better gain a deeper understanding of the information collected for my study. Fernández and Wagner (2016) asserted the use of a case study research design enriches the exploration of phenomena in their natural context. Case study research design reflects the personal experience of the research study participants and guarantees success in understanding a situation in great depth for a defined timeframe (Pacho, 2015). In using the multiple case study research design, interviewing of participants, organizational documentation collection, and observation, and field notes were among the crucial sources of data.

Researchers use the phenomenological approach to research people who have experienced a phenomenon and how they lived through it (Sauro, 2015). Sloan and Bowe (2015) suggested that the sample sizes of participants are small, and thus allows the researcher to become deeply involved in the data and phenomenon. Becoming deeply involved in the data is a facet of case study research designs as well; however, the sample size may not be large enough to yield the intended information to answer the research question. Researchers use phenomenological research to gain a phenomenological understanding of the perspectives and experiences of their sample population, rather than an explanation of a phenomenon from participants' experiences (Woodgate et al., 2017); therefore, a phenomenological research design will not be appropriate for my study as my intent is to explore the research question and gain a deep understanding from a larger sample population.

Hallett and Barber (2014) suggested that researchers use the ethnography research design to study a specific culture or group over a period without the use of interviews and observations, which is the intent of this study. Researchers use ethnography research design to observe and understand subjects of their research study for knowledge production, leading to political intervention or nonintervention into the lives of the study's subjects (Reed, 2016). The intent of my study was to explore the strategies used by my participants and not to intervene in their lives. After an extensive review of current research, Astuti (2017) offered the opinion that ethnography research design requires researchers to let go of the participatory experience and turn against it. The intent of my study was neither to participate in the organizations of my participants or turn against

data collected from them; therefore, the ethnography research design was not appropriate for my study.

Another qualitative research design considered was narrative. Per Singh, Corner, and Pavlovich (2015), researchers use this research design to gain the meaning of life through stories. The focus of my study was not to gain meaning of life but to explore strategies in use by my participants; hence, I chose not to use narrative research design. The narrative research design involves researchers gathering stories from participants that may not have been analyzed, and an explanation of the data collected can change (Lewis, 2015). Data analysis was a vital component of my study as the data collected underwent coding and categorization into themes to enhance my understanding of the data collected to answer the research question consistently without changing. Hossain (2017) described that narrative research designs focus on what information is disclosed, and not how it is disclosed. I intended to document how participants answer the interview questions, as well as create field notes and record the interviews; therefore, the narrative research design was not appropriate for my study.

Per participant organization, data saturation was reachable when all participants responded to specific questions with the same answer. Each participant's case is worked vigorously to obtain a deep understanding of the data security management strategies in use, no matter how long it takes (Stake, 2006). Fusch and Ness (2015) suggested that when no additional information, themes, codes are uncoverable, and the findings of the research duplicatable by other researchers, data saturation has occurred. Data saturation is inadequate when researchers use just one facet of reaching data saturation, such as the

researcher hearing it all (Morse, 2015). Instead, saturation should be determined by a multitude of factors, including data collection, and an in-depth understanding of the topic of study, among others. Harvey (2015) recommended that member-checking is usable in qualitative research methodology to verify data collection accuracy and completion from participants. Therefore, to confirm data saturation in my research study, member checking with participants was one of the characteristics I used to ensure no additional information was uncoverable.

Population and Sampling

The population of my study includes database administrators and system administrators of three small-scale government contracting IT organizations in the northeastern region of the United States. The population for the study has knowledge and experience around data security management strategies. I chose two database administrators and two system administrators from three organizations using the heterogeneous purposive sampling approach based on defined criteria.

Cati, Kethuda, and Bilgin (2016) asserted the specific criteria defined must be attainable by the sample to become a research population. Therefore, all 12 participants met the criteria of a five-year minimum work experience and knowledge of data security management strategies and worked at their organizations for a minimum of five years. Determining the sample size needed to reach data saturation for a case study is known to be a difficult determination to make (Boddy, 2016). The number of participants, the collection of data and related documents, and ensuring triangulation, are strategies to help ensure data saturation is attained for my study on small-scale organizations. The United

States Small Business Administration (SBA) describes a small-scale firm as one that has a minimum of 500 employees (SBA, 2012). The SBA considers and categorizes small businesses according to its chart of size standards, which reflects the size of small businesses ranging anywhere from 500 to 1,500 employees (SBA, 2016). Also, Fugard and Potts (2015) suggested the use of thematic analysis to analyze qualitative data collected in similar research studies prior to mine, and how the sample size affects those research studies. Considering the key points stated in the above paragraph may ensure attaining data saturation.

The site and setting of the interview may impact the quality of the interview and the data collection. I coordinated to set up interviews with each participant via the gatekeeper of each organization. As suggested by Pryce, Tweed, Hilton, and Priest (2017), I sent written and verbal information about my research study and made my participants aware their responses would be confidential, and they could withdraw at any time prior to chief academic officer (CAO) approval. I planned to interview each participant in-person or via a remote communication medium such as Skype for Business or Google Hangouts. I estimated that my interviews would take about 30 minutes to 1 hour. If it took longer, I was sure to be attentive to the participants' comfort and would take a break. Kasim and Al-Gahuri (2015) asserted building trust and maintaining good rapport with participants is key to data collection and the research study. I reminded my participants before the interview about their confidentiality and preservation of their privacy, as one of many approaches I used to build trust, comfort level, and establish a good relationship. Another approach I used for ensuring quality data was collected during

the interviews was by improving the reliability of interview instruments before using them by seeking feedback from my research committee (Richardson et al., 2017). I planned to hold the interviews in private in a conference room or a quiet enclosed office space to minimize distractions.

Ethical Research

Ethics in research is an important aspect. The need to ensure ethical behavior and activities is to protect and preserve the privacy and confidentiality of the research participants. For my qualitative research study, I conducted the research ethically and honestly to minimize harm to all my participants. By email, I provided all my participants with a form that contains information about their consent to my research study. Obtaining informed consent from my participants attempts to secure their ethical rights (Biros, 2018). Achieving consensus to proceed with my research study did not only pertain to enrolling participants, but also conveyed information about rights as human subjects to uphold, protect, and respect the rights of my participants. In addition, attaining consensus involved the communication of the research question under study, the methodology in use, as well as the benefits and harms to the participants of my study (Zhang, 2017). The consent process also informed participants of voluntary research study participation, voluntary disclosure, and discuss privacy and confidentiality of research artifacts.

I ensured to communicate in the consent form the terms and conditions for participating in the study and provided details on the option to opt-out during the initial phase of the research study. Nair and Ibrahim (2015) suggested that considerations made to ensure confidentiality of participants are essential to ensuring ethical safeguards in the

consent form. As the researcher, I protected the confidentiality of the participants in the research study.

I informed participants both verbally and in writing of the option to withdraw at any time prior to chief academic officer (CAO) approval. Although Hershey and Hession (2017) suggested that demands, discomforts, or difficulties associated with my study may influence participants to withdraw, I ensured participants were not coerced or obligated in any way to prevent them from withdrawing. Also, I did not offer any monetary incentives to participants for participating in my research study. A copy of the study results would be made available to anyone who requests a copy.

The data collected from this multiple case study would be stored securely for five years in a private safe box that would be only accessible by me. Preserving the confidentiality and privacy of my participants' data builds trust and establishes a good rapport (Hoyland, Hollund, & Olsen, 2015). I ensured I deidentified participants and their organizations; I used pseudonyms to protect their identity, as well as preserve their privacy and confidentiality (Dessi & Sebastian, 2017). I will destroy the data collected by following procedures set forth for the destruction of data obtained after five years.

Data Collection

The data collection methods I used in the study included 12 open-ended questions, semistructured in-person interviews, organizational documents, including archival records, and direct observations. In Appendix C, I discuss in more detail the direct observation protocol. Based on the policies and procedures governing a participant organization, I obtained publicly available documents through the United States

Department of Defense (DOD) Chief of Information Office and the NIST websites. As suggested by Yin (2014), the interview, as the mode of collecting research data, via verbal communication with each participant of my study, is conversational, yet guided by the research purpose. As noted by Scheibe, Reichelt, Bellmann, and Kirch (2015), the relaxed nature of the conversation fosters participants to respond to interview questions freely. A consent form was sent to each participant prior to conducting the interviews to obtain agreement from each participant. The consent form included information pertaining to the use of an audio recording device.

Instruments

I served as the primary data collection instrument as the researcher of this multiple case study. Neuman (2014) asserted the researcher is the ideal data-gathering device as the researcher can pursue emerging dimensions of a study that is beyond the scope of other instruments designed beforehand. Other data collection instruments for the research study include semistructured interviews, direct observations, documentation, and archival records analysis. Also, I made the participants aware prior to conducting the interview that I would be recording the interview.

The semistructured interviews were performed using an interview protocol, which can be found in Appendix A. Dikko (2016) suggested an interview protocol serves as rules and guidelines by which researchers go by to conduct interviews. Following an interview, protocol facilitates the interview conversations and ensure consistency by helping me to ask participants the same

questions (Castillo-Montoya, 2016). The benefit of recording the interview ensures that if the researcher forgets any keynotes, the researcher can go back to the recording to fill them in. Additional cues could also be drawn from participant gestures or tone that may contribute to the research study.

I used methodological triangulation and performed member checking with each interview participant separately. After review and agreement from the participants that the information collected is accurate and reflects their views, I imported the data collected into a software program called NVivo. As suggested by Houghton et al. (2015), this software helps researchers to break down the data collected into manageable pieces. I also informed the participants about the use of the NVivo software and storage of the data following the Walden University research data retention guidelines.

Data Collection Technique

Data collection commenced once I obtained Walden University's Institutional Review Board (IRB) approval. I conducted this study under Walden IRB approval number 11-13-18-0604496. Semistructured interview questions were used for my interviews, and interactions during the interview process were recorded using the Audacity software. Prior to the interview, I emailed the consent forms to each participant and did not follow a paper-based approach. On the day of the interview, I arrived at the participant's site or logged in to the remote software early and tested the Audacity software to verify it can capture the audio within the interview setting to ensure proper functionality and quality. I conducted interviews for each participant onsite at their respective organizations or via a remote communication medium such as Skype for

Business or Google Hangouts. After I collected data from each participant of my study, I transcribed the data.

As part of the data collection process, I took direct observational field notes. Stuckey et al. (2014) suggested that researchers use direct observations to help confirm or challenge interview data. I used the interview notes to inform the discussions during observations. If deviations were noted between the interview notes and direct observation, I asked the participant for clarification. After transcription of each interview and direct observation, I conducted member checking with each participant. Santos, Silva, and Magalhaes (2017) concluded that member checking ensures the accuracy and consistency of the transcription of the interview. The outcome of the member checking processing is the feedback obtained from participants (Liao & Hitchcock, 2018). Feedback from the member checking process enhances the quality of the interview data collected. Improving the quality of data collected from interviews through member checking enhanced the trustworthiness of my research study results.

As part of the organizational documents and archival records collection, if any, I worked with the organizational point of contact. Kasim and Al-Gahuri (2015) asserted lack of knowledge and understanding of participants could have an adverse impact on a research study. Therefore, I ensured that there a clear understanding and expectation of the need for the documents. I requested electronic copies of the data via email and analyzed each resource per participant organization entirely offsite at my home office personally.

Data Organization Techniques

After the interviews, I transcribed the audio recordings into a format that is accessible and readable, such as Microsoft Word. I aimed to complete the transcription process within a week of the final participant interview. Bannon (2015) concluded researchers should develop a solution that could help them to diagnose how serious the issue of missing data is within a specific dataset. Therefore, I ensured during the interview process that I accounted for any questions a participant was unable to answer due to nondisclosure or sensitivity reasons. Using this check, I could assess the level of impact of the missing data to my study. I performed an analysis of the data collected from each participant, and then merged the data obtained along with the existing data collected from the prior participants, and then analyzed further. I leveraged Microsoft Excel to maintain a log of my activities and to help me stay focused and organized. Any reports generated after the study would be shared with participants of each respective organization. I encrypted the removable media holding the information gathered and stored it in a secure location in my home for safekeeping. I tried my best to limit the number of hard copy artifacts. However, I labeled any hardcopy artifacts clearly and securely stored them in a similar fashion as the data saved to the encrypted, removal media. Should any of the hardcopy data be needed in electronic format, I would scan them.

