2021

Insider Threats' Behaviors and Data Security Management Strategies

Gladys C. Cooley
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Gladys C. Cooley

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. Keri Heitner, Committee Chairperson, Management Faculty
Dr. Danielle Wright-Babb, Committee Member, Management Faculty
Dr. Nikunja Swain, University Reviewer, Management Faculty

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

Walden University
2021

Abstract

Insider Threats' Behaviors and Data Security Management Strategies

by

Gladys C. Cooley

MA, Walden University, 2021

MA, George Washington University, 1999

MA, Ohio University, 1984

BBA, University of Panama, 1982

Dissertation Submitted in Partial Fulfillment

of Requirements for the Degree of

Doctor of Philosophy

Management Information Systems

Walden University

August 2021

Abstract

As insider threats and data security management concerns become more prevalent, the identification of risky behaviors in the workplace is crucial for the privacy of individuals and the survival of organizations. The purpose of this three-round qualitative Delphi study was to identify real-time consensus among 25 information technology (IT) subject matter experts (SMEs) in the Washington metropolitan area about insider threats and data security management. The SMEs participating in this study were adult IT professionals and senior managers with certification in their area of specialization and at least 5 years of practical experience. The dark triad theory was the conceptual framework used for describing behaviors attributed to reasons and motivators for insider threats in public and private organizations. The research questions pertained to reasons and motivators for insider threats in organizations, security strategies and early interventions used, and potential policies and procedures to manage insider threats' access to systems. One open-ended survey and two closed-ended surveys were disseminated via Survey Monkey. Data analysis consisted of data reduction through consolidation, data display, and data verification. Data were analyzed through categorization and direct interpretation using a 5-point Likert agreement scale. The findings revealed consensus about reasons and motivators such as insufficient guidelines and training, lack of background investigations, and financial gain and money; security strategies and early interventions; and policies and procedures to manage insider threats' access to systems. Overall, training was the most important element preventing insider threats. The findings may inform how organizations build safe working environments that increase employee recruitment, retention, and loyalty while reducing identity theft and increasing data security in organizations.

Insider Threats' Behaviors and Data Security Management Strategies

by

Gladys C. Cooley

MA, Walden University, 2021

MA, George Washington University, 1999

MA, Ohio University, 1984

BBA, University of Panama, 1982

Dissertation Submitted in Partial Fulfillment

of Requirements for the Degree of

Doctor of Philosophy

Management Information Systems

Walden University

August 2021

Dedication

I dedicate this dissertation to my children, who were always my inspiration and to whom I wish to leave a legacy of perseverance, professional growth, and hard work; to my mother and my siblings and the rest of my family, who encouraged me to achieve my goals, and kept me in their prayers. Also, to my colleagues and friends who had a role in my success and accompanied me through this journey.

Acknowledgments

To all members of my dissertation committee, especially my committee chair, Dr. Keri Heitner, whose support, and guidance finally allowed me to attain this milestone; Dr. Danielle Wright-Babb, second committee chair for her consistency and clarity; to Dr. Raghu Korrapati, Senior Core Faculty, College of Management and Technology; Dr. Sandy Kolberg, former Program Director for the PhD. in Management Program, my academic advisor, Dr. Richard Hay, who made sure I never missed an enrollment; and to Walden University's outstanding editor, Ms. Carey Little Brown, for her valued feedback, thank you for your support.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

The increasing use of information technology (IT) for daily activities has contributed to information systems' vulnerabilities and insider threats in public and private organizations (National Institute of Standards and Technology [NIST], 2016). Insider threats can be trusted employees, vendors, and associates with internal access to systems in any organization who display a disregard for established access policies and procedures. Insider threats' unauthorized activities lead to fraud, theft, and data sabotage (NIST, 2016; Rabai et al., 2014). This study provides real-time views and opinions from IT subject matter experts (SMEs) about managing insider threats' activities, identifying insider threats' risky behaviors, and what countermeasures need to be applied. Risky behaviors may manifest as antisocial actions, as described in the conceptual framework of the dark triad theory, leading to negative consequences for individuals and organizations such as identity theft, loss of reputation, income, business, and trust (Crysel et al., 2013). Spain et al. (2014) noted that personality traits related to the dark triad have become more prominent in recent years. Furnham et al. (2014) defined dark personality traits as characteristics that reflect a motivation to elevate the self and harm others. Among other conceptualizations in the dark triad theory, narcissism, psychopathy, and Machiavellianism have represented the most popular operationalization of dark personality behaviors in social studies.

The relationship between the social networks and systems access by insiders at work could be measured by any of the constructs of the dark triad (O'Boyle et al., 2012). The study of personality characteristics has resulted in a model that has been used to

describe insider threats' behaviors (Goodboy & Martin, 2015). Such characteristics have been traced to the dark triad's traits of manipulation, self-centeredness, and a lack of team and interpersonal relations (Jonason et al., 2017). With the current study, I provided an opportunity for SMEs to provide real-time traits, based on their experiences, if applicable to their organizations.

Understanding the dark triad behaviors could help managers in public and private organizations to curtail insider threats' antagonistic actions, manage a lack of agreeableness in staff, and instill honest and ethical behaviors (Sokolowski et al., 2016). As insider threats became more prevalent in this age of instant communication, it was critical to identify current reasons and motivators for insider threats, as new security policies and real-time strategies are needed to rapidly resolve the operational risks posed by new technology requirements and unauthorized access to data (Green, 2014). New technologies may have enabled faster communications, but also the unauthorized access of insider threats to sensitive, confidential, and personally identifiable information in part because of management's urgency for system deployments, especially during the implementation of emerging technologies (NIST, 2016).

The unauthorized access of corporate systems has been the result of actions by untrained new hires, departing employees, and disgruntled employees (American Bar Association [ABA], 2017; NIST, 2016; Ponemon Institute, 2017). By uncovering real time strategies for onboarding, offboarding, systems' management, and policies and procedures, this study could help public and private organizations to develop awareness and countermeasures to prevent insider threats and data breaches, especially during new

system deployments. Running parallel efforts for security protocols acquisitions, and innovative technology implementations is not always possible due to management approvals, budgets, and employees' buy-in (Green, 2014; NIST, 2016). The new findings from the current Delphi study regarding risky and toxic behaviors may serve as a baseline for developing employee training and development opportunities, along with new security strategies, and controls (NIST, 2016; Trochim et al., 2015).

Demands from innovative technologies' system implementations, human resource management, training, and business requirements place additional burdens and challenges on the roles and responsibilities that IT program and project managers exercise in public and private organizations (NIST, 2016). IT managers are responsible for new systems, security, implementations, and data management, along with staffing, making it a priority to develop countermeasures to prevent unauthorized access to data systems and preserve the confidentiality, integrity, and accessibility of data on a need-to-know basis (National Initiative for Cybersecurity Education [NICE], 2016). The challenges that managers experience include maintaining adequate access controls and staffing levels, hiring personnel possessing the network systems and cybersecurity skills specified in contract requirements, or the hiring organizations, and retaining current skilled IT personnel (NICE, 2016). I included a purposeful sample in this study comprised of 25 IT SMEs in the Washington metropolitan area, that is, Maryland, Virginia, and the District of Columbia.

As insider threats continue to rise, creating known and unknown risks to society, findings from this Delphi study could provide real-time strategies, best industry practices,

and greater awareness of insider threats' behaviors (Abdallah & Gheyas, 2016; Amigorena, 2014; Ponemon Institute, 2017). Managers could use the findings of this study to generate early interventions to curtail insider threats' toxic behaviors and data breaches.

This dissertation consists of five chapters and appendices. Chapter 2 is a comprehensive literature review that includes insider threats' past events, history, and present challenges (Walden University, n.d.). Chapter 3 addresses the study methodology and includes data gathering, analysis, and strategy. Chapters 4 and 5 include reporting of the Delphi study's final analysis, conclusions, and recommendations.

Background of the Study

Data breaches occurring at the Office of Personnel Management, Department of State, Internal Revenue System, Department of Defense, Democratic National Convention, Marriott, the Microsoft Corporation, the Central Intelligence Agency (CIA), and Equifax were eye-opening examples of the impacts of insider threats' intentional, or unintentional data breaches in public and private organizations. Gelles et al.'s (2012) "Mitigating the Insider Threat" quantitative survey indicated that 40% of the employees interviewed responded that they were treated unfairly, or unethically by employers; 27% did not consider the ethical consequences of posting comments, photos, and videos online; and 74% said that it was easy to damage a company's reputation using social media. Data losses stated in the Federal Bureau of Investigation Crime Report averaged $4.63 billion. (FBI, 2016c).

Problem Statement

Insider threats and data security have been an ongoing problem for public and private organizations (NIST, 2016; Padayachee, 2016). As insider threats increase in this era of fast communications, it was important to discover the reasons and motivators of insider threats in the workplace, as new security protocols and real-time strategies were required to be developed to quickly address the operational risks that were introduced with innovative technologies (Green, 2014). The general problem is that insider threats' activities lead to data breaches in public and private organizations (Greitzer et al., 2013; Hampton et al., 2014; NIST, 2016; Ponemon Institute, 2017; Rosenfeld et al., 2012; Sokolowski et al., 2016).

In 2017, insider threats accounted for 54.4% of all incidents and losses among the SMEs surveyed by the Ponemon Institute (2017). As insider threats become more prevalent, increased awareness of risky behaviors and real-time solutions must be gathered from SMEs who can share their knowledge and opinions on the subject. Because insider threats continue to rise, increased awareness of risky behaviors and real-time strategies needed to be gathered from SMEs, who could share their experiences about the subject of insider threats, and their antisocial or risky behaviors. Spain et al. (2014) and Roeser et al. (2016) found that risky behaviors can manifest as antisocial acts that have negative workplace consequences. The specific problem was that there was no current consensus among SMEs concerning employees' risky behaviors, preventive strategies, and controls needed to protect data in public and private organizations (Pew Research Center, 2017; Rosenfeld et al., 2012; Sokolowski et al., 2016). SMEs identified

risky behaviors and activities that predispose some employees to commit data security breaches have not been recently addressed in current qualitative studies (Abdallah & Gheyas, 2016; Amigorena, 2014; Greitzer et al., 2013).