Additionally, transcripts captured, member checking write-ups, and notes, as well as logs from direct observation, underwent conversion into electronic format to be included in the data analysis activities. Names of participants and organizations, as well

as other identifying information, were masked to ensure privacy and confidentiality. Gustarini, Wac, and Dey (2015) concluded that the retrieval of rich data is enhanced if data collection is anonymous. The data was then be loaded into the NVivo qualitative data analysis (QDA) software to perform thematic coding, as well as further analysis. NVivo supports researchers by reducing manual tasks and helps to discover tendencies and recognize themes (Adetoro-Adewunmi & Damilola-Ajayi, 2016). At the end of the data collection and analysis process, I will retain all data stored, both soft and hard copies, for five years before destroying them. I purged the data stored on the removable drive and shred hard copy documents. Electronic copies of organizational documents were stored on a removable storage media. The electronic data was then be imported into NVivo for thematic coding and analysis.

Data Analysis Technique

Performing an iterative and continuous analysis of the data collected improved the quality of my study in general, leading to more reliable findings to answer my research question. I used a thematic coding and analysis technique for my research study and NVivo, a qualitative data analysis (QDA) tool, to assist with this activity. Scheibe et al. (2015) suggested that such software may assist in the organization and analysis of interview data, but the success of the use of the software as a research tool depends on me, the primary research instrument. Also, the use of computer software to assist with data analysis is crucial as qualitative data analysis requires time, is extensive, and meticulous (Yakut Cayir & Saritas, 2017). According to Robins and Eisen (2017), NVivo software is essential for the successful completion of research projects involving a large

volume of data to be analyzed within an intense timeframe. Using NVivo software helped me to save time and effort, especially with the research design I have chosen.

From the thematic coding and analysis activity, themes were identified in a horizontal cross-section fashion of my participants. The thematic coding and analysis process involved identifying, analyzing, and reporting patterns I found in the data collected. Maintaining consistency in coding ensures minimization of challenges with data management, organization, and analysis (Vaughn & Turner, 2015). I created and used labels, based on a determined naming convention, to properly isolate each theme and information relating to that specific theme. As part of the analysis process, I also leveraged the chosen conceptual framework, GST, to serve as an additional viewpoint by which I analyzed the data collected for the research study.

Reliability and Validity

It is vital for qualitative research studies to possess the elements of authenticity, which is reliability and validity (Noble & Smith, 2015). Researchers ensure reliability and validity in qualitative studies using a variety of techniques, including the review of post-interview transcripts, member checking, and triangulation, among other methods and practices. Florczak (2017) asserted that if one wants to know about the meaning or gain an in-depth understanding of a certain life event or phenomenon, one will choose a qualitative approach. Researchers use the qualitative approach to help answer difficult 'what' questions, or when they need a new perspective about a phenomenon. Measuring the quality and trustworthiness of a qualitative study is achievable using four criteria: credibility, transferability, dependability, and confirmability (Morse, 2015). The

mechanisms I leveraged to establish credibility, transferability, dependability, and confirmability follow.

Dependability

The research quality of dependability refers to the extent to which a measure, procedure, or instrument produces the same results when used repeatedly (Lili-Anne & Eeva-Mari, 2015). In my study, ensuring I used the same interview instruments across all participants shows consistency. Lawrence (2015) suggested the crux of reliability in qualitative studies resides in uniformity. Yielding consistency provided stability during the aggregation and measurement of the interview results, thus ensuring reliability. Cypress (2017) asserted researchers need to be proactive and take responsibility to ensure the reliability of their research studies. Therefore, to be proactive and take responsibility to ensure reliability in my research study, I used strategies congruent with the qualitative methodology to ensure the reliability and trustworthiness of the study. These strategies included the use of interview and direct observation protocols, conducting member checking, and ensuring transparency throughout the research process, as well as providing a clear description of the data collection and analysis instruments, as well as techniques. Dependability of my research findings was confirmed after performing member checking to ensure my interpretations of the data collected were an accurate depiction of the views of my participants. Another approach I used to ensure dependability is direct observations. Field notes captured during the direct observation activities were used in conjunction with organizational documents and triangulated with the interview data.

Credibility

Credibility establishes the feasibility of the research study results from the study participants' perspective. Noble and Smith (2015) asserted that clearly and accurately reflecting the data collected, as well as accounting for bias that may have influenced research findings, ensures credibility. One area of ensuring credibility is accounting for bias that may influence my research. Nair (2018) suggested researchers need to be cognizant of areas where bias is injected, including data supplementation, theory confirmation, and model simplification. I ascertained bias was not introduced when collecting, transcribing, analyzing, and reporting the research study results.

In addition, explaining the data collection instruments and processes, as well as ensuring consistency with each participant during the entire study, helped to establish credibility. I conducted member checking after interviewing with participants to validate the accuracy of data collected. As part of the member checking process, I returned the data collected to participants to check for accuracy and resonance with their experiences (Birt, Scott, Cavers, Campbell, & Walter, 2016). Performing member checking enhanced the level of trust of the data collected, and hence, the quality of the research study results. Also, the conduction of direct observation offered an additional facet that I used for the triangulation of data I collected from the study participants. After collecting data from each participant within each organization, as well as across organizations, I ensured data saturation is reached.

Transferability

Researchers must ensure enough information has been provided for other researchers to transfer research findings to ensure transferability. Researchers must apply techniques to allow for the generalization or transferability of the results beyond the specific study (Weis & Willems, 2017). With the challenge of invalidity caused by the narrowing of the scope of the qualitative phase in mind, I ensured the methods and practices I used for conducting the research study remain intact and not tainted. Marshall and Rossman (2016) stated that the burden of demonstrating research study findings apply to another context or are transferable would be made by another researcher and not the original researcher of the study. The interview protocol, direct observation protocol (see Appendix C), other research study materials, as well as results from my study, would be retained for five years. Connelly (2016) suggested researchers support transferability in their study with a rich, detailed description of the research study context, location, and participants. Retaining the artifacts provides readiness while ensuring integrity, should there be a need for auditing or reuse of the research artifacts and data for further analysis or studies.

Confirmability

The quality of confirmability in qualitative research is the degree to which other researchers can confirm the findings of a research study (Korstjens & Moser, 2018). Confirmability ensures the research findings are strictly based on the data collected in the research study, and not made up. Abdalla, Oliveira, Azevedo, and Gonzalez (2018) emphasized the need to promote triangulation to reduce the influence and effects of the researcher. I interviewed all the participants of the study as part of my strategy to enhance

confirmability. Interviewing all participants enhanced the quality of the data collected as it included all participants' responses and organizational artifacts. Also, the data collection consisted of audio, text, and interview transcripts, thus conforming to qualitative approach requirements. I structured the interview questions in a manner that spoke to the participants and drew valid responses. Kihn and Ihantola (2015) suggested that researchers follow a systematic way of building upon prior research and drawing valid responses from their study participants. Therefore, in this qualitative research study, I sought validity by drawing valid responses from my participants; therefore, I ensured the structure of my questionnaires and interview questions spoke to my participants.

Transition and Summary

In Section 2, I described my role as the researcher of this study, participants, research method, research design, population and sampling, and the ethical research aspects of this study. Additionally, details in this section included data collection instruments, data collection techniques, data organization techniques, and data analysis. This section also included discussions on ensuring reliability and validity for this study, leading to the conclusion of this section of my study with a transition and summary section.

The next section of this study, Section 3, includes a presentation of the findings for my study, application to professional practice, and implications for social change. Further discussions offer recommendations for action and recommendations for further research. This section then concludes with discussions on reflections, and a conclusion.

Section 3: Application to Professional Practice and Implications for Change

The focus of this study was exploring data security management strategies that have been implemented by organizations to prevent data breaches by malicious insiders. In this section, I will showcase findings from data collection and data analysis, as well as describe how this study may contribute to research in the field and society. Additionally, I will address positive implications for social change. I will conclude with suggestions for future work and reflect on the study.

Overview of Study

The purpose of this qualitative, multiple case study was to explore data security strategies that database administrators and system administrators use for preventing data breaches by malicious insiders. The data for this research study came from performing semistructured interviews with database and system administrators, analyzing organizational documentation, and conducting direct observation. The section begins with a brief synopsis of why and how the study surrounding data management strategies was conducted, and I then provide a summary of the study findings.

Presentation of the Findings

At the inception of this study, I sought to address the following research question: What data security management strategies do database and system administrators use to prevent data breaches caused by malicious insiders? The results of this study may be used to help address the specific IT problem that some database and system administrators lack data security management strategies to prevent data breaches by malicious insiders in small-scale IT government contracting firms. In this section, I will present the findings

for my research study and present the four major themes that emerged after conducting the study. I used methodological triangulation to analyze the following sources of data, including semistructured interviews, direct observation of a training meeting, organizational documents, procedures related to managing and strategizing data security. I used follow-up member checking to enhance the methodological triangulation and to validate the correct representation of the data. The four major themes that emerged from data analysis were as follows: (a) enforcement of organizational security policy through training, (b) use of multifaceted identity and access management techniques, (c) use of security frameworks, and (d) use of strong technical control operations management mechanisms. These themes illustrate potential strategies that could be used to secure data from breaches by malicious insiders I small-scale government contracting organizations.

Theme 1: Enforcement of Organizational Security Policy through Training

One emergent theme from data analysis was the enforcement of organizational security policy through training. According to Mann (2008), humans are targeted because they are the weakest link in any security chain. The findings from the case studies showed that organizational personnel is the most important asset in any organization and could be the weakest link in the information security chain. The study shows that security training of personnel could help improve employee security savviness, leading to an overall enhanced security posture of an organization by minimizing the likelihood of data breaches occurring. Based on the study findings, security training could be in a generic or targeted format to ensure all employees comply with organizational policies and withhold

a certain organizational culture to maintain or enhance the security posture of that organization.

Participants from the study noted that targeted security training is based on the roles of personnel within an organization. Some targeted training sessions are facilitated by vendors of the applications they use, and others take the form of an internal subject matter expert (SME) training the other technical staff. Also, research study participants noted that targeted training is sometimes conducted onsite, and on other occasions, selected technical staff is sponsored for offsite training. For an organization to maintain a culture of security, there needs to be, at a minimum, an annual requirement for all employees to undergo some form of security training. In the case of government contracting organizations, which is the case for this study, annual security compliance training of organizational personnel is required as part of the organization strategy and required by the government agency for which work is being performed.

Table 3

Frequency of First Major Theme

Major/Minor Theme	Participant		Document		Direct Observation	
	Count	References	Count	References	Count	References
Training	8	35	3	6	1	3

Note. Theme 1, enforcement of organizational security policy through training; *n* = frequency.

Al eight interview participants from both organizations indicated the importance of having security training built into the overall organizational strategy and culture for the

implementation of a firm data security management strategy to guard against data breach by malicious insiders. The interviewees noted the importance of having a mechanism in place to measure the effectiveness of security training offered. Training employees creates awareness and educates on ways to avert techniques used by malicious insiders, such as social engineering, tailgating to access restricted areas, and shoulder surfing, among others. Company A P1 noted that "taking an annual training was an organizational strategy," and P4 from the same company added that "job-related training; Okta tool training specifically; SMEs are trained by vendors." The notes from both participants aligned with a statement by Participant 1 from Company B, who noted that "we have an annual required cybersecurity four-hour training and is mandatory, which issues a certificate to the employees" as an organizational mechanism to ensure staff is compliant with data security management protocols. Company A P4 in the direct observation training session mentioned a targeted upcoming training session for an employee: "employee A has the privilege of going to training and learning how to do this so he can take over doing this going forward." Company A P1 noted that "organizations should reach out to external resources for best practice and training." Company B P2 summarized the training needs by noting that training must be in these forms: "mandatory training; targeted training for privileged employees, and general training for all users." Company A P1, P3, and P4, as well as Company B P2, and Company B P4, all reported in their interviews, the need for organizations to train their personnel, especially privileged and technical staff, to undergo more rigorous and frequent training sessions to safeguard sensitive information from data breaches. Further, all eight interviewees

alluded to some form of annually required training to ensure compliance and educational awareness to maintain organizational security culture.

The theme of enforcement of organizational security policy through training aligns well with GST as the conceptual framework for this study because GST considers factors within a system, an organization in this sense, that can shape the outcomes, or organizational culture in this case, leading to an altered output from the system, which is a reduction in the threat of malicious insiders causing data breach. Syynimaa (2017) noted that the GST allows ICT practitioners to describe the enterprise and its components and how the components within the enterprise system are controlled to execute a change that can be managed. Caws (2015) explained how GST was and is still used to break down partitions between entities that left each busy in its own existence, and how that affects the synergy and outcome. Von Bertalanffy (1972) described how to be able to determine what changed as the outcome of a system, and there is a need to look at the system in the context of the history of the system. Reviewing the nature of a system prior to asserting factors that may influence that system provides a way to assess the cause of change and the level of impact the change had on the system.