Purpose of the Study

The purpose of this qualitative Delphi study was to uncover what real-time consensus existed among 25 IT SMEs in the Washington metropolitan area for managing insider threats and data security in public and private organizations. The purpose statement supported the problem statement of the study (Locke et al., 2004). SMEs in the Washington metropolitan had an opportunity to provide feedback about security strategies and preventive controls used to deter insider threats and risky behaviors and protect data in their organizations (Hampton et al., 2014; Rosenfeld et al., 2012; Sokolowski et al., 2016). By creating greater awareness about employees' risky behaviors, I hoped to facilitate early interventions to prevent insider threats and data breaches in public and private organizations (Abdallah & Gheyas, 2016; Amigorena, 2014; Ponemon Institute, 2017). The dark triad theory was the conceptual framework of this study for identifying and classifying activities and risky behaviors as viewed by SMEs. Recent qualitative research on data security breaches with a focus on employee behaviors was lacking in the literature. Instead, quantitative research that was heavily focused on the financial impact of insider threats was extensive, leaving a gap for real-time qualitative research on the subject (Ponemon Institute, 2017). This Delphi study was used to convene a targeted sample, or panel of 25 SMEs in public and private organizations to achieve consensus on reasons, motivators, strategies, and best security

practices, policies, and procedures to manage insider threats in public and private organizations (Hoffmann et al., 2018).

Research Questions

The research questions were derived from the problem statement and the purpose statement. Hancock and Algozzine (2015) noted that a well-formulated research question can be used to support the purpose and meaning of the statements and that these questions do not present an ethical constraint. Twenty-five IT professionals holding certifications in the Washington metropolitan area were selected as the sample for this Delphi study. During Round 1, the overarching research question was the following:

RQ1. What is the level of consensus among a panel of SMEs regarding the reasons for insider threats in organizations?

The sub questions included in the study were:

SQ1. What are the motivators for insider threats in the workplace?

SQ2. What are the security strategies and early interventions used by organizations to prevent data breaches and insider threats?

SQ3. What policies and procedures can be developed to manage insider threats' access to systems in organizations?

Conceptual Framework of the Study

The dark triad was the conceptual framework that grounded this study for recognition of the essential behaviors of insider threats as described by industry SMEs (Legg, 2017). Although other frameworks were considered for this study, a conceptual framework was preferred to raise awareness for detecting behaviors that could help to

respond to insider threats (Beck & Harter, 2015; Cohen, 2015). A conceptual framework allows for social constructs, data gathering and analysis, and data saturation when sufficient consensus has been reached.

The use of the dark triad theory as a determinant for behavioral observation, combined with industry-standard monitoring systems and controls, can uncover more possibilities for developing preventive actions, policies, and procedures to improve security efficiency (Legg et al., 2017). Dark triad theory offered a framework for previous studies that was used to justify the need for this study. Traits such as Machiavellianism, narcissism, and psychopathy, were used as behavioral markers to ground this study and can be seen in the examination of the literature review in Chapter 2, as the central elements of this conceptual framework (Walden University, n.d.). Little empirical research had been conducted to study the phenomenon of reasons and motivators for insider threats (Thoroughgood & Padilla, 2013). The dark triad theory was developed to offer explanations on traits that have been traced to manipulative social behaviors associated with insider threats' behaviors, feelings, disregard for following guidelines and organizational policies, and risky activities, as can be observed in Table 4 (Sokolowski et al., 2016; Thoroughgood & Padilla, 2013). Giammarco and Vernon (2015) noted that individuals displaying narcissism have an inflated self-view and focus on themselves. Psychopathy is characterized by arrogant and deceitful personality, high impulsivity, low empathy, low anxiety, and thrill-seeking behaviors (Giammarco & Vernon, 2015).

Nature of the Study

A qualitative Delphi method was my chosen research methodology for this study, while other research methods such as grounded theory and case study were also under consideration (Charmaz, 2014; Urquhart et al., 2010). However, due to the iterative nature of insider threats and the changing requirements for IT professionals, gathering the consensus of SMEs could render a better real-time outcome for identifying toxic employee behaviors, noting industry best practices, and discovering real-time security countermeasures for insider threat behaviors and data breaches. The changing nature of insider threats and innovative technologies create a major demand for determining what industry best practices are followed by SMEs in the Washington metropolitan area. The phenomenon of insider threats has been an increasing problem for systems users in academia, banking, medicine, and practically any area that requires confidentiality, privacy, and for the safe transferability of personally identifiable information (PII) (NIST, 2016). Insider threats and data security have been ongoing challenge for public and private organizations (NIST, 2016; Padayachee, 2016). As insider threats increase in this era of fast communications, it is important to uncover the reasons and motivators for insider threats in organizations (Green, 2014). I presented real-time security countermeasures used by SMEs that, when utilized in the workplace, these may prevent insider threats' toxic behaviors and data breaches as better access controls are implemented. I applied the conceptual framework of the dark triad theory to help understand what makes insiders turn against their organizations, how insider threats are fostered in organizations, and how to bring to light security strategies that may help shape

attitudes about the security of innovative technologies, data confidentiality, integrity, and accessibility. These findings could generate early interventions to prevent insider threats' toxic behaviors and data breaches in public and private organizations.

I used a qualitative Delphi study to gather consensus from 25 IT SMEs in the Washington metropolitan area about reasons and motivators for insider threats, and what real-time strategies, policies, and procedures they used to manage insider threats and data security in public and private organizations. These SMEs possessed at least 5 years of experience in an IT position managing security, information systems, cybersecurity, and risk management, as stated in their LinkedIn professional profiles and as required to achieve their certifications. I selected a Delphi study because it was suitable to develop a deeper knowledge and understanding of the topic and to uncover real-time experiences and lessons learned from SMEs, and I used three rounds of surveys (Marshall & Rossman, 2016; Yin, 2014).

The Round 1 open-ended survey questions addressed reasons and motivators for insider threats in public and private organizations, strategies and and early interventions used in participants' organizations for data breaches and insider threats, and what policies and procedures could be used to manage insider threats and protect data. The responses from the Round 1 survey open-ended questions were used to establish the closed-ended questions for the Round 2 survey. In this qualitative study, the 25 SMEs' level of agreement for reaching consensus was achieved when at least 60% of them agreed, strongly agreed, and the combined consensus numbers fell in the *agree*, or *strongly agree* range of the 5-point Likert-type scale used in this study (Habibi et al., 2015).

Cleary et al. (2014) noted the importance of gaining qualitative data from individuals that could provide potential for exploring a topic in depth within the boundaries of an interpretative, or conceptual framework, or even perspectives. The findings in this study stemmed from the SMEs' experiences with insider threats, and these may be useful in raising awareness among individuals and organizations about insider threats' identifiable traits and behaviors as depicted by the dark triad theory (Cope, 2013; Habibi et al., 2015).

The findings in this Delphi study may be valuable to readers, scholars, and researchers looking to learn more about insider threats, data security, and the dark triad theory because they are representative of the security tools, and approaches that SMEs use in public, and private organizations. Further definitions may assist in increasing the reader's understanding of security measures, and protocols.

Definitions

The following section contains definitions of terms used in the current study. A glossary appears in Appendix A.

Access: Access is the ability to gain entry to a location, and make use of any assets, systems, resources, and information (NIST, 2016).

Big data: 'Big data' are extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior, and interactions. Big data offer the potential to collect large amounts of documents gathered from various sources (Hashem et al., 2015; NIST, 2016).

Breach: A breach is an unauthorized disclosure of classified, or unclassified information (NIST, 2016).

Cyber: Cyber refers to internet-related technology offering deliberate actions to alter, disrupt, deceive, degrade, or destroy (NIST, 2016).

Data security management: Data security management is the prevention of data loss, or integrity resulting from the exposure of proprietary, sensitive, or classified information, either through a voluntary, or involuntary data leakage, or unauthorized data access (NIST, 2016).

Insider: An insider is any person with authorized access to any department, or agency resources to include personnel, facilities, information, equipment, networks, or systems (NIST, 2016).

Insider threat: Insider threat refers to the threat that an insider will use authorized access, wittingly ,or unwittingly, to do harm to the security of the United States through the unauthorized disclosure of information, or through the loss, or degradation of departmental resources, or capabilities (Center for Development of Security Excellence, n.d.).

Subject matter expert (SME): A SME is a person with bona fide expert knowledge about what it takes to do a job. For this study, SMEs included first-level supervisors, managers, directors, and incumbent supervisors who could capture the key requirements of a position and provide multiple points of view on the criticality of the tasks and competencies (U.S. Office of Personnel Management [OPM], 2020).

Assumptions

General assumptions implied in this study included factors and observed behaviors affecting organizational performance, as well as how information technology professionals viewed job satisfaction and management perceptions (Ghazzawi, 2008; Kurtessis et al., 2015; Maslow, 2012). As a trusted member engages in risky behaviors that affect an organization's systems, networks, data, and reputation, the life of an organization may be at risk. Beebe and Rao's (2010) and Willison and Warkentin's (2013) studies showed that insider threats might exert power by holding authorization and access to an organization. Security breaches affect the financial performance of public and private organizations with factors such as reputation, tangible and intangible assets, and trust issues (Avery & Ranganathan, 2016). Because of the findings in these studies, three primary underlying assumptions were considered in this study.

The first assumption was that the SMEs had experienced situations whereas a trusted member of the team engaged in a risky behavior that led to data breaches, spilling, or similar risks, or rising to positions of power, and that the SMEs' responses on this subject were provided truthfully and in good faith and without the fear of retribution due to the nature and confidentiality of a Delphi study. Second, I assumed that the feedback provided in areas of insider threat behaviors, management, and security strategies was such that it could help students, new researchers, practitioners, and new hires in public and private organizations to raise awareness and to develop better strategies to protect their assets. Third, I assumed that none of the SMEs responding to the survey engaged in insider threat activity. Assuming SMEs' responses could alleviate outcomes and

performance impacts, Avery posited that information on security breaches affects the financial performance of organizations with factors such as reputation, tangible and intangible assets, and trust issues (Avery & Ranganathan, 2016).

Scope and Delimitations

The scope of this study covered insider threats' risky behaviors (i.e., reasons and motivators); best strategies for detection, prevention, and data security management; and policies and procedures to manage insider threats in public and private organizations, as agreed upon by 25 SMEs in the Washington metropolitan area. Insider threats and data security have been an ongoing problem for public and private organizations (NIST, 2016; Padayachee, 2016; Yaseen & Panda, 2011). Ponemon Institute (2017) researchers reported in a 2016 survey that malicious insiders represented 54.4% of all events. In 2016, the Ponemon Institute (2017) survey showed losses with the sum of $3.6 billion. Panetta's (2017) report of disruptive technologies addressed the potential impact of artificial intelligence and all intelligent things in increasing risks and disruptions within a broad industry, opening the door to data vulnerabilities and further opportunities for insider threats in public and private organizations (Garner, 2018).

Due to emerging technologies and industry changes, it is necessary to manage insider threat escalations successfully (NIST, 2016). Therefore, increased awareness about the risky behaviors of insider threats and real-time strategies require subject matter consensus (NIST, 2016). Risky behaviors may manifest as antisocial actions leading to negative consequences in the workplace (Roeser et al., 2016; Spain et al., 2014).

Antisocial behaviors have been identified in insider threats using a dark triad theory categorization; such examples have included famous insider-threat incidents such as those involving Edward Snowden and Chelsea Manning (Azizli et al., 2016; Kaplan & Hecker, 2014). Using a panel of SMEs from public and private organizations including government, contractors, and other industries within the certified IT participant pool could render a cross-sectional discussion of antisocial behaviors, and best practices to identify and control risky behaviors in the workplace; adding new knowledge about best industry strategies to protect data and manage insider threats from a global perspective, rather than from an individualized organizational perspective.

These certified IT SMEs could consist of program/project managers, chief information officers, chief information security officers, security administrators, security and systems analysts, network engineers, software developers, and database and website administrators with a minimum of 5 years of IT and system management experience. My findings in this study may help remind systems and computer users of what is appropriate, or not when accessing websites, using social media, clicking on links, granting access, and ignoring basic computer security activities (such as logging in and out of one's computer and keeping passwords confidential).

In this dissertation, I have included a definition of terms section and a description of the methodology, findings, and conclusions to ensure that readers become familiar with the key topics of the study and to assist with the transferability of knowledge and lessons learned (Hohmann et al., 2018). Houghton et al. (2013) noted that for purposes of transferability, readers must be able to understand a study's findings. Supporting this

understanding has involved a thorough effort on my part to provide detailed information for readers, including methodology, data collection, sample processes, research methods, findings, and summaries, which could provide value to readers' own studies (Houghton et al., 2013).

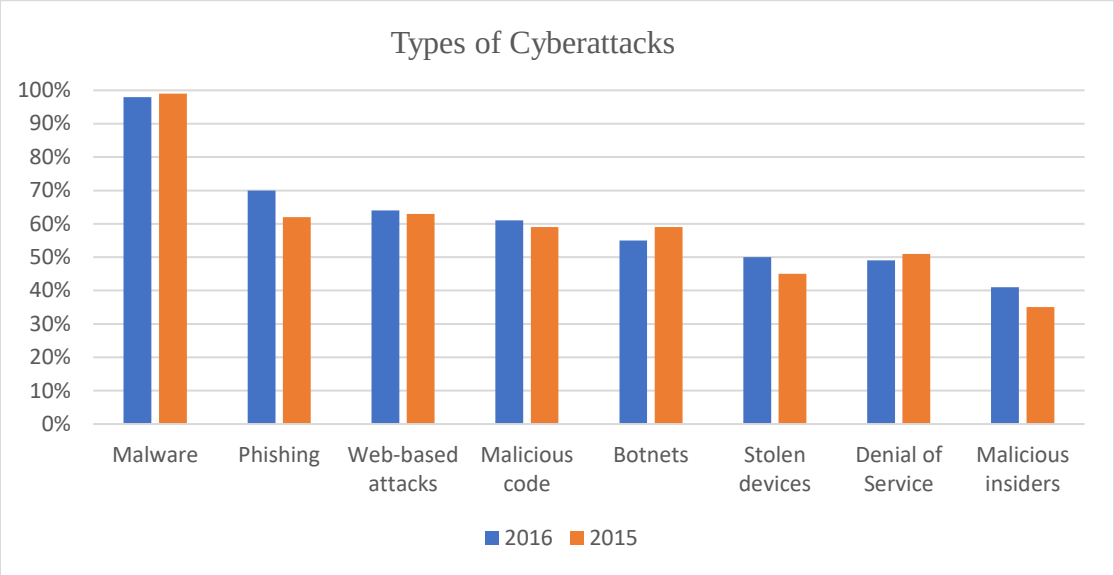
Delimitations of this study include unresolved measures for credibility, or trustworthiness, transferability, dependability, and confirmability for ensuring unbiased qualitative results (Charmaz, 2014; Firmin et al., 2014; Lincoln & Guba, 2000). Specifically, this study addressed strategies for insider threat prevention and data security from the perspective of 25 SMEs. Data analysis included three main categories that contributed to data reduction through consolidation, data display, and data verification (Adler & Clark, 2015). No demographic data were requested from SMEs that might have included race, gender, or national origin. The data gathered were analyzed through categorization and direct interpretation (Yazan, 2015). The findings may lead to better risk detection and data confidentiality, integrity, and accessibility as agreed upon by participating SMEs (Singh, 2014). These findings may also generate early interventions to prevent insider threats' toxic behaviors and data breaches.

Significance of the Study

This Delphi study was conducted to provide an opportunity to contribute to the body of knowledge in the IT field and increase awareness about insider threats' risky behaviors and new security strategies. The participation of a panel of 25 SMEs from public and private organizations rendered a cross-sectional discussion of best practices, adding new knowledge about industry strategies used by these SMEs to protect data and

manage insider threats viewed from a global perspective, rather than from an individualized organizational perspective. A 2015 Ponemon Institute survey uncovered that an additional 237 organizations experienced data losses resulting from insider threat activity—an increase of 29% relative to the institute's 2013 report (Ponemon Institute, 2017); thus, generating early interventions to prevent insider threats' toxic behaviors and data breaches in the workplace was always a best security practice. This qualitative Delphi method was used to provide SMEs' expert opinions about best security practices on insider threat prevention and identification that could help public and private organizations when developing policies, procedures, and training (NICE, 2016). My conclusions from these findings may contribute to narrowing the gap in the literature on understanding how to effectively recognize and prevent insider threats' activities and risky behaviors, how to implement best industry practices, and what type of new training programs could support professional development and enhance the IT profession. With this study, I may also increase awareness about strategies to identify, detect, and prevent insider threat activities such as the ones identified in Figure 1 in public and private organizations.

Figure 1



Note. From *2017 Cost of Data Breach Study: Global Analysis Benchmark Research*, by Ponemon Institute, 2017. In the Public Domain. (https://www.ncsl.org/documents/taskforces/IBM_Ponemon2017CostofDataBreachStudy.pdf).

SMEs' responses about insider threat prevention could serve to support practitioners in the field and to develop more effective policies and procedures (Ferreira & Otley, 2009; Loeser, 2013). Because researchers conducting quantitative research have focused on the impact of monetary losses, or bottom-line impacts generated by insider threats' actions, rather than the behaviors of those who perpetrated threats, this Delphi study could provide the baseline needed to identify and deter insider threats. The results of this study may also significantly reduce systems failures and occurrences of lost, or stolen confidential information, such as the one experienced by OPM and Equifax Credit Reporting that affected many individuals (Maasberg et al., 2016). A Delphi technique

provides a manager with an excellent platform to develop better employee programs that discourage employees from turning against their organizations (Stolfo et al., 2013).

Significance to Practice

Research is required for a variety of purposes, including gaining, or improving subject knowledge, comprehending facts and situations, and developing new skills. Because research is such an important first step in resolving a wide range of personal, professional, educational, and socioeconomic issues, this qualitative Delphi study can be used as a starting point for anyone looking for more information and lessons learned about insider threats that 25 SMEs provided based on their past experiences with insider threats' reasons and motivators, and the strategies, policies, and procedures that they used in public and private organizations. These findings are not intended to be a one-size-fits-all solution for all insider threat behaviors and countermeasures; rather, as the demand for speedier communications grows and newer technologies necessitate quick responses, these findings may become more relevant as the need for faster communications increases and emerging technologies demand expeditious electronic communications for business, education, and other industries, sometimes overlooking the role that security management, training, and access controls play in opening the door to intentional, or unintentional insider threats' mishaps in organizations (NIST, 2016).

Because insider threat activities continue to disrupt productivity in public and private organizations, and because awareness of the reasons and motivators for insider threats as viewed by the 25 participating SMEs can alleviate some of the cultural issues often overlooked during a process, this Delphi study may be useful to program managers,

project managers, IT practitioners, researchers, and students. Several quantitative surveys, such as those of the Ponemon Institute (2017), the Deloitte (2013) TMT Survey Security findings, and the PricewaterhouseCoopers (PwC, 2020) survey, have been introduced to show how insider threats continue to grow and be a challenge for IT managers. These surveys heavily focus on the financial impact of data losses, not the reasons and motivators for insider threats and what opportunities social media and social engineering provide employees for facilitating data breaches (Hashem et al., 2015). Insider breaches are user centric; therefore, continuous monitoring and controls are needed for early interventions (Glasser & Lindauer, 2013). The real-time feedback and consensus of the SMEs resulted in helpful identifiers, methods, and controls for managing insider risks and data breaches in private and public organizations.

Significance to Theory

This qualitative Delphi study included a unique perspective from SMEs in understanding real-time preventive strategies and controls to identify and decrease insider threat behaviors and data breaches in public and private organizations. This research was enhanced by the application of the dark triad theory as the conceptual framework to develop new insights into real-time traits and behaviors that could provide new opportunities to enhance the body of knowledge and the profession. The feedback that I received from SMEs may lead to better deterrence strategies and improved recruitment and training practices (Greitzer et al., 2013; NIST, 2016). Limited qualitative research existed that could explain why information technology practitioners turned against their

organizations and allowed cyber compromises and breaches to network systems (Stolfo et al., 2013).