In alignment with the GST, the type of training required to affect a security-aware employee culture is known by the principle key players who set the organizational training policy; therefore, training programs that are not relevant to the organization are not provided to employees. For instance, an IT service-based organization that does not deal with health data may not train their employees on securing data according to HIPAA

privacy laws. Therefore, the emerged theme of enforcement of organization security through training aligns with the GST.

The literature supports this theme and is pertinent to the emerged theme of my study that enforcing organizational security through training, especially mandatory training, can enhance the security posture via the improvement of the organizational culture. Company A P3 and P4, and all participants of Company B discussed the impact organizational mandated training has had on their respective organizations.

Methodological triangulation was achieved, as two of the collected organizational documents, as well as the direct observation on training, supported this theme. For example, according to the AC-2 control of the NIST Special Publication (SP) 800-53, special training is required for some types of information systems. With the adoption of this policy by organizations, technical personnel would gain knowledge of the appropriate way of handling and managing accounts that access special systems to better protect them from tampering, which could lead to a data breach. In my direct observation of a training session, I obtained insight into training sessions planned for personnel that would be administering a yet-to-be-introduced configuration management database (CMDB) that would help to manage information about enterprise-wide hardware and software assets. Also, scholarly literature coincided with the methodological triangulation to shed light on the effect of training, both general and targeted, on organizational culture that inhibits data breaches.

Revamping the security culture of an organization through security training programs could be an effective measure to minimizing the likelihood of data breach

threats, and ultimately the retention of trust between government contractors and the government agency they support. Aurigemma and Mattson (2017) asserted that employees under the DoD umbrella are required to complete a meticulously tracked mandatory information security training annually and that failure to comply with the training requirements could result in a loss of access to DoD IT systems at a minimum. The observation made by Aurigemma and Mattson in their research confirms the claim made by Korpela (2015), who discussed that security training is valid preventative controls to prevent social engineering, which is one of the mechanisms leveraged by malicious insiders to gain unauthorized access to cause a data breach. The findings of both works of literature align with participants' reports. The literature and methodological triangulation provided some validation of the impact of organization security training programs on data breach prevention in small-scale government contracting organizations.

Aligning organizational training with organizational objectives should be paramount in security training program offerings. Casey et al. (2016) suggested that employee training is not only effective to enhance knowledge, but also to maintain awareness of policy in place within an organization. One such scenario is to prevent data contamination, which is the transfer of information a higher classification to a lower one. The assertions by Casey et al. aligns with the conclusion drawn in a study by Saa, Moscoso-Zea, Costales, and Lujan-Mora (2017) on the data security challenges organizations encounter when transitioning to a cloud-based system. Saa et al. noted the need for companies to educate their staff using training programs and campaigns about

data security risks and the necessary actions to mitigate those risks to prevent sensitive corporate information from becoming compromised. The GST, therefore, explains why a system could become more secure by infusing it with a change, such as training, to change the outcome of that system, which is a reduction in the likelihood of a data breach by malicious insiders occurring.

Theme 2: Use of Multifaceted Identity and Access Management Mechanisms

The use of multifaceted identify and access management mechanisms was another theme that emerged from the data and is vital when implementing data security management strategies to prevent data breaches by malicious insiders stemming from relaxed access management mechanisms. Identity and access management mechanisms come in a variety of shapes, along with a level of complexity. According to Kennedy and Millard (2016), multifactor authentication is a more robust technique for maintaining the security of sensitive data. The effective use of multifactor authentication could be a combination of either two of three authentication mechanisms: something an employee has, something an employee knows, or something an employee is. The first form of authentication is generally in the form of physical devices such as a token, a proximity card, or key fob, among others, that an employee swipes, touches, or inserts into a physical reader to gain access to a location, a room, or a computer, among others. The second form of authentication involves something an employee knows, including a passphrase, a pin, a password, or a combination of the previously stated options. The third form, also known as biometric authentication, comprises the use of a bodily part or function, such as the veins in the palm, iris, retina, or fingerprint, among others. The

latter is usually frowned upon due to the invasiveness and the use of highly sensitive personally identifiable information, which may not be stored or transmitted properly.

The higher the effectiveness of the strategy used for identity and access management, the higher the chances of avoiding nonrepudiation, which is the term for an individual claiming they were not the actor of a specific action. Finally, the theme of the use of multifaceted identity and access management mechanisms requires the use of multiple, or multi-factor authentication techniques to be effective for decreasing the chances of successful attempts for attacks by malicious insiders, such as user impersonation, privilege escalation, and fraud.

Table 4

Frequency of Second Major Theme

Major/Minor Theme	Participant		Document		Direct Observation	
	Count	References	Count	References	Count	References
Use of multifaceted identity and access management mechanisms	8	116	3	6	1	3

Note. Theme 2, use of multifaceted identity and access management mechanisms; n = frequency.

Three of the organizational documents collected, and the direct observation on training, supported the theme of the use of multifaceted identity and access management mechanisms, therefore achieving methodological triangulation. Based on my analysis of the NIST Special Publication (SP) 800-53, an organizational document collected from

Company A, I noted that AC-2(8) control discusses trust relationships and mechanisms, which are established with appropriate authorities, such a certificate authority, or CA, to validate related authorizations and user privileges. By leveraging this type of policy, organizations are endowed with a sense of validity due to the endorsement provided by a trusted third party, thus, providing a form of checks and balances in the user account provisioning process. It then becomes more challenging for a malicious insider to create a token or access card on their own. Ensuring users are authenticated through a single source was an in-depth topic during the direct observation training session. Scholarly literature also coincided with the methodological triangulation to enhance the finding that the use of multifaceted identity and access management mechanisms may be a data security management strategy to prevent data breaches by malicious insiders.

All eight participants from both participant organizations indicated that the use of multi-factor authentication and a variety of access management mechanisms, including the use of roles, auditing, and strict access controls, are important strategies to discourage malicious insider activity that could lead to a data breach. For instance, the use of a multifaceted approach means the malicious insider will need to be sophisticated enough to circumvent all the controls in place to reach the system containing the target data. For instance, a malicious insider may attempt to escalate their privilege to access a system outside of their role; however, with additional controls in place such as an access control list or firewall could prevent or slow down the malicious insider. As part of effective data security management strategies, the eight interviewees indicated that a layered approach, including password management and enforcement, and privileged user access

management, reduces the probability of a malicious insider successfully carrying out a data breach. Company A P1 discussed encryption of authentication tokens to systems, and ensuring passwords are set to expire so that they can be updated regularly.

In some cases, in addition to role-based security, profile base security at the application level is implemented to add another layer of protection is added. Company A P3 noted that roles and extra built-in mechanisms "restricts access based on what kind of role the user plays in the organization, depending on that we have profile settings, and we only give a user those privileges, and only those resources will be seen by them." As a layered strategy, the administrative techniques of this strategy cannot be overlooked. Company A P3 again stated that:

> any requests need to be approved as far as access requests go. Anytime access is required, a ticket is created, and the ticket goes through several approval layers, and depending on the approvals on the business side, IT side, and manager of the requester, then the ticket comes back to us, and we validate, and then after that we provide access.

Having an audit trail of account provisioning can assist with making account management audits easier, which is another essential activity some organizations conduct regularly to ensure account provisioning is done according to organizational policy. Company A P4 noted further that the need to use department-based access management is key especially in cases where specific groups of users need to access systems containing sensitive data.

From Company B, P1, P2, P3, and P4 indicated that measures are in place for varying levels of access to the corporate network, such as the use of virtual private networks for encrypted connections, and jumps as an added layer of identity and access management mechanisms that an organization can leverage as part of their data security management strategy. Company B P1 added that "there's no way you can access our system using another laptop, except using the government-provided laptops," which provides an added layer of security. Company B P3 confirmed that there are security measures in place to prevent unauthorized access, role-based access, such as firewall rules, and account lockout policies to prevent brute-force attacks: "if somebody tries to randomly access or try to guess a log in and try to tamper, we will lock the account on the third attempt, so the account is not accessible after that." The basis of identity and access management is the use of known information of users of the system to authenticate and authorize their access to the system. Each users' information and allowable method of authentication are known. For instance, users cannot connect to the organizational network or system using personal computers.

The type of identity and access management mechanism implemented to ensure authentication, authorization, and accountability may vary from one system to the next. A system containing sensitive information may have a stronger identity and access management strategy compared to a less sensitive system. The varying levels of strength of identity and access management mechanism per system are known by the key players of the organization who established the use of such controls; as a result, mechanisms that may not be relevant or effective in securing a target system may not be implemented. For

instance, a system classified as top secret may require biometric authentication in addition to the use of a token, whereas a system classified as confidential may only require the use of a token. The GST, therefore, explains why a system could become more secure by introducing varying levels in strength of identity and access management mechanisms to alter the outcome of that system by reducing the likelihood of a data breach by malicious insiders occurring.

The literature supports the theme of the use of multifaceted identity and access management mechanisms. Rao and Selvamani (2015) asserted that fine-grained access control mechanisms, such as using of credential or attributed based policies, may better secure access and data processing. The assertion made by Rao and Selvamani links my research study's findings back to the concept of function, structure, and process, which portray the GST as the conceptual framework for this study. The function of gaining access to a system within a specific structure follows an implemented process that can permit or reject a user's access to data. The output of such activities within a system is the ability to strengthen the target system's security, as well as providing the capability to monitor user access activity. Chang and Ramachandran (2016) asserted that the use of identity and access management strategies promotes user security and monitoring.

The literature also strengthens the finding that links the use of multifaceted identity and access management mechanisms to data security management strategies that may be used by organizations to prevent data breaches by malicious insiders. Wang, Pei, and Zhang (2019) found that identity management becomes a key problem in a system when design defects persist, as direct risks of a data breach will be incurred. Identity and

access management is the first technical layer of defense users, both privileged and nonprivileged, go through to access a system. All eight interviewees indicated support for effective identity and access management controls by noting that identity and access management is a key organizational security control to minimize malicious insider threats, which may lead to data breaches. Pol (2019) also asserted that the deployment of identity and access management mechanisms are essential controls that enable an organization to detect or prevent data breaches resulting from unauthorized access to systems. From the literature, there is an alignment with the finding that the use of multifaceted identity and access management mechanisms are data security management strategies that may help organizations prevent data breaches caused by malicious insiders.

Theme 3: Use of Security Frameworks Specific to Organizational Needs

The need to use security frameworks specific to organizational needs was another theme that emerged during data analysis. Organizations must comply with the overarching governmental mandates and regulations set forth by their regulating and other governing bodies. From my analysis of both case study organizational interviews and documentation collected, I noted that data security management strategies must align with the policies that result from the rules and regulations that govern a specific organization. For instance, Company A falls under the department of defense space and complies with the Federal Information Security Management Act (FISMA) and NIST requirements. These are frameworks that help to protect data, operational information, and assets against threats, including data breaches caused by malicious insiders. Based on the analysis of findings, there is a need for ongoing compliance with the regulations

governing an organization. Over time, the frameworks change, and new controls are added. When that happens, a review of the existing practices is performed, and policies are updated to conform to the updated security framework. Organizations, therefore, must repeatedly review and assess how they are complying with regulations and guidelines set forth by external stakeholders, to remain compliant.

Table 5

Frequency of Third Major Theme

Major/Minor Theme	Participant		Document		Direct Observation	
	Count	References	Count	References	Count	References
Use of security frameworks specific to organizational needs	5	28	5	253	1	4

Note. Theme 3, use of security frameworks specific to organizational needs; n = frequency.

Both participant organizations indicated that the use of some form of an industry-specific security framework that fits organizational needs is key to employing data security management strategies to prevent data breaches. For instance, the NIST framework requires organizations to establish insider threat programs, which is a mechanism that could be used to train organizational personnel on how to detect and report suspicious insider activity. An organizational culture that is well-equipped with insider threat management programs may stand a greater chance of preventing data

breaches by malicious insiders. Company B P1 noted that complying with organization security policy allows the organization to remain in compliance at the federal government level. Company A P1 stated that "anything we have implemented is based on FISMA compliance guidelines," and noted the need to seek external assistance: "our management should make this kind of decision to seek help from outside consultants to make sure and are following FISMA compliance." In response to the interview question of what programs are used to ensure that users or staff are compliant with data security management protocols, Company A P2 stated that they use security compliance templates that are built on STIGs. The information provided by the interviewees underscores the cruciality of ensuring the most recent and updated versions of security framework policies and regulations are followed.

The data collected from both organizations also shows that security frameworks do not always have to be technical to be effective but can also be administrative in nature. For instance, Company A P4 stated that:

> policy is just probably the biggest tool we are using in the ways of security awareness training, where they take that annually, just so they're aware of phishing and what they shouldn't be clicking on, and what they shouldn't be transmitting, and then policy to back that up in the event that somebody actually does do that.

A malicious insider with easy access to an organization's email system could easily obtain email addresses of employees and easily distribute an insecure link to other users on the network who may click on the link to collect sensitive data. On the technical side,

one measure to ensure that new systems or changes to existing ones do no introduce vulnerabilities into the enterprise which could be taken advantage of by malicious insiders was noted by Company A P4:

> we'll have our security team use their security tool to scan it for compliance against the CIS benchmark, and we have a threshold of, maybe it has to meet a 90% of the CIS benchmark, just because it will flag everything as negative and that will be detrimental to the organization from locking it down too much.

The note from Company B P4 indicates the need for organizations to ensure that security controls put in place are not overbearing, leading to low productivity levels of personnel. Company A P2reflects evidence of this approach by stating that "there are NIST and FISMA guidelines, among others that do assist with coming up with the security policies and guidelines from the enterprise level, and database in particular." The theme of using security frameworks specific to organizational needs that emerged from the data collected confirms the necessity for organizations to include the use of security frameworks as part of their data security management strategy.

The organizational documents that were collected for data analysis supported the importance for an organization to follow an industry-specific security framework, and the necessity to comply with the policies and regulations set forth for that organization. The need to validate the specific framework is applicable and effective is another essential aspect of this theme. Company B P2 asserted that "the guideline should be double-checked; there should be a system in place to make sure whatever security policy you have put in place is working." The wealth of data collected and the findings from

interviews, member checking, direct observation, and document analysis led to methodological triangulation for the theme of the use of security frameworks specific to organizational needs.

The literature supports the theme of using security frameworks that are specific to organizational needs as a data security management strategy to prevent data breaches by malicious insiders. Chang and Ramachandran (2016) noted in their work on cloud computing adoption frameworks that a multilayered framework provides more fine-grained defense countermeasures to better protect an organization and its assets. Moreover, recent literature supports further the theme of using security frameworks specific to organizational needs. Anisetti, Ardagna, Damiani, and Gaudenzi (2017) noted that it is equally critical for organizations to measure the effectiveness of the security framework in use by conducting audits on the systems on which the security framework is applied. Pacheco, Tunc, and Hariri (2018) in their study of security frameworks for the Internet of Things (IoT) stated the need for frameworks to be trustworthy, secure, as well as meet security needs at every layer of a system, instead of in an ad-hoc and afterthought manner. Based on the findings of this study and literature, the data support the need for organizations to have a comprehensive, yet relevant, security framework implemented as an integral aspect of their data security management strategy.

The theme of use of security frameworks specific to organizational needs aligns well with GST as the conceptual framework for this study because GST considers elements within a system, a company in this case, that can influence the outcomes, a more robust system due to an enhanced data security management strategy, leading to an

altered output from the system, a reduced likelihood of data breaches caused by malicious insiders. Based on a study conducted by Iwu, Kapondoro, Twum-Darko, and Lose (2016), the GST is a good lens to use for the study of the relationships between components in a system, to measure outcomes based on criteria or input.

A data security management strategy must be comprehensive to identify and include the various components that work together in a system. The relationships established, facilitate easy identification of strengths and weaknesses within the system, allowing reinforcements to be made. For instance, a weakness in a logical security control that manages user authentication to a server can be identified and remediated by supplementing with the implementation of physical control of the use of a secured server room that is not accessible remotely. The goal of implementing a security framework is to ensure the certainty of the end goal, which is a more secure system. Additionally, tracking the effectiveness of the security framework implemented is a vital activity that is performed to ascertain that the security controls are working. Therefore, the theme of the use of security frameworks specific to organizational needs aligns with the GST, whereby a specific outcome is required based on inputs to a system.

Theme 4: Use of Strong Technical Operations Management Mechanisms

The final theme to emerge from data collection and analysis was the use of strong technical operations management mechanisms. The theme of the use of strong technical operations management mechanisms encompasses establishing system baselines, applying data encryption, following industry best practices around backup strategies, and

security auditing. Baselines are used for comparing the original or ‘gold’ state of a system to the end state of that same system after changes are performed.

Cases, where benchmarks are used, include capturing network traffic patterns over a specific period, provisioning a server with a ‘previously hardened’ configuration template, and establishing the original code base for an application in a code repository. Baselines aid in the assessment of deltas between the original and end states of a system (Edgar et al., 2004). After identifying the changes between the old and new states of a system, anomalies can then be flagged for review.

Encryption is an effective technique to ensure confidentiality and integrity in systems. Encryption techniques can be used to protect data that is stored within systems, as well as when data is transferred or moved from one system to another, also known as point-to-point encryption. The type of data determines the type and strength of the encryption technique that is considered. The purpose of encrypting data while at rest and in-motion is to prevent unauthorized access and preserve the principle of need-to-know.

One of the most effective strategies for data loss is backup restores, keeping in mind the recovery point and time objectives of an organization. Backup strategies must be a functional and frequently reviewed activity in an organization. Backups can be full or incremental, including transactional and differential backups, or a combination of the options mentioned, depending on the needs of the organization. Conducting backup recovery exercises to guarantee the effectiveness of the backup strategy in use is a crucial activity.

Another strategy to prevent data loss is the use of data loss prevention (DLP) solutions on employee workstations. Email and file transmissions are monitored to detect egress of data that violate organizational policy, leading to the prevention of data breach attempts by malicious insiders. Additionally, DLP tools may also be configured to minimize phishing attempts to exfiltrate data through filtering controls to ensure PII data is not being sent outside the organization. Preventing the use of external and thumb drives by disabling universal serial bus (USB) ports is another data loss prevention technique. Locking down USB ports prevents database and system administrators from transferring data without going through the appropriate data transfer channels. In cases where flash drives are required to transfer large amounts of data, approvals for exceptions are obtained and specially encrypted drives are provisioned to database and system administrators. After usage, the flash drive is then wiped and made ready for future use.

Conducting security auditing provides system custodians a way to monitor events, review logs, and identify any threats that could impact the confidentiality, integrity, and availability of the system entrusted to them. Security auditing can be either proactive, in the sense of administrators conducting regular reviews of the system to detect unauthorized actions and anomalies, or reactive, for example, when investigative activities are conducted to detect the root cause of an incident. Although contingency planning and incidence response planning do not prevent data breaches, they go together with back up strategies that an organization may choose to leverage. Contingency plans help organizations minimize or prevent a disruption in operations while pursuing a response to an incident. For instance, should there be a data breach that causes loss of

data, the organization can failover their operations to an alternate site by activating their contingency plan, while leaving the state of the current system in a contained state while incidence response and investigative activities are performed.

Table 6

Frequency of Fourth Major Theme

Major/Minor Theme	Participant		Document		Direct Observation	
	Count	References	Count	References	Count	References
Use of security frameworks specific to organizational needs	8	188	5	185	1	17

Note. Theme 4, use of strong technical operations management mechanisms; n = frequency.

All eight study participants from both organizations revealed the importance of using strong technical operations management mechanisms as data security management strategies to prevent data breaches. Participant 2 from the same organization also noted that database backups are encrypted and cannot be restored without knowledge of the password used for encryption. About backup strategies, Participant 2 from Organization A said that:

> if we find out that data is corrupted, hopefully, we have a backup of that data on the disc, and the system administrators side of it, in the use of VMware, hopefully, they do have...I know it is very advanced now, where they can check

> block-by-block snapshots, so we can restore up to the point-in-time, which was detected that data was corrupted, so we don't really lose much data.

Participant 1 from Organization B also stated that "we have daily backups that we take, and we also have data gaps, which is a live backup set – which is replications." Additionally, Participant 3 from the same organization stated that "there is always a site at a certain location where we have a backup system where we get replication through the current system up to the minute." Uninterruptable Power Supply (UPS) is another form of backup strategy which can help to prevent data loss should there be a power outage.

Finally, on the subject matter of auditing, Participant 2 from Organization A remarked that auditing is performed as part of their baselines review activities. Participant 3 from Organization B also stated that "we rely on the sysadmin team to get the process ID and session information and look into the audit file to see what the login or database account was used to get into the system." Participant 4 from Organization B mentioned a dedicated IT audit department assists with unauthorized access and intrusion detection. Additionally, two often overlooked areas of auditing are data transfer and destruction. Participant 1 from Organization B stated that printing activities of users are tracked, including who printed, what they printed, and which printer was used. Dumpster diving is a threat vector to these two phases of the lifecycle of data. Malicious insiders do not use shredders dedicated for destroying printouts or extracts that contain sensitive information, but rather throw the printouts away, only to retrieve them later.

Furthermore, data salvaging by malicious insiders from the hard drives of decommissioned servers poses a threat to organizational data security safeguards. For

instance, a hard drive containing trade secrets could be sold at a lucrative price to a competitor organization, which could gain a competitive advantage over the victimized organization. Therefore, tracking data transfers and destruction is a critical component of a holistic data security management strategy.

The importance of this theme was highlighted after conducting an analysis of four organizational documents and allowing for methodological triangulation. The AC-2(4) control of the NIST SP 800-53 (Rev. 4) document notes the need to automatically audit information systems for account creation, modification, enabling, disabling, and removal actions, and notifying the appropriate personnel of the actions that were performed on the system. A document titled CIS Windows Benchmark discusses over 80 references of use of strong technical operations management mechanisms, including auditing rights assignments and security policy changes on a system, account management events, ensuring entire system backups are performed, and encrypting system drives using a tool called BitLocker. Another organizational document referred to the use of backup power supplies as part of the contingency strategy, the use of an independent third party for system auditing, as well as performing annual in-house auditing.

The literature aligns with the findings from the theme of using strong technical operations management mechanisms. Forde (2017) asserted the need for businesses to encrypt their sensitive data to avoid the possible loss clients and the expenses associated with reporting breaches. Jingguo et al. (2015) noted that a strong mitigation technique against threats to data and services availability is the use of real-time backup images stored offsite. In the event where organizations use cloud service providers for storage

needs, relying on a third-party auditor to conduct compliance to service level agreements, monitoring feedback for service utilization, and the possibility of any potential insider threats or attacks, demonstrate efficiency and effectiveness when auditing all key stakeholders (Razaque & Rizvi, 2016). Concerning contingency plans, Caruso (2003) stated that contracting organizations must include contingency responses to disasters and security controls, for both vendors, and on the organization outsourcing its IT.

More recent literature additionally supports the theme of the use of strong technical operations management mechanisms and aligns with the findings. Deprecated performance is a known effect of encryption. Despite the performance risk, Chen, Hu, and Li (2019) assert that data encryption has become an indispensable step in protecting privacy. The use of symmetric encryption can help alleviate the performance issues often noticed with the implementation of data encryption on large data sets. Zhang and Li (2017) noted that not only should backups be created by anyone in the organization, but also backup strategy techniques must include authentication based on digital certificates, role-based access to backups, baked-in process and auditing, detection of legitimate backup storage and restore target. This approach discussed in conjunction with other data breach detection techniques may be effective in minimizing the likelihood of data breaches caused by malicious insiders. On the subject-matter of contingency plans and incidence response, Padilla and Freire (2019) assert that not only do companies have to have such strategies in place as part of their organizational policy, but also to prevent economic damages from attacks. Economic damages may include lawsuits, costs incurred from switching systems from production to the contingency site, and reverting to

production after remediation activity is completed. The objective of conducting security audits is not only to improve an organization's risk management process but, more importantly, to hold the responsibility of legal compliance (Satoh & Samejima, 2017). Auditing provides organizations insight into the effectiveness of organizational policy and processes so that adjustments can be made, should they be proactive or reactive.

The theme of using strong technical operations management mechanisms aligns well with the GST as the conceptual framework because GST explains the effect on the relationships between elements that constitute a system. In this case, using the GST as the lens for this study shows the result of the data security management technique of leveraging strong technical operations management mechanisms in an organization, to prevent a negative outcome, a data breach. Von Bertalanffy (1972) discussed how the interdependence of objects working together could yield some result rather than the objects working in isolation. The interview participants indicated a variety of techniques are necessary to ensure defense-in-depth to better protect data from malicious insiders. In contrast, although the grey systems theory, a contradicting theory to the GST, can be useful in evaluating relationships, the theory focuses on uncertain components and outcomes of the subject system (Li, 2016). The goal of participant organizations of the study leveraging a mixture of data security management strategies is to ensure exploitable threats within the system that could be exfiltrated by malicious insiders to cause data breaches are mitigated. Therefore, the grey systems theory contradicts the emerged theme of the use of strong technical operations management mechanisms to prevent data breaches.