While the proposed relationship between the dark triad personality traits, related constructs, and external process antecedents was derived from past literature, further empirical research was needed (Maasberg et al., 2016). The results of this qualitative Delphi study could help clarify issues that affect IT practitioners, researchers, and new employees, helping organizations increase their return on investment by preventing data breaches and increasing employee morale and retention, hence diminishing a lack of loyalty and costly departures. Pinder noted that there is a link between employee loyalty, commitment, and turnovers (Parker, 2008; Pinder, 2008). Employee departures can leave an organization vulnerable to threats and breaches in system management (Evans & Reeder, 2010; Kramer et al., 2011; Mahoney, 2011).

Significance to Social Change

Social change occurs when employees feel empowered, work in a risk-free environment, and are trusted and valued by their employers (Project Management Institute [PMI], 2015). Historically, organizations with good countermeasures had less stressful environments, along with higher employee morale and retention, thus facilitating positive social change (NIST, 2016). Knowledge sharing and industry best security practices are essential to the survival of organizations (NIST, 2016). Upon this foundation, the prevention of insider threats and misuse of organizational assets could benefit from a real-time deeper understanding of the role that corporate behaviors, training, best industry practices, and employee buy-in have in improving data security

countermeasures and preventing insider threats in organization. This Delphi study's findings can be used for transferable approaches to raise awareness about the importance of employee security training and development and to sustain safer environments, as agreed upon by 25 SMEs in public and private organizations.

In the literature review, case studies provided a historical review of the similarities and differences between prior psychological research on insider threats' activities and behaviors (Baughman et al., 2014); therefore, the social change implications of this study may be that, as systems and cybersecurity threats and attacks become more frequent and sophisticated, a greater awareness may be created about the relevance of security training programs and knowledge sharing as a perspective for the survival of public and private organizations (Baughman et al., 2014). Upon this foundation, risk management frameworks could become a prime function in the prevention of intrusions, identity theft, and misuse of organizational assets (Hampton, 2009).

Many quantitative studies' researchers have focused on lack of technological innovations as an excuse for insider threats. However, less has been written about how insider threats are grown in public and private organizations, and the role that managers and culture play as enablers of insider threats (Hoffmann et al., 2012). The SMEs' consensus presented in this Delphi study could support the implementation and development of training programs that could lead to professional development and employee recognition, thus enhancing positive social change that supports the organization.

Summary and Transition

The value of safeguarding sensitive assets in public and private organizations by maintaining data integrity and developing policies and procedures that address emerging technologies and cyber security were critical aspects of this study (NIST, 2016). As a result, countermeasures that 25 SMEs in the Washington metropolitan area used in their day-to-day operations to protect their data were uncovered in this Delphi study. In Chapter 1, I gave an introduction of the study, including the background, problem statement, purpose, research questions, conceptual framework, nature of the study, concepts, assumptions, scope, delimitations, and significance of the study to practice, theory, and social change. The 25 IT SMEs who took part in this study provided real-time data, strategies, and impartial opinions about the effect of emerging technologies on untrained, or disgruntled workers, all while remaining anonymous thanks to the SurveyMonkey electronic tool. In Chapter 2, I present a comprehensive literature review to support the need for this study, as well as the main impacts of insider attacks and the effects of risky employee behaviors on data security management.

Chapter 2: Literature Review

Insider threats and data security have been an ongoing problem for public and private organizations (NIST, 2016; Padayachee, 2016). As insider threats increase in this era of fast communications, it was important to discover the reasons and motivators of insider threats in the workplace, as new security protocols and real-time strategies were required to be developed to quickly address the operational risks that were introduced with innovative technologies (Green, 2014). The general problem is that insider threats' activities lead to data breaches in public and private organizations (Greitzer et al., 2013; Hampton et al., 2014; NIST, 2016; Ponemon Institute, 2017; Rosenfeld et al., 2012; Sokolowski et al., 2016).

The increasing use of IT systems has led public and private organizations to look for new security strategies and controls during the implementation of innovative technologies (NIST, 2016). Countermeasures, policies, training, and strategies needed to prevent insider threats are underrepresented in the present literature, that primarily focuses on the quantitative (financial) aspects of losses resulting from insider threats (Department of Homeland Security [DHS], 2013, NIST, 2016). The awareness needed to identify and decrease insider threat opportunities in public and private organizations during systems innovations and upgrades could be achieved through training and risk awareness efforts that could generate early interventions to prevent insider threats' toxic behaviors and data breaches in schools and businesses (Spector et al., 2005).

The findings from this Delphi study provide real-time strategies and best industry practices and may create greater awareness of the employee behaviors representing

known and unknown risks to society; these findings could facilitate early interventions to prevent insider threats' toxic behaviors and data breaches (Abdallah & Gheyas, 2016; Amigorena, 2014; Ponemon, 2017).

The dark triad theory's constructs may aid in the development of a conceptual framework for classifying the risky behaviors and activities that the SMEs defined as predisposing certain employees to commit data security breaches, that had not been discussed in recent literature. Insider threat theories and best business cybersecurity practices are supported and facilitated by the following areas: employee and management perceptions, innovative technologies, the role of security awareness and training, best industry practices, risk management frameworks, and federal mandates, as introduced in this chapter.

Literature Search Strategy

The tools and databases that I used for this review included the Walden University Library, Google Scholar, JSTOR, ScienceDirect, ProQuest, Wiley, and libraries. Additional materials included the Federal Information System Management Act (FISMA), NIST, and Department of Defense-approved manuals for cyber detection, prevention, and correction. The method for identifying newly published journal articles included a Boolean approach. The search for relevant materials included keywords included in the definitions noted in Chapter 1, such as *access*, *classified information*, *compromise*, *employee*, *insider*, *insider threats*, *security*, and *unauthorized disclosure*. In addition to these main categories, articles specifically related to references and definitions concerning areas such as cybersecurity, information technology/systems, cybercrime,

computer security, and risk management underwent another Boolean search for clarifications throughout the study and as feedback was received from the responses to the surveys.

A literature review aids in gaining a deeper understanding of a topic under investigation and provides readers with a better understanding of the nature and breadth of the analysis (Torraco, 2005). I carefully examined the breadth of insider threats literature reviews, several case studies, and the general population at the beginning of this process. According to Torraco (2005), the scope of the literature review, the number of studies, and the general population are often analyzed at this stage. French et al. (2002) noted that a reviewed subject and conclusions could ground a study and provide a deeper understanding of areas of a research study. My primary objective for the literature review strategy was to provide supporting data and evidence of the need for new and updated strategies to prevent insider threats in public and private organizations and present viable actions to increase individual and organizational awareness. Ninety percent of the literature cited in this review was published within the last 5 to 7 years, with the remaining 10% representing older publications needed to explain the history of IT and insider threats in their early beginnings.

Conceptual Framework

The dark triad theory has been used to assess key features and sources of information regarding the motivations of insider threats as depicted by Abdallah and Gheyas (2016). Insider threats' core features, such as callousness, disagreeableness, and interpersonal exploitation, were previously tested constructs of the dark triad theory

traits, that is, Machiavellianism, psychopathy, and narcissism (Figueredo et al., 2015; Hodson et al., 2009). Recent findings in the psychology field have identified traits such as self-serving behaviors and a life strategy for immediate gratification and risk-taking behaviors as traceable to insider threats' traits and the dark triad (Spain et al., 2014).

Maasberg et al. (2016) noted that dark triad personality traits could be traced to the insider threat cases of individuals such as Brian Regan, Robert Hansen, Aldrich Ames, Ryan Anderson, Ronald Hoffmann, and Michael Penn. Table 1 provides traceable examples of insider threats and dark triad traits depicting an unusual need for attention, a sense of entitlement above the rules, arrogance and compensatory behaviors for self-esteem, lack of impulse control, lack of conscience, and a chronic history of disobeying the rules and organizational policies as being shared by most individuals (Maasberg et al., 2016).

Table 1

Insider Threat Cases and Dark Triad Personality Traits

Dark triad personality characteristics in insider threat cases	Brian Regan	Robert Hanssen	Ames Aldrich	Ryan Anderson	Ronald Hoffmann
Unusual need for attention	x	x	x	x	x
Sense of entitlement/above the rules	x	x	x	x	x
Arrogance	x	x	x	x	x
Compensatory behaviors for self-esteem	x	x	x	x	x
(Lack of impulse control					
Lack of conscience)					
Chronic rule violations as in sociopathy	x	x	x	x	

Note. From "Law Enforcement Enterprise Portal (LEEP)," by Federal Bureau of Investigation, 2016 (https://www.fbi.gov/services/cjis/leep). In the Public Domain.

Literature Review Related to the Concept of the Dark Triad

Table 1, drawn from the FBI 2016 Internet Crime Report, depicts famous insider threat cases that align with characteristics of the dark triad personality traits. For example, former Master Sergeant Brian Regan, a father of four, was an Air Force retiree who worked as a contractor for TRW at the National Reconnaissance Office (NRO) in Chantilly, Virginia. Former MSgt Regan had accrued over $117,000 in credit card debt and was said to be paranoid about the future. He sold secrets to Libya and China until

finally arrested by FBI agents at Dulles International Airport for stealing classified materials from the NRO (FBI, 2016b). Regan showed compensatory behaviors for low self-esteem due to his dyslexia. He also lacked impulse control, showing symptoms of paranoia (Maasberg et al., 2016).

FBI Special Agent Robert Hanssen had authorized access to a multitude of national security data. He voluntarily provided information to the former Soviet Union and Russia. Because of his assignments within the FBI, Hanssen gained access to some of the most sensitive and highly classified information in the U.S. government. For his espionage, Hanssen received over $600,000 (FBI, 2016d). Insider threat Hanssen showed an unusual need for attention, a sense of entitlement, arrogance, and a lack of conscience, or sociopathy (Jordan et al., 2016; Maasberg et al., 2016).

CIA 31-year veteran Ames Aldrich was a case officer who was fluent in Russian and an expert in foreign intelligence. He spied for Russia from 1985 until the day of his arrest in February 1994. Like the previous insider threats, Aldrich had accumulated excessive debt and lived beyond his means. He was paid over $1.88 million for his treason (FBI, 2016a). Aldrich showed arrogance, greed, and financial need that transferred to a sense of entitlement by selling national security secrets; he also showed a lack of conscience (Maasberg et al., 2016).

Former Private First Class (Pfc). Ryan Anderson, an Everett native, and Washington National Guardsman, wanted to defect from the United States to join al-Qaida, train its members, and conduct terrorist attacks against the United States (Poe, 2011). For his efforts, he was arrested by FBI Agents while still on duty at Joint Base

Lewis-McCord. While on duty, Anderson displayed a sense of entitlement and compensatory behaviors to increase his self-esteem; he displayed chronic rule violations with a disregard for military life in general and his open desire to join forces with al-Qaida (Maasberg et al., 2016).

A former sailor with a top-secret clearance and a job dealing with sensitive information in the Navy, Robert Hoffmann had achieved great exposure to information on U.S. nuclear fleets and operations that he was willing and able to sell to the enemy. Hoffmann was disgruntled and resentful toward the Navy. Hoffmann blamed the Navy for his divorce and lack of career advancement. Near his retirement in 2011, Hoffmann attempted to divulge top secret national defense information. His efforts fell short, and he was arrested and found guilty of espionage in 2013 (FBI, 2017). Hoffmann demonstrated an unusual need for attention and a sense of entitlement above the rules; he was also arrogant and lacked mindfulness (Maasberg et al., 2016).

Insider threats are not exclusively attributed to men. In 2001, Ana Montes, a highly respected former senior analyst with the Defense Intelligence Agency assigned to translate and analyze data from Cuba, whose family tree extended to siblings working for the FBI, was arrested in Washington, DC for providing classified information about intelligence, military strategies, and other sensitive operations to the Cuban government (Carmichael, 2007; Tucker, 2002). Montes's treason was ideological, as she demonstrated during her sentencing, where she unapologetically stated, "I obeyed my conscience rather than the law" (Tucker, 2002). Because of Montes's risky behaviors and disregard for national security policy, four American undercover agents lost their lives in

Cuba. Montes's behaviors can be construed as above the rules, lacking mindfulness, and psychopathic, as described by Maasberg in relation to insider threat cases and dark triad personality traits (Goodboy & Martin, 2015).

Unhappy, or unengaged employees may develop risky behaviors consistent with the character traits posed by the dark triad theory (Maasberg et al., 2016). Mahoney (2011) contended that there is a link between employee loyalty, commitment, and turnover that can leave an organization vulnerable to threats and data breaches, that may be linked to employee behaviors, perceptions, and buy-in. A lack of work continuity, training, and familiarity with organizational policies are also identifiable factors for facilitating insider threats in public and private organizations (Evans & Reeder, 2010; Mahoney, 2011; Pinder, 2008). Gelles et al.'s (2012) survey identified the most common behaviors that insider threats exhibit as including public and private disclosures, violent behaviors when addressing a problem, social media leaks, and a lack of compliance with security practices. Social media access, workforce demographics, and changes in computing and networking have been identified as the most motivating factors (Gelles et al., 2012). As stated earlier, innovative technologies may open the door to intentional, or unintentional insider breaches due to a lack of training, privacy, security, and institutional knowledge (Brenner, 2010; NIST, 2016).

The dark triad theory is used for interest alignment and relational distance to measure self-interests, corporate interest alignment, and social interactions (Gottschalg & Zollo, 2007). In the cases of insider threats presented above, motivations were the driving force behind risky behaviors and betrayals, regardless of whether these were for financial,

ideological, or religious reasons, or whether they were purely the result of retributive and manipulative personalities. Social dominance, power, and authority have been considered as leading drivers of the dark triad constructs (Burris et al., 2013).

Machiavellianism is considered a manipulative personality characteristic that reflects relational strategies marked by self-interest, deception, and manipulation (Baughman et al., 2014; Paulhus & Williams, 2002). Jakobwitz and Egan (2006) noted that Machiavellianism has been represented by manipulative personalities, self-interest, deception, and manipulation. Narcissism, a form of a clinical personality disorder, presents the elements of grandiosity, entitlement, dominance, and superiority (Azizli et al., 2016; Jakobwitz & Egan, 2006).

Individuals displaying narcissism have an inflated self-view and focus on themselves (Giammarco & Vernon, 2015). Paulhus and Williams (2002) noted that traits of psychopathy were characterized by arrogant and deceitful personalities, high impulsivity, low empathy, low anxiety, and thrill-seeking behaviors. Traits of Machiavellianism and psychopathy have often been associated with negative creativity, while narcissism has been associated with less fluency and creativity (Jonason et al., 2017). These constructs were tested in two item response theory studies conducted by Persson et al. (2017) and Jonason et al. (2017). The characteristics mentioned have been associated with past examples of insider threats that have included Edward Snowden's 2013 disclosures of the government's extensive surveillance of private citizens' phones and email records (Peterson, 2014; Pew Research Center Project Survey, 2017) and

Chelsey Manning's data security breaches of sensitive and classified information from U.S. military networks (Londoño, 2014).

Data breaches have also occurred at the OPM, the Department of State, the Internal Revenue Service, the Department of Defense, the 2016 Democratic National Convention, and the CIA (Bennett, 2016; Flaherty et al., 2016; Schleifer, 2016). These historical precedents support the need to further investigate insider threats and identify real-time security strategies that could effectively protect data during the deployment of new technology (Talke & Snelders, 2013).

Additional traits and dimensions are applicable to socially malicious behaviors. Adverse personality traits are characterized by observable socially malicious behaviors, such as emotional coldness, duplicity, self-promotion, and aggressiveness (Baughman et al., 2014). Paulhus and Williams (2002) identified three-personality empirical and conceptual overlaps within the known personality traits of the dark triad theory. These traits were neuroticism, Machiavellianism, and psychopathy that are associated with low conscientiousness.

Paulhus and Williams (2002) and Ramsay and Westerlaken (2016) explained in their studies that insider threats shared a sense of entitlement, superiority, privilege, lack of remorse, lack of empathy, and a tendency to exploit others. Jonason et al. (2017) and Persson et al. (2017) found that psychopathy was associated with narcissistic and deceitful attitudes, high impulsivity, low empathy, low anxiety, and thrill-seeking behaviors. Machiavellianism and psychopathy have often been associated with negative creativity, while narcissism has been associated with less fluency and creativity. In their

evaluations of two constructs during the item response theory studies, narcissism, psychopathy, and Machiavellianism were identified as behaviors that portrayed a flexible approach to interpersonal control (Jonason et al., 2017; Persson et al., 2017).

Stolfo et al. (2013) noted that the efforts for controlling unauthorized access to electronic resources and malicious behaviors had been a part of organizations since the creation of electronic systems (Stolfo et al., 2013). This can be evidenced by the Kemmerer and Porras's development of an Intrusion Detection Framework in 1995. Therefore, as technologies change, so should the security strategies of public and public organizations (Stolfo et al., 2013).

Jakobwitz and Egan (2006) noted that Machiavellianism has been represented by manipulative personalities, self-interest, deception, and manipulation. Narcissism, a form of a clinical personality disorder, presents the elements of grandiosity, entitlement, dominance, and superiority (Azizli et al., 2016; Jakobwitz & Egan, 2006). Individuals displaying narcissism have an inflated self-view and focus on themselves (Baughman et al., 2014; Giammarco & Vernon, 2015; Paulhus & Williams, 2002). Organizational and personal online activities that could be affected by the above threats include banking, schools, and universities; e-Commerce, hospitals, the entertaining industry, the IRS, OPM, trade, intelligence, and scientific organizations (NIST, 2016). It was because of the economies of scale and the organizations' dependency on IT system that it becomes crucial for entities and individuals to maintain their information in a confidential, need-to-know, and unaltered manner (Diller & Nuzzolilli, 2012; Harris, 2010). A model defining classes and levels of threat impacts was developed by Rabai et al. (2014). This

comprehensive model accounts for threats that include viruses, computer worms, and even political warfare that were caused by intentional, malicious, outsider's human actions (NIST, 2016). This qualitative study, using a dark triad theory as a conceptual framework, did not address political warfare. On Table 2, I showed levels and types of insider threats' activities and consequences.

In 2017, the Pew Research Center conducted a research study on network and systems, finding out that 49% of the world was connected online, and that an estimated 8.4 billion was connected worldwide via Internet, iPhones, iPads, Laptops and Desktop computers. The greater the connectivity, the greater the risks and concerns about data privacy and insider threats. Failing to maintain a privacy policy affects businesses, and individuals regarding their finances, health information, personal identifiable information, and any other confidential information (Pew Research Center, 2017).

As employees continue to open emails at work from unknown sources and unknown links, and visit social networking websites, organizations would be at risk of phishing, spear phishing, whaling and vishing. Each one of these techniques have been associated to social engineering (Meyers, 2018). Phishing is conducted via email across large audiences, spear-phishing targets an individual. Whaling targets high-value targets, such as executives. Vishing uses telephones to attract its victims (Information Assurance Support Environment, 2013; Panetta, 2017).

Table 2

Levels of Threat Impacts

Types of insider threats' activities and consequences		
Malicious	Unintentional	Intentional
	Corruption of information	Destruction of information
	Theft, loss of information	Corruption of information (viruses)
	Illegal usage	Theft, loss of information
	Disclosure of information	Illegal usage
	Denial of use	Disclosure of information
	Elevation of privilege	Elevation of privilege
	Destruction of information	Denial of usage
Nonmalicious	Unintentional	Intentional
	Corruption of information, theft, illegal use	Destruction of information, corruption, loss
	Disclosure/destruction	Illegal usage
	Denial of use	Disclosure of information

Note. From "Classification of Security Threats in Information Systems," by B. A. Rabai, M. L. Jouini, B. Aissa, and A. Milli, 2014, *Journal of King Saud University—Computer and Information Sciences*, *25*(1), p. 493. (https://doi.org/11.0016/j.jksuci.2012.06.002).