Applications to Professional Practice

The issue that formed the basis of this study is the perceived lack of strategies used by database and system administrators in small-scale government contracting organizations to prevent data breaches caused by malicious insiders. The application of data security management strategies by organizations contributes to the prevention of unwanted and unexpected expenses that could be incurred from data breaches (Padilla & Freire, 2019). The findings in the study resulted in some key themes that other organizations can use as part of their strategies to enhance their data security management strategies to prevent data breaches carried out by malicious insiders. There were various thoughts on the data security management strategies, implying that there are several strategies in use in the IT field, where the implementation of those strategies depends on the needs, and regulations that govern an organization. Most of the participants noted that they relied on training, security frameworks, and technical strategies tailored to their role and organization instead of a generic strategy. After analyzing the collected data, I identified four themes: enforcement of organizational security policy through training, use of multifaceted identity and access management techniques, use of security frameworks, and use of strong technical control operations management mechanisms. Organizations and IT practitioners in their role of protecting data from malicious insiders can use the results of this study.

Organizations that store data which, when breached, can cause grave damage either to their customers, the organization itself, or nation, can use these results to establish or enhance their organizational policies and strategies they use to secure their

data. Moreover, the findings of this study may be valuable in professional practice by helping database administrators and system administrators to expand their knowledge and understanding of the complex nature of insider threat and how it relates to data breaches. An effective data security management strategy can improve the security posture and culture of an organization, such as the overarching data security management policies in place, leading to a more robust framework to promote data confidentiality, integrity, and availability.

Implications for Social Change

The findings of this study add to the existing body of knowledge and literature by contributing information and knowledge on data security management strategies for preventing data breaches by malicious insiders. This study's findings may also influence positive social change by bringing focus and awareness to the management of sensitive data and protecting access to data from malicious insiders. The data from the study emphasizes the conclusions drawn reflected in the emerged themes to be beneficial for the implementation of data security management strategies.

The value this study brings to society is that it shows how organizations can implement strategies to secure their data to ensure confidentiality, integrity, and availability, and ultimately prevent the damages that can be caused by data breaches. The study's findings show that many of the participants agree on a variety of strategies, to include organizational policy enforcement through training, the use pf multifaceted identity and access management techniques, the use of security frameworks geared toward organizational needs, and use of strong technical operations management

mechanisms. The growing need to secure sensitive data has influenced a variety of solutions to be implemented based on implementations known to be successful in preventing data breaches across the IT industry.

Beneficiaries of effective data security management strategies include customers, employees, the government contracting organization, organizational partners, vendors of the systems in use by the government contracting agency, and the government agencies for which the contracting organization performs work. The highest effect of damage is felt by the citizen whose information may become compromised in a data breach. Identity theft resolution could sometimes take years, and in some cases, the harm caused to the individual may be irreversible.

In cases where malicious insiders disclose national secrets to foreign adversaries, reveal trade secrets to competitors, or leak classified information to citizens without a need-to-know, the relationship between the organization and its clients or partners becomes tarnished, and international relations and partnerships suffer. A more secure system builds trust between organizations and their clients, as well as vendors and business partners. The benefit of such a relationship could result in increased profitability for an organization and foster better international relations with allies.

Finally, an organization with effective data security management strategies builds trust, reliability, and confidence with the agency work is being performed, resulting in a win-win scenario. Trust, reliability, and confidence could lead to additional contracts being awarded, and in the long run, a profitable outcome for the organization. Moreover,

citizen information is better secured from threats that may be imposed by malicious insiders.

Recommendations for Action

The employees of an organization are the first line of defense for securing data, which is one of the most valuable assets of an organization. More so, privileged employees, including database administrators and system administrators, are entrusted as the custodians of organizational data, therefore, have direct access to data with no restrictions based on their role and clearance level. The nature of the type of access given to users, including database and system administrators, creates a risk for an organization if these trusted insiders become malicious. To mitigate or reduce the likelihood of the threat of malicious insiders, a layered-security approach is key to provide in-depth safeguards against data breaches.

As suggested by the participants of this study, organizations should ensure users are trained as a strategy to enforce organizational policy, use a multifaceted approach for identity and access management, ensure that the security frameworks being used fit organizational needs, and use strong technical operations management techniques. The suggested strategies ensure that a holistic solution is implemented to protect data in all phases of its lifecycle, from creation, through use, and transfer, to destruction. Findings from this study are important to data custodians, information system owners, and organizational data security policymakers.

The two case study organizations and contacts will receive copies of the results of this study through email so it may be propagated to data security management matter

experts who could share the findings with personnel within their purview and sphere of influence, as well as others in the broader scope of ensuring data security within their organizations. My immediate goal is that this final study will be published and made available for public searches when companies are in search of data security management strategies to prevent data breaches. As a long-term goal, I intend to share, wherever possible, the results using appropriate and effective platforms, including my place of work, conferences, training seminars, and data security management stakeholders in the broader research community.

Recommendations for Further Study

Malicious insiders continue to pose a threat to the organization, and sometimes the impact from data breaches can be grievous, and the damage irreversible. Insider attacks are motivated by several reasons and carried out several forms, especially when it comes to data destruction. Some organizations participate in programs where old servers are given away to charity organizations within the country or abroad. When proper techniques are not used to destroy remnants of data left on hard drives after decommissioning, a malicious insider could take advantage of this loophole due to inside knowledge. Therefore, the proper strategies in use for data destruction at the end of the data lifecycle should be investigated further to assist in determining the views held by database administrators and system administrators in this regard. Also, the results of the study depend significantly on the experiences of the participants, as well as the sample size of the study. I recommend that researchers interview large-scale government contracting organizations, or simply, private organizations, to cover participant

experiences in those types of settings. To further shed light on data security management strategies in use by database administrators and system administrators to prevent data breaches by malicious insiders, researchers may consider a study into the factors that motivate malicious insiders to perpetrate data breaches.

Reflections

A statement made by one of the participants struck a chord with me. The participant asserted that what a user does with depends on what that user has been trained for, and I would like to add that it also depends on the motives of the user. As the researcher, I was the main instrument for data collection and analysis. The research process was an eye-opening experience for me as I had the opportunity to learn about strategies the participants of my study use to prevent data breaches. There is a great deal of potential for organizations to utilize their data security management strategies across the data life cycle. As a researcher, having worked with databases in my career, it was interesting to learn about the perspectives of other professionals who ensure data does not reach the wrong hands. As such, I took necessary precautions to minimize personal bias by avoiding injecting any personal values, subjective views, and inclinations. I strived to learn throughout the research activities, including recruiting participants, member checking, direct observation, and the data collected as part of this study. I ensured the credibility of the study and immersed myself in looking at things from a variety of perspectives. An example of this is that organizational policy changes are not only influenced by regulations mandated by governing bodies in a top-to-bottom fashion, but

also the activities of a hacker, and malicious insider activities, following a bottom-up approach.

Summary and Study Conclusions

In my endeavors to explore strategies in use by database administrators and system administrators to prevent data breaches by malicious insiders, I discovered the complex nature of insider threat, and on a good note, strategies that can be used to reduce the likelihood of data breaches by malicious insiders. The motivations of malicious insiders continue to influence the perpetration of data breaches. Enhancing the organizational security culture to a level where employees are trained to identify symptoms of a potential insider threat, a policy on how to handle such a threat, and when to report such threats can assist in stopping or minimizing the occurrence of data breaches. Managing insider threats should be baked into the policy of an organization to create a heightened awareness. Implementation of such a policy, in conjunction with the themes identified from the data collected for this study, could provide an organization with an arsenal of counter insider threat measures. The use of methodological triangulation ensured the themes and findings of this study across a range of data sources to be validated. The interview participants involved in this study have had success in preventing data breaches from the implementation of the data security management strategies they use at their respective organizations. Having identified the emerged themes between the two participant organizations, the study's findings could have a significant influence and impact on the data security management strategies in use by other organizations in the government contracting sector. The findings and conclusion of

the study may contribute to social change because the strategies identified can be implemented across the entire organization, to protect sensitive data better, and prevent data breaches that could negatively impact customers, citizens of a nation, the organization itself, partners, vendors, and the nation at large.

References

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulation as a methodological alternative. *Administração: Ensino e Pesquisa, 19*(1), 66–98. doi:10.13058/raep.2018.v19n1.578

Adetoro-Adewunmi, Y., & Damilola-Ajayi, O. (2016). Attitudes of Nigerian facilities management professionals to the benefits of benchmarking. *Facilities, 34*(7/8), 468–492. doi:10.1108/f-06-2014-0057

Agrafiotis, I., Erola, A., Goldsmith, M., & Creese, S. (2016). A tripwire grammar for insider threat detection. *In Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats* (MIST '16), 105-108. doi:10.1145/2995959.2995971

Ajzen, I. (2004). Theory of planned behavior. *Encyclopedia of Health and Behavior*. doi:10.4135/9781412952576.n208

Alhadeff-Jones, M. (2008). Three generations of complexity theories: Nuances and ambiguities. *Educational Philosophy & Theory*, *40*(1), 66-82. doi:10.1111/j.1469-5812.2007.00411.x

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567-575. doi:10.1016/j.chb.2015.03.054

Ali, O., & Ouda, A. (2016). A classification module in data masking framework for business intelligence platform in healthcare. *2016 IEEE 7th Annual Information*

Technology, Electronics, and Mobile Communication Conference (IEMCON). doi:10.1109/iemcon.2016.7746327

Alihodzic, A., Tuba, E., & Tuba, M. (2017). An upgraded bat algorithm for tuning extreme learning machines for data classification. *Proceedings of the Genetic and Evolutionary Computation Conference Companion (GECCO '17)*. doi:10.1145/3067695.3076088

Allen, M. (2017). *The sage encyclopedia of communication research methods* (Vols. 1-4). Thousand Oaks, CA: Sage Publications

Andersson, J., & Caporuscio, M. (2016). Aligning architectures for sustainability. *Proceedings of the 10th European Conference on Software Architecture Workshops - ECSAW '16*. doi:10.1145/2993412.3004849

Anisetti, M., Ardagna, C. A., Damiani, E., & Gaudenzi, F. (2017). A security benchmark for OpenStack. *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*. doi:10.1109/cloud.2017.45

Astuti, R. (2017). On keeping up the tension between fieldwork and ethnography. *HAU: Journal of Ethnographic Theory, 7*(1), 9–14. doi:10.14318/hau7.1.003

Atkinson, C. (2016). Review of security in cyberspace: Targeting nations, infrastructures, individuals. *Crime, Media, Culture, 12*(1), 117-119. doi:10.1177/1741659015618797

Atkinson, P. (2017). *Thinking ethnographically.* 55 City Road, London: Sage Publications.

Aurigemma, S., & Mattson, T. (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security, 25*(4), 421. doi:10.1108/ICS-11-2016-0089

Bakar, N. A., & Selamat, A. (2016). Detection of data confidentiality violations using runtime verification and quality assessment. *2016 2nd International Symposium on Agent, Multi-Agent Systems, and Robotics (ISAMSR)*. doi:10.1109/isamsr.2016.7809997

Bannon, W. (2015). Missing data within a quantitative research study: How to assess it, treat it, and why you should care. *Journal of the American Association of Nurse Practitioners*, 27, 230-232. doi:10.1002/2327-6924.12208

Barnham, C. (2015). Quantitative and qualitative research. *International Journal of Market Research*, *57*(6), 837-854. doi:10.2501/IJMR-2015-070

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, 68, 145-159. doi:10.1016/j.cose.2017.04.009

Biros, M. (2018). Capacity, vulnerability, and informed consent for research. *Journal of Law, Medicine & Ethics, 46*(1), 72-78. doi:10.1177/1073110518766021

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research, 26*(13), 1802-1811. doi:10.1177/1049732316654870

Blasco, J., Tapiador, J. E., Peris-Lopez, P., & Suarez-Tangil, G. (2015). Hindering data theft with encrypted data trees. *Journal of Systems & Software*, 101, 147-158. doi:10.1016/j.jss.2014.11.050

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal*, 19, 426-432. doi:10.1108/QMR-06-2016-0053

Bölte, S. (2014). The power of words: Is qualitative research as important as quantitative research in the study of autism? *Autism, 18*(2), 67-68. doi:10.1177/1362361313517367

Bridgen, S. (2017). Using systems theory to understand the identity of academic advising: A case study. *NACADA Journal, 37*(2), 9-20. doi:10.12930/NACADA-15-038

Burns, A., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 190. doi:10.1016/j.chb.2016.11.018

Buthelezi, M. P., Van Der Poll, J. A., & Ochola, E. O. (2016). Ambiguity as a barrier to information security policy compliance: A content analysis. *2016 International Conference on Computational Science and Computational Intelligence (CSCI),* 1360. doi:10.1109/CSCI.2016.0254

Carson, D., Gilmore, A., Perry, C., & Gronhaug, K. (2001). *Qualitative marketing research.* London, England: Sage Publications