The National Institute of Standards and Technology (2016) has emphasized the need for real-time security standards and best practices that address interoperability, usability, and privacy during emerging technologies, and this continues to be a critical goal for the public and private sectors (NIST, 2016; Panetta, 2017). Innovative technologies such as the Cloud, Big data, mobile technologies, social media, and Websites needed to expedite communications were likely to deliver new risks and vulnerabilities during the implementations phase and thereafter (Claycomb & Nicoll, 2012). Likewise, telecommuting, and remote access create a boundary-less system that can facilitate unauthorized access. Managers in public and private organizations that are not cognizant of the need to train, develop and value their employees could fall victims of disgruntled employees and insider threats' actions (Castellion & Markham, 2013). Insider threats' actions can generate low loyalties and high turnover in public and private organizations that can affect working environments, data management, and security, widening the costly gap between employee coercive behaviors and organizational performance (Figueredo et al., 2015).

New employees who lack the expertise to identify and manage threats could heighten the impact of risks, insider threats and financial loses (Dinev & Hu, 2007; Assante & Tobey, 2011; NIST, 2016). Public and private organizations that experience high turnover lose money and time getting new employees indoctrinated, trained and knowledgeable of policies and procedures to secure a compliant environment (Anderson & Moore, 2006; Ghazzawi, 2010). Other issues enabling an increment of unintentional

insider threats using the internet and computers may be the result of skilled IT staff (NIST, 2016).

As more threats were introduced to the systems, the appearance of hackers accessing systems without authorization were enabled by employees accessing links and the internet (NIST, 2016). As external threats were welcomed in by insiders, they exploit the speed, convenience, and anonymity of the Internet to commit a range of damages to individuals and organizations worldwide (NIST, 2016). These damages can be exemplified by impersonations, crimes such as child pornography using somebody else's credentials and financial gain. It was important to introduce a footnote into external threats because they represent the second element of systems breaches, as insider threats facilitate their entry into organizations. The Federal Information System Management Act (FISMA) of 2002 designated the National Institute of Standards and Technology (NIST) to develop standards and guidelines necessary to build risk management frameworks and security controls for the prevention of cyber attacks and insider threats (NIST, 2016).

Benefits of the Dark Triad Theory

The Ajzen's theory of planned behavior was representative of associations among Machiavellianism, narcissism, and psychopathy, as predicted in the dark triad theory (Zhao et al., 2016). The Ajzen's theory using the dark triad theory was proven beneficial when analyzing tendencies for corruption in a series of studies using hypotheses about corruption and beliefs (Bai et al., 2014; Zhao et al., 2016). The author concluded that the dark triad personality behaviors positively predicted bribe-offering and bribe-taking

intentions (Zhao et al., 2016). The study findings associated traits such as Narcissism and psychopathy with the belief that one could get away with wrongdoing without suffering the consequences. This research is important because it examines the theoretical and functional effects of the dark triad personality traits, as well as why individuals participate in crime despite the consequences. The reasons may vary for those depicting innate dark triad antisocial traits and those seeking monetary rewards. Cybersecurity was defined as the state of protecting business assets, data, and systems against criminal, or unauthorized use, and the security measures were taken to achieve this effort (ISACA. https://www.isaca.org). Some of the insider threat opportunities occur while accessing websites, opening links, and connecting with social media. External hackers and unauthorized users could look for potential loopholes to access passwords, personal information, identity theft, financial information, health records and other sensitive data to damage a system, ruin an organization's reputation, or gain financial rewards by disclosing trade secrets, confidential and classified information to third parties (NIST, 2016). According to Verizon's 2016 Data Breach Incident Report, 30% of 2015 security incidents were caused by a lack of employee preparation and knowledge of the organization's best cybersecurity practices.

Insider Threats Discussion

Insider threats perpetrate unauthorized access activities leading to fraud, theft, and data sabotage (Rabai et al., 2014). Insider threats are not new to the industry (NIST, 2016; Padayachee, 2016; Stalla-Bourdillon et al., 2014). Early efforts for data access controls can be traced to the Kemmerer and Porras's Intrusion Detection Framework

developed in 1995 for handling unauthorized computer access. Historically, people have played a key role in the execution of data management activities (Stalla-Bourdillon et al., 2014). For this reason, intentional, or unintentional damage to data systems has been attributed to new, untrained, disgruntled employees, or to those seeking financial rewards and recognition (NIST, 2016; Posey et al., 2011).

The impact of innovations and emerging technologies has given rise to some of the *enablers* of insider threats in public and private organizations, increased by the ability to interact in social media activities leading to spear-phishing and social engineering that raise the level of data vulnerabilities through a lack of employee security awareness, cybersecurity training, and password protection utilization, or by using poorly configured and patched devices (Information Assurance Support Environment, 2013; Panetta, 2017).

Data leakage can easily occur via social networking, and accidental disclosure, or loss of information and, or company equipment (Spitzner, 2013a. Through the art of "Phishing," or 'the act of obtaining personal information directly from the user through the Internet' (Kaspersky, 2013). Mallery (2009) noted that one important factor in information security implementations was to properly provide training for employees and the development of a security culture within an organization (Mallery, 2009). D'Arcy et al. (2009) established the need for ongoing research on security awareness and noted that current research often refers only to the relationships between security awareness and behavioral intentions indicating the need for studies examining the relationship between the former and the actual information security-related behaviors, that was, compliance with information security policies (Assenza et al., 2019; D'Arcy et al., 2009).

Rabai et al. (2014) classified security threats in information systems, as malicious and not malicious. Within this group, activities affecting security may be intentional, or unintentional (Rabai et al., 2014). Today, employees that telework and those working from disperse locations may present a concern for public and private organizations facing security breaches, and intentional, or unintentional data leaks (NIST, 2016). Malicious, or intentional insider threats were widely recognized as motivated by money, politics, or revenge (Software Engineering Institute (SEI), 2013). However, the Software Information Institute (SEI) noted that unintentional breaches can occur from present and former employees, contractors, or business partners, or anyone who has, or has had authorized access to an organization's network, the system in a myriad of ways (SEI, 2013). However, negligence has been identified as the most common cause for unintentional insider threats according to the Ponemon 2015 survey (The Ponemon Institute: Unintentional Insider Risk in the United States and German Organizations, June 2015). Other instances of unintentional insider threats were identified as accidental disclosures of sensitive information via Internet, improper disposal of records, such as paper documents; and use of devices such as cell phones, laptops and other devices containing confidential information, either lost, or stolen (SEI, 2017; Ponemon, 2017).

Abdallah and Gheyas (2016) developed an insider threat prediction model providing three classifications and domain factors to address insider threats that is a part of this study. Abdallah and Gheyas (2016) noted that this model accounts for the traits observed in the dark triad theory however, these classifications were developed as guidance, and should not be viewed as a panacea for new insider threat activities arising

from innovative technologies (Abdallah & Gheyas, 2016). In this model, the first factor introduces a predisposition to malicious behaviors that may seem to indicate that perpetrators were inclined to disobey laws and regulations and that they have a disregard for authority (Dang, 2014). This behavioral feature was based on evidentiary sources that were linked to past delinquent behaviors (Abdallah & Gheyas, 2016). The second factor in Abdallah and Gheyas (2016) model directs us to problems associated with mental disorders medically diagnosed as depressive behaviors, paranoia, schizophrenia, and bipolarity. In this instance, social networking activities may also provide valuable information about patterns of behavior and personal targets (Papageorgiou et al., 2017).

Abdallah and Gheyas (2016) viewed personality factors such as Narcissism. psychopathy, sociopathy, and neuroticism, like those portrayed in the dark triad theory, using evidentiary sources such as insiders' self-centeredness, social distancing, moral disengagement, and a lack of responsibility for their actions. On Table 3, I depicted a list of behavioral features and evidentiary sources, as stated by Abdallah and Gheyas (2016).

With the advent of innovations and constant changes in information technologies, the risks of telecommuting, and remote access, poorly trained personnel using social networks, may neglect to change, or protect their passwords, or even sign off when stepping away from their laptops and desktop computers (Talke & Snelders, 2013). These practices present a problem for public and private organizations due to the opportunity for free access to their networks and data (NIST, 2016). Reasons for this poor judgment on the part of users have been attributed to a lack of training, security policies and supervisory oversight (Majchrzak & Markus, 2013; NIST, 2016).

The Department of Homeland Security (DHS) stated that Cybersecurity risks and vulnerabilities assimilate diverse approaches. For example: Phishing has been the most effective method due to a mix of user ingenuity and awareness; Hacking consists of gathering identity and data information; Social engineering, or social networking used to gather information via Internet; scanning and enumeration takes advantage of security loopholes in the organization to infiltrate the network and damage systems; BOTS are programmed to obey remote instructions, create spam, and attack target systems, and networks, BYOD (Bring your own Device), represented by any personal iPhones, iPads, or personal computers used in the workplace (Department of Homeland Security, 2013; NIST, 2016).

Table 3

An Insider Prediction Model

Domain factors	Behavior features	Evidentiary sources
predisposition to malicious behavior	predisposition towards legal regulations and authority. Delinquent behavior in the past	social networking sites. Interaction with honeypot files in the honeypots (designed to purposely engage and deceive hackers); past criminal history
mental disorders	paranoia, depression, schizophrenia, bipolarity	clinical diagnoses. Social networking activities
personality factor	narcissism, psychopathy, sociopathy, neuroticism, self-focus, social distancing, moral disengagement, feelings of closeness, perception of punishment.	dark triad theory language, email communication patterns, website visit pattern, the temporal pattern of online and PC usage, online behavior. Insider communication, and a number of social media website visits.

Note. From "Detection and Prediction of Insider Threats to Cybersecurity: A Systematic Literature Review and Meta-Analysis," by A. E. Abdallah and I. A. Gheyas, 2016, *Big Data Analytics, 1,* Article 6 (https://doi.org/11.0186/s41044-016-0006-0). In the Public Domain.