Caruso, V. L. (2003). Outsourcing information technology and the insider threat (No. AFIT/GIR/ENG/03-01). *Air Force Institute of Tech Wright-Patterson AFB OH School of Engineering and Management.* Retrieved from https://pdfs.semanticscholar.org/27d4/4bb821c336538b9e2c0f19812611e7adb13e.pdf

Casey, W., Morales, J., Wright, E., Zhu, Q., & Mishra, B. (2016). Compliance signaling games: Toward modeling the deterrence of insider threats. *Computational & Mathematical Organization Theory, 22*(3), 318-349. doi:10.1007/s10588-016-9221-5

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative Report, 21*(5), 811–831. Retrieved from http://nsuworks.nova.edu/tqr/

Cates, S. (2015). Feature: The evolution of security intelligence. *Network Security*, 2015, 8-10. doi:10.1016/S1353-4858(15)30017-9

Cati, K., Kethuda, O., & Bilgin, Y. (2016). Positioning strategies of universities: An investigation on universities in Istanbul. *Education & Science / Egitim Ve Bilim, 41*(185), 219. doi:10.15390/EB.2016.2723

Caws, P. (2015). General systems theory: It's past and potential. *Systems Research and Behavioral Science, 32*(5), 514–521. doi:10.1002/sres.2353

Ceric, A. (2015). Bringing together evaluation and management of ICT Value: A systems theory approach. *Electronic Journal of Information Systems Evaluation, 18*(1), 19-35. Retrieved from http://www.ejise.com/issue/download.html?idArticle=946

Chae, Y., Katenka, N., & Dipippo, L. (2016). Adaptive threshold selection for trust-based detection systems. *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*. doi:10.1109/icdmw.2016.0047

Chang, V., & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing, 9*(1), 138–151. doi:10.1109/tsc.2015.2491281

Chen, S., Hu, W., & Li, Z. (2019). High-performance data encryption with AES implementation on FPGA. *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (Big Data Security), IEEE Intl Conference on High Performance and Smart Computing (HPSC), and IEEE Intl Conference on Intelligent Data and Security (IDS)*. doi:10.1109/bigdatasecurity-hpsc-ids.2019.00036

Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7*(5), e1211. doi:10.1002/widm.1211

Cho, I., & Lee, K. (2016). Advanced risk measurement approach to insider threats in cyberspace. *Intelligent Automation & Soft Computing, 22*(3), 405-413. doi:10.1080/10798587.2015.1121617

Claycomb, W. R. (2015). Detecting insider threats: Who is winning the game? *In Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats (MIST '15)*, 51-51. doi:10.1145/2808783.2808794

Connelly, L. M. (2016). Understanding research. Trustworthiness in qualitative research. *MEDSURG Nursing*, *25*(6), 435-436. Retrieved from https://www.medsurgnursing.net/archives/16nov/435.pdf

Cousins, J. B., & Bourgeois, I. (2014). Multiple case study methods and findings. *New Directions for Evaluation*, *2014*(141), 25-99. doi:10.1002/ev.20077

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing, 36*(4), 253-263. doi:10.1097/DCC.0000000000000253

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security, 2015*(1), 5–8. doi:10.1016/S1353-4858(15)70007-3

Dessi, K., & Sebastian, K. (2017). Rethinking data sharing and human participant protection in social science research: Applications from the qualitative realm. *Data Science Journal,* 16. doi:10.5334/dsj-2017-043

Dieye, M., Zhani, M., & Elbiaze, H. (2017). On achieving high data availability in heterogeneous cloud storage systems. *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM).* doi:10.23919/inm.2017.7987295

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic insurance). *The Qualitative Report, 21*(3), 521-528. Retrieved from http://nsuworks.nova.edu/tqr/vol21/iss3/6

Di Mauro, C., Fratocchi, L., Orzes, G., & Sartor, M. (2018). Offshoring and backshoring: A multiple case study analysis. *Journal of Purchasing and Supply Management, 24*(2), 108–134. doi:10.1016/j.pursup.2017.07.003

Drack, M., & Schwarz, G. (2010). Recent developments in general system theory. *Systems Research & Behavioral Science, 27*(6)*,* 601–610. doi:10.1002/sres.1013

Edgar, G. J., Bustamante, R. H., Farina, J. M., Calvopina, M., Martinez, C., & Toral-Granda, M. V. (2004). Bias in evaluating the effects of marine protected areas: The importance of baseline data for the Galapagos Marine Reserve. *Environmental Conservation, 31*(3), 212–218. doi:10.1017/s0376892904001584

Fernández, D. M., & Wagner, S. (2016). Case studies in industry: What we have learnt. *In Proceedings of the 4th International Workshop on Conducting Empirical Studies in Industry* (CESI '16). doi:10.1145/2896839.2896844

Fitroh, F., & Utama, D. N. (2017). Synthesizing a soft system methodology use in information systems research field: A systematic review. *2017 5th International Conference on Information and Communication Technology (ICoIC7)*. doi:10.1109/icoict.2017.8074722

Flood, R. L. (1990). Liberating systems theory: Toward critical systems thinking. *Human Relations, 43*(1), 49–75. doi:10.1177/001872679004300104

Florczak, K. L. (2017). Adding to the truth of the matter: The case for qualitative research. *Nursing Science Quarterly, 30*(4), 296-299. doi:10.1177/0894318417724466

Forde, E. S. (2017). Security strategies for hosting sensitive information in the commercial cloud. *ScholarWorks*. Retrieved from the Walden Library databases

Fugard, A., & Potts, H. (2015). Supporting thinking on sample sizes for thematic analysis: A quantitative tool. *International Journal of Social Research Methodology*, 18, 669-684. doi:10.1080/13645579.2015.1005453

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20,* 1408-1416. Retrieved from http://www.nova.edu/ssss/QR/QR20/9/fusch1.pdf

Goldberg, H. G., Young, W. T., Memory, A., & Senator, T. E. (2016). Explaining and aggregating anomalies to detect insider threats. *2016 49th Hawaii International Conference on System Sciences (HICSS).* doi:10.1109/hicss.2016.344

Graves, J. (2017). Data flow management: Why and how. *Network Security, 2017*(1), 5-6. doi:10.1016/S1353-4858(17)30004-1

Gray, D. E. (2013). *Doing research in the real world* (3rd ed.). London, UK: Sage Publications

Grbich, C. (2015) Narrative analysis: The socio-cultural approach to analyzing short participant stories. *Sage Research Methods Datasets*. Sage Publications. doi:10.4135/9781473947498

Green, C. A., Duan, N., Gibbons, R. D., Hoagwood, K. E., Palinkas, L. A., & Wisdom, J. P. (2015). Approaches to mixed methods dissemination and implementation research: Methods, strengths, caveats, and opportunities. *Administration and Policy in Mental Health*, *42*(5), 508-523. doi:10.1007/s10488-014-0552-6

Gustarini, M., Wac, K., & Dey, A. K. (2015). Anonymous smartphone data collection: Factors influencing the users' acceptance in mobile crowdsensing. *Personal and Ubiquitous Computing, 20*(1), 65–82. doi:10.1007/s00779-015-0898-0

Hallett, R. E., & Barber, K. (2014). Ethnographic research in a cyber era. *Journal of Contemporary Ethnography, 43,* 306-330. doi:10.1177/089124161349774

Harvey, L. (2015). Beyond member checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education*, 38, 23-38. doi:10.1080/1743727X.2014.914487

Hasking, P., & Schofield, L. (2015). Examining alcohol consumption with the theory of planned behavior: Do health and alcohol knowledge play a role? *Psychology, Health, and Medicine*, 20, 838–845. doi:10.1080/13548506.2014.969748

Hershey, D. S., & Hession, S. L. (2017). Recruitment and retention of a challenging population: Lessons learned and design implications. *Applied Nursing Research*, 38,111-117. doi:10.1016/j.apnr.2017.09.001

Hina, S., & Dominic, D. D. (2016). Information security policies: Investigation of compliance in universities. *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)*, 564. doi:10.1109/ICCOINS.2016.7783277

Ho-Jae, L., Min-Woo, P., Jung-Ho, E., & Tai-Myoung, C. (2015). New approach for detecting leakage of internal information: Using emotional recognition technology. *KSII Transactions on Internet & Information Systems, 9*(11), 4662-4679. doi:10.3837/tiis.2015.11.023

Hossain, D. M. (2017). Discourse analysis: An emerging trend in corporate narrative research. *Middle East Journal of Business*, *12*(4), 3-9. doi:10.5742/MEJB.2017.93084

Houghton, C., Murphy, K., Shaw, D., & Casey, D. (2015). Qualitative case study data analysis: An example from practice. *Nurse Researcher, 22*(5), 8-12. doi:10.7748/nr.22.5.8.e1307

Hoyland, S., Hollund, J. G., & Olsen, O. E. (2015). Gaining access to a research site and participants in medical and nursing research: A synthesis of accounts. *Medical Education, 49*(2), 224-232. doi:10.1111/medu.12622

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance.*Computers in Human Behavior*, 81, 282-293. doi:10.1016/j.chb.2017.12.022

Imran, M., Hlavacs, H., Haq, I. U., Jan, B., Khan, F. A., & Ahmad, A. (2017). Provenance based data integrity checking and verification in cloud environments. *Plos ONE, 12*(5), 1-19. doi:10.1371/journal.pone.0177576

Internet Crime Complaint Center. (2016). *2016 Internet crime report* (Data file). Retrieved from https://pdf.ic3.gov/2016_IC3Report.pdf

Irfan, M., Abbas, H., Sun, Y., Sajid, A., & Pasha, M. (2016). A framework for cloud forensic evidence collection and analysis using security information and event management. *Security & Communication Networks, 9*(16), 3790-3807. doi:10.1002/sec.1538

Ismail, W. B. W., Widyarto, S., Ahmad, R. A. T. R., & Ghani, K. A. (2017). A generic framework for information security policy development. *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 1. doi:10.1109/EECSI.2017.8239132

Iwu, C. G., Kapondoro, L., Twum-Darko, M., & Lose, T. (2016). Strategic human resource metrics: A perspective of the general systems theory. *Acta Universitatis Danubius: Oeconomica*, (2), 5. Retrieved from http://journals.univ-danubius.ro/index.php/oeconomica/article/download/3191/3218.

Jingguo, W., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attach proneness of information systems applications. *MIS Quarterly, 39*(1), 91-A7. Retrieved from https://misq.org/insider-threats-in-a-financial-institution-analysis-of-attack-proneness-of-information-systems-applications.html

Jung, S., Valero, M., Bourgeois, A., & Beyah, R. (2015). Attacking and securing beacon-enabled 802.15.4 networks. *Wireless Networks (10220038), 21*(5), 1517-1535. doi:10.1007/s11276-014-0855-2

Kasim, A., & Al-Gahuri, H. A. (2015). Overcoming challenges in qualitative inquiry within a conservative society. *Tourism Management*, 50, 124-129.doi:10.1016/j.tourman.2015.01.004

Kast, F. E., & Rosenzweig, J. E. (1972). General system theory: Applications for organization and management. *Academy of Management Journal, 15*(4), 447 - 465. doi:10.2307/255141

Kennedy, E., & Millard, C. (2016). Data security and multi-factor authentication: analysis of requirements under EU law and in selected EU member states. *Computer Law & Security Review, 32*(1), 91-110. doi:10.1016/j.clsr.2015.12.004

Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis,* 59, 111-128. doi:10.1016/j.orbis.2014.11.009

Kihn, L., & Ihantola, E. (2015). Approaches to validation and evaluation in qualitative studies of management accounting. *Qualitative Research in Accounting & Management, 12*(3), 230-255. doi:10.1109/QRAM-03-2013-0012

Korpela, K. (2015). Improving cybersecurity awareness and training programs with data analytics. *Information Security Journal: A Global Perspective, 24*(1-3), 72-77. doi:10.1080/19393555.2015.1051676

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. doi:10.1080/13814788.2017.1375092

Kozleski, E. (2017). The uses of qualitative research. *Research & Practice for Persons with Severe Disabilities, 42*(1), 19-32. doi:10.1177/1540796916683710

Kumar, M., Meena, J., Singh, R., & Vardhan, M. (2015). Data outsourcing: A threat to confidentiality, integrity, and availability. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT).* doi:10.1109/icgciot.2015.7380703

Lamba, H., Glazier, T. J., Schmerl, B., Pfeffer, J., & Garlan, D. (2015). Detecting insider threats in software systems using graph models of behavioral paths. *In*

Proceedings of the 2015 Symposium and Bootcamp on the Science of Security (HotSoS '15). Article 20, 2 pages. doi:10.1145/2746194.2746214

Last, D. (2016). Forecasting zero-day vulnerabilities. *In Proceedings of the 11th Annual Cyber and Information Security Research Conference (CISRC '16)*. doi:10.1145/2897795.2897813

Lawrence, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care, 4*(3), 324-327. doi:10.4103/2249-4863.161306

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* (11th ed.). New York, NY: Pearson

Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015, June). Automated insider threat detection system using user and role-based profile assessment. *IEEE Systems Journal,* 99. 1-10. doi:10.1109/JSYST.2015.2438442

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice, 16*(4), 473-475. doi:10.1177/1524839915580941

Li, W. (2016). Applying grey system theory to evaluate the relationship between industrial characteristics and innovation capabilities within Chinese high-tech industries. *Grey Systems: Theory and Application, 6*(2), 143–168. doi:10.1108/gs-02-2016-0005

Li, W., Yin, J., & Chen, H. (2016). Targeting key data breach services in underground supply chain. *2016 IEEE Conference on Intelligence and Security Informatics*

(ISI), Intelligence and Security Informatics (ISI), 2016 IEEE Conference on, 322. doi:10.1109/ISI.2016.7745501

Liang, N., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems, 33*(2), 361-392. doi:10.1080/07421222.2016.1205925

Liao, H., & Hitchcock, J. (2018). Reported credibility techniques in higher education evaluation studies that use qualitative methods: A research synthesis. *Evaluation and Program Planning*, 68, 157–165. doi:10.1016/j.evalprogplan.2018.03.005

Lili-Anne, K., & Eeva-Mari, I. (2015). Approaches to validation and evaluation in qualitative studies of management accounting. *Qualitative Research in Accounting & Management*, (3), 230. doi:10.1108/QRAM-03-2013-0012

Liu, F., Shu, X., Yao, D., & Butt, A. R. (2015). Privacy-preserving scanning of big content for sensitive data exposure with MapReduce. *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy - CODASPY '15*. doi:10.1145/2699026.2699106

Liu, S., & Lin, Y. (2010). Introduction to grey systems theory. *Grey Systems*, 1-18. doi:10.1007/978-3-642-16158-2_1

Liu, S., Yang, Y., Xie, N., & Forrest, J. (2016). New progress of grey system theory in the new millennium. *Grey Systems, 6*(1), 2–31. doi:10.1108/GS-09-2015-0054

Maasberg, M., Warren, J., & Beebe, N. L. (2015). The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits. *2015 48th*

Hawaii International Conference on System Sciences. doi:10.1109/HICSS.2015.423

Malecic, A. (2017). Footprints of general systems theory. *Systems Research & Behavioral Science, 34*(5), 631-636. doi:10.1002/sres.2484

Mann, I. (2008). *Hacking the human: social engineering techniques and security countermeasures.* Aldershot, United Kingdom: Gower Publishing

Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage Publications

Mayoh, J., & Onwuegbuzie, A. J. (2015). Toward a conceptualization of mixed methods phenomenological research. *Journal of Mixed Methods Research, 9,* 91-107. doi:10.1177/1558689813505358

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. Perfusion, 30, 537-542. doi:10.1177/0267659114559116

Miller, S., & Coutts, C. (2018). A multiple case study of local& creative financing of bicycle and pedestrian infrastructure. *Case Studies on Transport Policy, 6*(2), 257–264. doi:10.1016/j.cstp.2018.03.008

Moghaddasi, H., Sajjadi, S., & Kamkarhaghighi, M. (2016). Reasons in support of data security and data security management as two independent concepts: A new model. *The Open Medical Informatics Journal*, 10, 4–10. doi:10.2174/1874431101610010004

Morgan, D. L. (2015). From themes to hypotheses: Following up with quantitative methods. *Qualitative Health Research*, *25*(6), 789-793. doi:10.1177/1049732315580110

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research, 25*(9), 1212-1222. doi:10.1177/1049732315588501

Nair, L. l. (2018). Scientific integrity in qualitative research (SCIQUAL) seminar 2017. *Forum: Qualitative Social Research, 19*(1), 288-295. doi:10.17169/fqs-19.1.2964

Nair, S. C., & Ibrahim, H. (2015). Informed consent form challenges for genetic research in a developing Arab country with high risk for genetic disease. *Journal of Genetic Counseling, 24*(2), 294-299. doi:10.1007/s10897-014-9763-y

National Institute of Standards and Technology. (2011). Cybersecurity, innovation, and the internet economy. Retrieved from https://www.nist.gov/sites/default/files/documents/itl/General-Dynamics-C4-Systems_NIST-RFC-110801.pdf

Neuman, D. (2014). Qualitative research in educational communications and technology: A brief introduction to principles and procedures. *Journal of Computing in Higher Education, 26*(1), 69-86. doi:10.1007/s12528-014-9078-x

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing, 18*(2), 34-35. doi:10.1136/eb-2015-102054

Norman, Z. (2015). Reflection on organization theory: Connecting general system theory to open systems theory. *SSRN Electronic Journal*. doi:10.2139/ssrn.2671070

Nostro, N., Ceccarelli, A., Bondavalli, A., & Brancati, F. (2013). A methodology and supporting techniques for the quantitative assessment of insider threats. *Proceedings of the 2nd International Workshop on Dependability Issues in Cloud Computing- DISCCO '13.* doi:10.1145/2506155.2506158

Omidvari, M., Abootorabi, S. M., & Mehrno, H. (2016). An investigation of the influence of managerial factors on industrial accidents in the construction industry using the gray FTA method. *Grey Systems: Theory and Application, 6*(1), 96–109. doi:10.1108/gs-01-2016-0001

Pacheco, J., Tunc, C., & Hariri, S. (2018). Security framework for IoT cloud services. *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*. doi:10.1109/aiccsa.2018.8612808

Pacho, T. O. (2015). Exploring participants' experiences using case study. *International Journal of Humanities and Social Science, 5*(4), 44-53. Retrieved from http://www.ijhssnet.com/

Padayachee, K. (2015). Aspectising honeytokens to contain the insider threat. *IET Information Security, 9*(4), 240-247. doi:10.1049/iet-ifs.2014.0063

Padilla, V. S., & Freire, F. F. (2019). A contingency plan framework for cyber-attacks. *Journal of Information Systems Engineering & Management, 4*(2), em0098. Retrieved from https://doi.org/10.29333/jisem/5898

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed

method implementation research. *Administration and Policy in Mental Health, 42*(5), 533-544. doi:10.1007/s10488-013-0528-y

Peticca-Harris, A., deGama, N., & Elias, S. R. S. T. A. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods, 19*(3), 376–401. doi:10.1177/1094428116629218

Phillips, D. M., Mazzuchi, T. A., & Sarkani, S. (2018). An architecture, system engineering, and acquisition approach for space system software resiliency. *Information & Software Technology,* 94, 150-164. doi:10.1016/j.infsof.2017.10.006

Pol, M. V. J. (2019). Identity and access management tools. *International Journal of Trend in Scientific Research and Development*, *3(*4*)*, 796–798. doi:10.31142/ijtsrd23935

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214. doi:10.1080/07421222.2015.1138374

Pouvreau, D. (2014). On the history of Ludwig von Bertalanffy's "general systemology," and on its relationship to cybernetics-part II: Contexts and developments of the systemologicalhermeneutics instigated by von Bertalanffy. *International Journal of General Systems, 43,* 172-245. doi:10.1080/03081079.2014.883743

Pryce, L., Tweed, A., Hilton, A., & Priest, H. M. (2017). Tolerating uncertainty: Perceptions of the future for ageing parent carers and their adult children with

intellectual disabilities. *Journal of Applied Research in Intellectual Disabilities, 30*(1), 84-96. doi:10.1111/jar.12221

Quigley, A. (2002). Insider job. *Networker, 6*(1), 20-24. doi:10.1145/505289.505290

Ramachandran, M., & Victor, C. (2016). Towards performance evaluation of cloud service providers for cloud data security. *International Journal of Information Management,* (4). 618. doi:10.1016/j.ijinfomgt.2016.03.005

Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science,* 48, 204-209. doi:10.1016/j.procs.2015.04.171

Razaque, A., & Rizvi, S. S. (2016). Triangular data privacy-preserving model for authenticating all key stakeholders in a cloud environment. *Computers & Security*, 62, 328-347. doi:10.1016/j.cose.2016.08.006

Reed, I. A. (2016). Ethnography, theory, and sociology as a human science: An interlocution. *Ethnography, 18*(1), 107–129. doi:10.1177/1466138115592417

Richardson, E. Z. L., Allison, K. R., Teleguario, H., Chacach, W., Tum, S., Gesink, D., & Berry, A. (2017). "Taking care" in intercultural research. *International Journal of Qualitative Methods, 16*(1), 160940691668082. doi:10.1177/1609406916680823

Robins, C. S., & Eisen, K. (2017). Strategies for the effective use of NVivo in a large-scale study: Qualitative analysis and the repeal of don't ask, don't tell. *Qualitative Inquiry, 23*(10), 768–778. doi:10.1177/1077800417731089

Roulston, K., & Shelton, S. A. (2015). Reconceptualizing bias in teaching qualitative research methods. *Qualitative Inquiry, 21*(4)*,* 332–342. doi:10.1177/1077800414563803

Rule, P., & John, V. M. (2015). A necessary dialogue: Theory in case study research. *International Journal of Qualitative Methods, 14*(4), 1-11. doi:10.1177/1609406915611575

Saa, P., Moscoso-Zea, O., Costales, A. C., & Lujan-Mora, S. (2017). Data security issues in cloud-based Software-as-a-Service ERP. *2017 12th Iberian Conference on Information Systems and Technologies (CISTI),* 1. doi:10.23919/CISTI.2017.7975779

Sallam, A., & Bertino, E. (2017). Detection of temporal insider threats to relational databases. *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*. doi:10.1109/cic.2017.00058

Santos, R. E. d. S., Silva, F. Q. B. d., & Magalhaes, C. V. C. d. (2017). Member checking in software engineering research: Lessons learned from an industrial case study. *2017 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM).* doi:10.1109/esem.2017.29

Satoh, N., & Samejima, M. (2017). Risk words suggestion for information security audit by bayeasian inference. *2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*. doi:10.1109/iiai-aai.2017.11

Sauro, J. (2015, October 15). 5 types of qualitative methods. Retrieved from https://measuringu.com/qual-methods

SBA. (2012). Frequently asked questions. Retrieved from https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf

SBA. (2016). Table of small business size standards. Retrieved from https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf

Scheibe, M., Reichelt, J., Bellmann, M., & Kirch, W. (2015). Acceptance factors of mobile apps for diabetes by patients aged 50 or older: A qualitative study. *Medicine 2.0, 4*(1), e1-e13. doi:10.2196/med20.391

Schlicher, B. G., MacIntyre, L. P., & Abercrombie, R. K. (2016). Towards reducing the data exfiltration surface for the insider threat. *2016 49th Hawaii International Conference on System Sciences (HICSS)*. doi:10.1109/hicss.2016.345

Schneider, A., Wickert, C., & Marti, E. (2017). Reducing complexity by creating complexity: A systems theory perspective on how organizations respond to their environments. *Journal of Management Studies, 54*(2), 182-208. doi:10.1111/joms.12206

Sen, R., & Borle, S. (2015). Estimating the contextual risk of databreach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314–341. doi:10.1080/07421222.2015.1063315

Setiawan, A. B., & Sastrosubroto, A. S. (2016). Strengthening the security of critical data in cyberspace, a policy review.*2016 International Conference on Computer, Control, Informatics and its Applications (IC3INA)*. doi:10.1109/IC3INA.2016.7863047

Shalev, N., Keidar, I., Moatti, Y., & Weinsberg, Y. (2016). WatchIT: Who watches your IT guy? *In Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats* (MIST '16). 93-96. doi:10.1145/2995959.2995968

Singh, S., Corner, P. D., & Pavlovich, K. (2015). Failed, not finished: A narrative approach to understanding venture failure stigmatization. *Journal of Business Venturing, 30*(1), 150-166. doi:10.1016/j.jbusvent.2014.07.005

Sloan, A. A., & Bowe, B. B. (2015). Experiences of computer science curriculum design: A phenomenological study. *Interchange (0826-4805), 46*(2), 121-142. doi:10.1007/s10780-015-9231-0

Small, W., Maher, L., & Kerr, T. (2014). Institutional ethical review and ethnographic research involving injection drug users: A case study. *Social Science & Medicine, 104,* 157–162. doi:10.1016/j.socscimed.2013.12.010

Sousa, D. (2014). Validation in Qualitative Research: General aspects and specificities of the descriptive phenomenological method. *Qualitative Research in Psychology*, *11*(2), 211-227. doi:10.1080/14780887.2013.853855

Stake, R. E. (2006). *Multiple case study analysis.* London: Guilford Press

Starfelt Sutton, L. C., & White, K. M. (2016). Predicting sun-protective intentions and behaviors using the theory of planned behavior: A systematic review and meta-analysis. *Psychology & Health, 31*(11), 1272–1292. doi:10.1080/08870446.2016.1204449

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

Stuckey, H. L., Kraschnewski, J. L., Miller-Day, M., Palm, K., Larosa, C., & Sciamanna, C. (2014). "Weighing" two qualitative methods. *Field Methods, 26*(4), 343–361. doi:10.1177/1525822x14526543

Suen, L. W., Huang, H., & Lee, H. (2014). A comparison of convenience sampling and purposive sampling. *Hu Za Zhi, 61*(3), 105-111. doi:10.6224/JN.61.3.105

Sulochana, M., & Dubey, O. (2015). Preserving data confidentiality using multi-cloud architecture. *Procedia Computer Science, 50(Big Data, Cloud and Computing Challenges),* 357-362. doi:10.1016/j.procs.2015.04.035

Syynimaa, N. (2017). The quest for underpinning theory of enterprise architecture - general systems theory. *Proceedings of the 19th International Conference on Enterprise Information Systems*. doi:10.5220/0006314904000408

Turner, S. F., Cardinal, L. B., & Burton, R. M. (2017). Research design for mixed methods. *Organizational Research Methods*, *20*(2), 243-267. doi:10.1177/1094428115610808

Ultra, J. D., & Pancho-Festin, S. (2017). A simple model of separation of duty for access control models. *Computers & Security*, 68, 69–80. doi:10.1016/j.cose.2017.03.012

Urciuoli, L., & Hintsa, J. (2017). Adapting supply chain management strategies to security – an analysis of existing gaps and recommendations for improvement.