Hewlett Packard conducted a study where 97% of employee devices contained private information, 75% did not have enough data encryption presenting a risk and vulnerability Escalation and misuse of employee privileges due to improper logins, and password resetting has been generated by a lack of adherence to policies and procedures. Employee-generated risks and vulnerabilities were the subject of the National Initiative for Cybersecurity Education (NICE) workshop sponsored by NIST in Gaithersburg, MD during the week of November 13-18, 2017. The mission of NICE was to facilitate and sustain an active network to promote education, training, and workforce development. NICE's educational initiatives support the practice of protecting the confidentiality, integrity, and accessibility of data systems that could become essential to corporate and individual performance (NICE, 2016).

The National Institute of Standards and Technology has identified several reasons for insider threats' motivation, this study; however, did not cover acts of terrorism, war, and political motivations. Past examples of insider threats have included leaks from Edward Snowden, and Bradley Manning, whose name subsequently changed to Chelsey Manning (Londoño, 2014; Bennett, 2016; Schleifer & Scott, 2016). Data breaches into the Office of Personnel Management, the Department of State, the Internal Revenue System, Department of Defense, the Democratic National Convention (Flaherty et al., 2016); the CIA, and Equifax (www.equifax.com; Flaherty et al., 2016). These patterns of behavior create a need for real-time strategies that could be applied to new training and development activities. Given the iterative nature of innovative technologies, a greater awareness about what risks and vulnerabilities were most prevalent in the IT community

could help thwart insider threats in public and private organizations, or at a minimum assist in the updating and revisions of security policies and standard operating procedures (NIST, 2016).

Computing Technology Advances and Vulnerabilities

The 1970s and 1980s saw the evolution of computing from the Wang, IBM, DELL, ACER, and Macintosh computers to the Microsoft and Apple Computers and processors, providing sophisticated laptops and desktop technologies (Whitworth & Ahnad, 2014). In 1990s Microsoft, created a more personalized approach to computers giving ordinary people tools such as word-processing at home. Soon thereafter, companies such as Google and the World-Wide-Web provided the ultimate access to the Internet. In the early 2000's computing evolved once more to become the social network that we now today with sites such as Facebook, LinkedIn®, Myspace, WhatsApp, and others (Hilbert & Davis, 2015; Whitworth & Ahnad, 2014). These innovations and software programs were created to increase communications and to provide faster, more efficient e-commerce transactions (Avery & Ranganathan, 2016).

The relationship between information systems and human interactions was undeniable, and its mutual influences were parallel with changes in information technology (Niederman et al., 2016). Niederman et al. (2016) also noted that as each technical innovation takes place, a need for new technical skills was born with each innovation creating a surge of requirements for technical skills that could require end users to learn new skills through training and development.

Cloud Computing

Many public and private organizations rely on Cloud computing services, peer-to-peer applications for file sharing, telecommunications, face-to-face conferences, Web portals, and high-bandwidths to conduct business activities. Although the definition of insider threats has had different connotations during pre and post technology innovations, all definitions seem to lead to the conclusion that, these are threats that occur inside the organization, by trusted people.

Therefore, knowing what was needed during systems upgrades, data migration, Cloud implementation and the decommissioning of legacy systems could require clear guidelines and an understanding of how to protect information assets from unauthorized access (Hunton & Norman, 2010; Sanbonmatsu & Strayer, 2013). Several technologies were developed to control breaches and data security in 199; however, I found limited qualitative research in the literature for one of the most dangerous threats, that was, the trusted individual who knows and has access to a privileged and confidential information, and his, or her motives for turning against the organization.

Insider threats can be intentional, or nonintentional (NIST, 2020; Rabai et al., 2014). In the past, most insider threats, or "internal threats" were classified in the context of logistical issues such as systems degradation (e.g., wires, building destruction, fires, water damages, equipment malfunction, information losses, and accidental damage of important files) (NIST, 2016). However, the human element has taken the front seat in separating insider threats from internal threats. An insider threat was a malicious threat to an organization that comes from people within the organization, such as employees,

former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data and computer systems. An internal threat was any failure of the infrastructure, communications, logistics, and IT resources (http://opensecuritytraining.info/CISSPMain_files; Salya & Ravi, 2013).

Salya and Ravi (2013) viewed the overutilization of innovative technologies in the form of web portals, Cloud, peer-to-peer applications, and web portals using high-bandwidth wireless networks as enablers of risks and easily accessible doors for insider threats (Salya & Ravi, 2013). Business in the Cloud, as it was the case of the Amazon Corporation, and many others has become an integral part of most individuals' purchasing options. Market changes and e-Commerce have led public and private organizations to explore with innovative, or cutting-edge technologies to become competitive, or get the best products, or services first (Heilbrun & Brown, 2011; Schubert & Leimstoll, 2007).

Honeypot Technologies

A honeypot is an isolated collection of systems, with the primary purpose to elicit exploitation from attackers either using real, or simulated decoy computer system to determine weaknesses in the system configuration, or passwords' strength (Kuman & Morarjee, 2014; Sastry, 2011). Honeypots were designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet (NIST, 2016; Sastry, 2011). Spitzner's (2013b) research focused on the fact that Honeypot technologies can be used to detect, identify, and gather information on specific threats (NIST, 2016; Spitzner, 2013).

Network-Based Threats

Many network controls exist as one layer of support to protect data. The most prevalent ones include Access by unauthorized persons, this can be internal, or external; however, external access has commonly known to occur due to internal failures. This means that users need to be always authenticated. The act described as Spoofing occurs when the configuration to networks, systems, or devices was affected (NIST, 2016). This happens when outsiders provide credentials to access another person's access. Eavesdropping, occurs when transmissions were intercepted by using someone else's login credentials, e-mail messages, or communications between servers. Malware occurs when an external attacker launches viruses to propagate from system to system (NIST, 2016).

This excessive use of the network can overflow the servers preventing any traffic. Denial of Service (DoS) attack was an attack that causes the system to malfunction, or crash preventing organizations from doing any business. Access Bypass was an individual's ability to attach devices to Wi-Fi, modems, or networks and gain access to the system bypassing security controls. Man-in-the-middle (MITM) attack was used to disrupt communications by impersonating parties and acting as if the communications were legitimate, but instead, these communications were conducted by the MITM (NIST, 2016; Gregory, 2017).

Tracing the source to systems threats is important for public and private organizations because of business continuity (Avery & Ranganathan, 2016). Therefore, having the security of controls that manage access to the systems in the organization was

paired to its survival (NIST, 2016). Kui et al. (2012) noted that not having direct access to the same trusted domain made monitoring threats difficult due to enforcing access control policies of the organization and user levels of access. In case of a potential insider threats' attack, sensitive data might be exposed, leaving the data owner vulnerable (Kui et al., 2012).

Big Data and the Internet of Things

Big Data files are stored in the Cloud and access through the Internet of Things' (IoT) connected devices. As Big Data move to the Cloud, hackers may follow the data (Ziegeldorf et al., 2014). The term Big Data was created to depict how information was received from multiple sources and formats (McAfee & Brynjolfsson, 2012; Walker, 2014). The use of Big Data in several sectors ranges from businesses, national security, science, and the public creating new challenges that require a new level of professional expertise and countermeasures for preventing and managing insider threats' incidents (Nurse, Buckley et al., 2014a; Page, 2015). Claycomb and Nicoll (2012) noted that developing risk management frameworks and security countermeasures while accessing the Cloud's Big Data and social networks may be a greater challenge as faster and quicker systems are developed.

Because the confidentiality, integrity, and accessibility of data are essential when conducting Internet activities, the speed of innovative technologies will call for better and stronger security strategies and more skilled personnel to prevent breaches, intrusions, and vulnerabilities (NIST, 2016). Chen and Zhang (2014) argued that the benefits of Big Data had surpassed the challenges of managing information systems. Some of these

benefits have included increased business opportunities and progress in many evolutionary and scientific fields (Chen & Zhang, 2014). Clark (2016) noted that a code of conduct for information systems should include contributing to the well-being of society to protect the privacy, integrity, and confidentiality of data (Clark, 2016).

The National Initiative for Cyber Education (NICE) noted that managing such innovative technologies could require a new breed of IT professionals possessing the right skills to operate sophisticated IT networks and systems (NICE, 2016). Heilbrun and Brown (2011) viewed IT risks in the form of early deployments of innovative technologies and a lag on training, as enablers of stressful environments where managers were rushed to deploy software and systems without the benefit of appropriate training (Heilbrun & Brown, 2011). This practice increases the likelihood of threats and vulnerabilities to the IT systems in public and private organizations. Poorly planned deployments of IT networks and software allowed for intrusions, denial of services, viruses, and spyware (Moore et al., 2008). Schubert and Leimstoll (2007) and other researchers have noted that virtual and remote teams increase the risks of cyber intrusions because of easy access from friends and family who could be trusted and can easily gain access to social network sites using corporate systems (Hunton & Norman, 2010; Majcrzak, 2013; Schubert & Leimstoll, 2007).

Although IT Managers share the responsibility for securing corporate systems, the data owners, or virtual employees have the ultimate responsibility for using and not sharing passwords, and for logging in and out of the systems while away from the computer (Rabai et al., 2014). The constant use of the Internet to conduct daily activities,

such as online banking, maintain hospital records, make doctors' appointments, attend virtual schools and university classes, shopping, dating, gaming, and even tax reporting creates a significant user dependency on IT systems and networks, making it vital for any organization and individuals to keep this information confidential, accessible, and unaltered (Majchrzak & Markus, 2013; NIST, 2016).

Cappelli et al. (2012) found that employee disgruntlement, or resentment was a recurring theme in IT sabotage cases. Fifty-seven percent (57%) of insiders who committed IT sabotage were disgruntled and often expected certain technical freedoms to have control over their organization's computer and network systems, or expected recognition, or prestige from management that did not occur (Cappelli et al., 2012). Zulkefli and Jemal (2014) noted that insider attacks were facilitated by the same benefits that faster communications can provide. One example was the emergence of Cloud computing that has become very popular with public and private organizations to store their data remotely using a subcontractor as a Cloud service manager. This new outlet has opened the door for increased risks, and security problems, such as contractors guarding the data may not exercise due diligence with the security protocols, or timely backups, the Cloud was borderless, and data may be stored anywhere needed to prevent cyber attacks (NICE, 2016, NIST, 2016).