International Journal of Logistics: Research & Applications, 20(3), 276-295.doi:10.1080/13675567.2016.1219703

U.S. Department of Health & Human Services. (1979). The Belmont Report. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

U.S. Department of Homeland Security. (2012). DHS 4300A sensitive systems handbook. Retrieved from https://www.dhs.gov/sites/default/files/publications/4300A-Handbook-Attachment-S1-Managing-CREs-Containing-SPII.pdf

U.S. Department of Justice. (2015). *Cybersecurity law enforcement: The "cutting edge" symposium.* Retrieved from https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-cybersecurity-law

U.S. Department of Labor. (2018a). *Occupational outlook handbook, database administrators.* Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/database-administrators.htm

U.S. Department of Labor. (2018b). *Occupational outlook handbook, network and computer systems administrators.* Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/network-and-computer-systems-administrators.htm

Vaughn, P., & Turner, C. (2015). Decoding via coding: Analyzing qualitative text data through thematic coding and survey methodologies. *Journal of Library Administration, 56*(1), 41–51. doi:10.1080/01930826.2015.1105035

Von Bertalanffy, L. (1968). *General systems theory: Foundations, developments, applications.* New York, NY: George Braziller. Retrieved from https://monoskop.org/images/7/77/Von_Bertalanffy_Ludwig_General_System_Theory_1968.pdf

Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal, 15*(4), 407–426. doi:10.2307/255139

Wagner, J., Rasin, A., Glavic, B., Heart, K., Furst, J., Bressan, L., & Grier, J. (2017). Carving database storage to detect and trace security breaches. *Digital Investigation, 22(Supplement)*, S127-S136. doi:10.1016/j.diin.2017.06.006

Wang, D., Wang, N., Wang, P., & Qing, S. (2015). Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity. *Information Sciences*, 321, 162-178. doi:0.1016/j.ins.2015.03.070

Wang, J. W., Zhang, W. J., & Wang, J. W. (2016). Design theory and methodology for enterprise systems. *Enterprise Information Systems, 10*(3), 245-248. doi:10.1080/17517575.2015.1080860

Wang, S., Pei, R., & Zhang, Y. (2019). EIDM: A ethereum-based cloud user identity management protocol. *IEEE Access*, 7, 115281–115291. doi:10.1109/access.2019.2933989

Weis, D., & Willems, H. (2017). Aggregation, validation, and generalization of qualitative data—Methodological and practical research strategies illustrated by the research process of an empirically based typology. *Integrative Psychological & Behavioral Science*, *51*(2), 223-243. doi:10.1007/s12124-016-9372-4

Woodgate, R. L., Zurba, M., Tennent, P., Cochrane, C., Payne, M., & Mignone, J. (2017). A qualitative study on the intersectional social determinants for indigenous people who become infected with HIV in their youth. *International Journal for Equity in Health*, 161-12. doi:10.1186/s12939-017-0625-8

Yakut Cayir, M., & Saritas, M. T. (2017). Computer assisted qualitative data analysis: A descriptive content analysis (2011 - 2016). *Necatibey Faculty of Education Electronic Journal of Science & Mathematics Education, 11*(2), 518-544. Retrieved from https://web.b.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=13076086&AN=128030298&h=8Zqy91mireXoiXc9JZhjsO6zBsOpvU2COUsx9gO%2faS990qPJgvScQhbNOTy3e2K5I16GF%2bwlIbaNcCNVrDWYbA%3d%3d&crl=c&resultNs=AdminWebAuth&resultLocal=ErrCrlNotAuth&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d13076086%26AN%3d128030298

Yin, R. K. (1981). The case study as a serious research strategy. *Science Communication, 3*(1), 97–114. doi:10.1177/107554708100300106

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

Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM, 57*(2), 31-35. doi:10.1145/2556938

Yuan, J., Malin, B., Modave, F., Guo, Y., Hogan, W. R., Shenkman, E., & Bian, J. (2017). Towards a privacy-preserving cohort discovery framework for clinical research networks. *Journal of Biomedical Informatics,* 66, 42-51. doi:10.1016/j.jbi.2016.12.008

Zaytsev, A., Malyuk, A., & Miloslavskaya, N. (2017). Critical analysis in the research area of insider threats. *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*. doi:10.1109/FiCloud.2017.16

Zhang, J., & Li, H. (2017). Research and implementation of a data backup and recovery system for important business areas. *2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)*. doi:10.1109/ihmsc.2017.209

Zhang, J. J. (2017). Research ethics and ethical research: Some observations from the global south. *Journal of Geography in Higher Education, 41*(1), 147-154. doi:10.1080/03098265.2016.1241985

Zhurin, S. I. (2015). Comprehensiveness of response to internal cyber-threat and selection of methods to identify the insider. *Journal of ICT Research & Applications, 8*(3), 251-269. doi:10.5614/itbj.ict.res.appl.2015.8.3.5

Appendix A: Interview Protocol

Interview: Exploring data security management strategies to prevent data breaches

Interview Protocol	
What you will do	**What you will say—script**
Introduce the interview and set the stage—often over a meal or coffee	The purpose of this qualitative multiple case study will be to explore the data security management strategies that database and system administrators use to prevent data breaches by malicious insiders in small-scale IT government contracting agencies. This research study may benefit the field of information security by increasing understanding of the complex nature of insider threats; data security management strategies that better protect sensitive information stored in databases. This study should provide database administrators and system administrators with a robust framework for assessing the data security management strategies in use to prevent data breaches by malicious insiders.
	Indicate that the interviewer will be taking notes.
	Indicate that the interviewer will be recording the

	conversation for transcription.
	Advise the participant there will be an opportunity to ask questions at the end of the interview.
Semistructured Interview Questions to confirm eligibility	• What is your current role and title? • How many years of database administration or system administration do you currently possess? • How long ago have you implemented a data security management strategy? • How many years of experience do you have in this type of role? • How many years have you worked at this firm?
Watch for nonverbal queues	1. What strategies do you use to prevent and protect your data from data breaches by malicious insiders?
Paraphrase as needed	2. What strategies have you implemented to detect and respond to data breaches?
Ask follow-up probing questions to get more in-depth	3. What corrective strategies do you use should a data breach occur, and what is your data breach contingency plan?
	4. What strategies do you use to identify and assess the level of risk should there be a data breach incident?

	5. Which data security management strategies work well and why?
	6. What external entities or factors play a role in deciding which strategies to implement based on your experience?
	7. What alerting mechanisms do you use should a data breach occur?
	8. What programs do you use to ensure staff is compliant with data security management protocols?
	9. What training strategies do you use to help keep you informed of current data breach events?
	10. What strategies do you use to establish the baseline of the data you manage and how often is the strategy reviewed or updated?
	11. Which data breach cases caused by malicious insiders have you experienced?
	12. What additional data security management insight would you like to provide or elaborate on prior to concluding this interview?
	13. The last interview question should be a wrap-up question such as: What additional experiences have you had…?

Wrap up interview thanking participant	Ask the participant if he or she has any questions and provide responses to these.
	Highlight the potentially positive aspects of working within the study.
	Describe the next steps in the interviewing process (e.g., member checks) and provide a clear timeframe for when the participant will hear from the interviewer again.
	Thank the participant for his or her participation and time
Schedule follow-up member checking interview	I would like to follow up with you in the next day or two to briefly go over a summary of your responses.
Follow–up Member Checking Interview	
Introduce follow-up interview and set the stage	This is a follow-up interview to go over the previous summary of answers.
Share a copy of the succinct synthesis for each individual question	Ask the participant if he or she has any questions and provide responses to the summary.
	Reintroduce the questions and answers.
	Ask if they have anything to add.

Bring in probing questions related to other information that you may have found—note the information must be related so that you are probing and adhering to the IRB approval. Walkthrough each question, read the interpretation and ask: Did I miss anything? Or, what would you like to add?	1. What strategies do you use to prevent and protect your data from data breaches by malicious insiders?
	2. What strategies have you implemented to detect and respond to data breaches?
	3. What corrective strategies do you use should a data breach occur, and what is your data breach contingency plan?
	4. What strategies do you use to identify and assess the level of risk should there be a data breach incident?
	5. Which data security management strategies work well and why?
	6. What external entities or factors play a role in deciding which strategies to implement based on your experience?
	7. What alerting mechanisms do you use should a data breach occur?

	8. What programs do you use to ensure staff is compliant with data security management protocols?
	9. What training strategies do you use to help keep you informed of current data breach events?
	10. What strategies do you use to establish the baseline of the data you manage and how often is the strategy reviewed or updated?
	11. Which data breach cases caused by malicious insiders have you experienced?
	12. What additional data security management insight would you like to provide or elaborate on prior to concluding this interview?

Appendix B: Human Subject Research Certificate of Completion

Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Michael Ofori-Duodu** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 01/17/2017.

Certification Number: 2275855.

Appendix C: Observation Protocol

The purpose of this observation protocol is to provide a step action table (job aide, Checklist) to help me to stay focused on the data and other details that I observe in the setting.

Directions: To start each observation, write a comprehensive description of the setting following the table below. Using the table on the next page, note the approximate time frames in which you make the observations, along with notes describing what you see occurring and any other details that you consider to be important. After the observation, review your notes and begin to identify key points (concepts and ideas) that may help you later in data analysis.

Name of Researcher	Michael Ofori-Duodu
Tentative Schedule	1:45 PM – 4:00 PM
Date:	April 10, 2019
The Background: Physical setting (Describe in thick rich detail what it looks like, sounds like, and any other details.	The meeting was held in the conference room on the third floor of the office space in Washington, D.C. The room could hold up to about 10 persons. There were three people in attendance. Attire was business casual, and the meeting was in a partially structured format where two presenters, the main presenter, and a second person, took turns to share the information on the upcoming implementation of a configuration management database (CMDB).

The Position: **(i.e., close, distance, etc.)**	The seating arrangement was a round-table format, so I had the opportunity to both observe the presentation, take audio recordings, capture detailed notes, and write down audience participation.
The Action: What happens? What is the sequence? Is there a cause and effect? If so, provide details.	The main presenter of the meeting discussed an upcoming CMDB tool implementation, which would replace the current toolset due to some gaps in security, scalability, and functionality, among others, that had been identified earlier. The CMDB will serve as a repository of all the configuration items in the enterprise, including servers, workstations, software, users, and how they relate to each other. Additionally, the new system will allow the review of a list of all the permissions the users of our databases have, and the level of access the users have to what application.
Type of Observation: **(direct or participant)**	The researcher performed a direct observation of the training session.
Areas Training Focused on:	How users will be authenticated based on existing data in the current system which would need to be migrated to the new system. Additionally, an overview of how the new system would integrate

	with the current single sign-on (SSO) system, Okta, and how the administration of the new CMDB system will be performed from a strategic management standpoint.
Time:	**Observation notes:**
2:00 PM	Presenter projected training meeting slides, which included the approach to migrate the existing data to the new system.
	Risks including data loss and mismatch were raised, and through brainstorming, potential solutions were presented.
	A YouTube video containing vendor information about the new CMDB tool was presented. The video provided information on configuration, integration, post-deployment maintenance, and security operations of the system.
4:00 PM	No questions. End of discussion and meeting.