Private and Public Cloud provides extended services to subscribers; however, this flexibility increases the possibilities that malicious insider attacks may occur to exploit the Cloud Big Data. The exchange for greater flexibility and cost-effectiveness in communications and accessibility could ultimately be costly if public and private

organizations fail to protect the data physically, or if its confidentiality and integrity become compromised (NIST, 2016; Tang et al., 2012). For example, contractors and third parties manage the Cloud. When corporations and individuals store their data in the Cloud, they relinquish their physical control over emails, banking, or financial information, tax returns, and other personal data to the Cloud service provider. Once a data owner places personal information into the Cloud, he, or she may also lose control over the information distribution if hacking, or other data theft actions occur (Tang et al., 2012), for example breaches in Equifax and other reliable service providers (Equifax, 2017).

Sundararajan et al. (2011) noted that clients were often concerned with this loss of control over their data. The main security concerns of clients were a loss of direct control of their data and being forced to trust a third-party provider with safeguarding confidential information. Security threats in the Cloud may consist of malicious system administrators, who pose a serious risk to clients (Sundararajan et al., 2011). Threats to data were not only originated by insider threats; while the latter has been often labeled as responsible for enabling external threats either by giving access, or by not following security policies (NIST, 2016).

Prevention and Detection of Insider Threats

Insider threats are conduits for technological threats because of their physical access to restricted areas, buildings, and any other designated area where software, or hardware can be stored. Salya and Ravi (2013), and NIST (2016) noted that an insider's motivation was linked to personal, professional, religious, political, and cultural goals. In

addition to systems and data management, insider threat crimes include espionage, identity theft, child pornography, and credit card fraud (FBI, 2016c). Unintentional threats are those threats introduced without the insiders' awareness. These threats include the accidental modification of software by corrupting data, programming error, user, or operator error (NIST, 2016; Rabai, Jouini et al., 2014). Rabai Jouini et al. (2014) developed a security system for insider threat classifications for Cloud computing environments that lists the most obvious external threats. Human, natural disasters and logistical threats run alongside external threats (Rabai et al., 2014).

Impact of Breaches

Because of unauthorized access, the security impacts can be described as the destruction of information, corruption of data, theft, or loss of information; disclosure of information, denial of service, user elevation of privileges and identify theft (NIST, 2016; Computer Software and Applications Conference, 2012). Tang, Wang, and Ming (2012) maintained that some of the most severe aspects of insider threat actions were intentional degradation of systems and data, blocking of computer and network resources, and the elevation of user privileges perpetrated through unauthorized password changes and the illegal usage of system functions (Tang et al., 2012).

Maasberg et al. (2016) noted that government and industry initiatives exist to implement security-operating procedures; however, the increasing numbers of insider threat incidents were a concern (Maasberg et al., 2016). Some of these initiatives were regulations, laws, governance, and others industry recommended practices, such as International Standards Organization (ISO) and CMMi designed as guides to achieve data

management security (Maasberg et al., 2016). New types of threats to IT systems appear to be on the rise (Maasberg et al., 2016; Ponemon Institute, 2017). Ayofe and Irwin (2010) noted the benefits that providing education and hands-on training to employees and contractors had on organizational performance. NIST/NICE provides continues education on risk management using the NIST Risk Management Framework (Ayofe & Irwin, 2010; NIST, 2016). Leadership's awareness of the tools and risk management strategies used by industry's SMEs could increase awareness of risk management techniques that could align with the organization's mission (Evans & Reeder, 2010; NIST, 2016).

Rabai et al. (2014) created a model that accounts for most NIST identified security threats and known risks to network systems (Rabai et al., 2014). These findings may facilitate an understanding of the scope and impact of insider threats in public and private organizations. Rabai et al., 2014 argued that this kind of classification was appropriate for organizations adopting large-scale systems where various user levels communicated through public networks (Rabai, Jouini et al., 2014).

Cyber Security Legislation

Cybersecurity initiatives for accessing government data include mandatory laws and regulations under the Federal Information Security Management Act (FISMA) (2002), the Federal Modernization Act (2014), and the Federal Information Technology Reform Act (FITARA) (2014) just to mention a few. Several standards have been developed, such as The Gramm Leach Bliley Act (GLBA) (1999), also known as the Financial Services Modernization Act (1999), and the Payment Card Industry Data

Security Standards (PCI-DSS) (2004) for online payments incorporated in Washington, DC in 2010. These regulations that define requirements that public and private organizations must follow to handle the security of credit card information and the security of IT systems (NIST, 2019).

Also, the ANSi/ASQ quality standards for quality assurance; DoD Series 8500 for employees accessing government networks. FIPS 199 and FIPS 200 for privacy and personal identifiable information, IEE1220 series, ISO; NIST and OMB Circular A-130 and A-123 are mandatory regulations and standards for the government. Private organizations that may be struggling to develop successful strategies to fit technological innovations have been able to benefit from the baselining of such standards to manage security transactions while doing business with the government (FedRamp. https://marketplace.fedramp.gov). The Health Insurance Portability and Accountability Act (HIPAA) (1996) is a framework used to control how public and private organizations share the process and transmit electronic patient health information (ePHI) (Public Law 104-191) (Department of Health and Human Services (HHS). https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html).

Quality standards such as those issued by the International Organization for Standardization (ISO) (2013), and the International Electro-Technical Commission (IEC; 15408-1; 2009), and directives such as Presidential Orders (HSPD-12); guidelines, and policies include the U.S. Homeland Security Presidential Directives (Department of Homeland Security, www.dhs.gov). The Personal Identifiable Information), FIPS-199, or Sensitive Personal Information FIPS-200, were privacy information security mandates.

These mandates were used as standalone, or in conjunction with other security requirements to identify and protect sensitive, proprietary, and personal information (NIST, 2016).

The Department of Homeland Security has developed information security threats and situational awareness training programs that include security, education, training, and awareness (www.dhs.com). One of DHS's training initiatives for dealing with contractors and employees includes the Systems Engineering and Technical Assistance (SETA). The goals of SETA were supportive of guidance to develop knowledge and training related to information security, as provided by the National Institute of Standards and Technology (Gansler et al., 2012). NIST is leading public and private organizations by changing the way organizations view their human and technological assets, changing how organizations manage security, social markets, e-Commerce, acquisitions, and employee relations that require that employees who access government systems be certified by a qualified organization (DoD-8500, DoD 8570 policy series, http: disa.mil/policy). IT audits were covered under the umbrella of FISMA (2002) and the Federal Information Systems Control Audit Management (FISCAM) of 2009. FISCAM provides a methodology for performing information systems control audits of federal entities as provisioned by the General Accounting Office (GAO) Financial Audit Manual (FAM). Other security controls can be observed under the umbrella of Sarbanes-Oxley legislation (SOX) of 2002, for separation of duties (NIST, 2016), that was, funding recipients cannot be the approvers of their own disbursements (Arping & Sautner, 2012).

The Role of the Information Technology Program/Project Manager in Systems Security

IT Managers play a pivotal role in the management and security of network systems. An IT program, or project manager must understand and participate in the acquisitions of information systems in the organization (NIST, 2016). Such was the importance of the IT program/project manager that public and private organizations have budgeted and dedicated entire departments to the management of information systems. Pearlson et al. (2016) noted that possessing the right IT skills for securing network systems was critical to add value to the organization (Pearlson et al., 2016). Drucker et al. (2008) considered the integration of efforts of management and staff to achieve common goals in the organization. This practice continues for IT managers during the information technology innovations and changes, needing to align personnel behaviors with security practices so that security governance and IT compliance could become the norm (Hasib, 2013; NIST, 2016).

The Role of the Leaders in Information Technology

Insider threats are risks to public and private organizations (NIST, 2016). Leadership awareness of the tools and risk management techniques used by industry could help their mission with the protection of data assets necessary to conduct expeditious business, personal and commercial activities (Jerko et al., 2019). eCommerce has created an information-dependent society in the United States and the world (Denis, 2012). The need to buy and own innovative technologies to be competitive needs the support of knowledgeable and willing employees that could safeguard systems

implementations and data access (Bharati & Chaudhury, 2009). Heilbrun and Brown (2011) viewed risks in the form of early deployment of emerging technologies and a lag on training, creating stressful environments whereas managers were rushed to manage threats without the benefit of prior training (Latest Technologies, 2011, Gartner, 2018). Ayofe and Irwin (2010) noted the importance of providing education and hands-on experience to safeguard cybersecurity and increase employee retention (Ayofe, 2010).

The 2011 Latest Technologies survey reported $2.28 million Cybersecurity professionals worldwide and a projected need to increase to $4.2 million in 2015 (Latest Technologies, 2011). Mahoney (2011) noted the need for retaining qualified cyber professionals and the role of training to protect IT infrastructures in the public and private sectors. Latest Technologies researchers (2011), noted the need that organizations had to develop adequate staffing levels, that was, trained and experienced IT professionals. Proficiency for defending cyber attackers requires several years of practice and education to efficiently protect data assets and organizational infrastructures (Hoffmann et al., 2018). Hoffmann et al. (2012) believed that cyber and digital crime could only increase and become more pervasive with time, that was, in the absence of countermeasures (Chang, 2010).

Although IT Managers share the responsibility for securing corporate systems, data owners, or collocated employees could have the ultimate responsibility for using, not sharing their passwords and for logging in and out of the system during absences (Sedighi et al., 2011). Managers in public and private organizations have been more cognizant of the impact that Cybersecurity breaches, internal threats, and vulnerabilities have in their

ability to expand their operational bases safely through their projects' lifecycle (NIST, 2016). Private organizations must maintain security controls to avoid the costly consequences of data breaches (Ciampa, 2010). For example, a private organization may not be able to compete for federal contracts due to a lack of security controls as those required Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a U.S. government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring and controls (Avery & Ranganathan, 2016; FedRAMP, 2017; U.S. General Services Administration (GSA), n.d.).

The Federal Information System Management Act (FISMA) of 2002 has influenced information security, governance and cybersecurity in the government using security frameworks such as the NIST Risk Management Framework (NIST, 2016, Maasberg, 2016). The diffusion of emerging technologies and the commercialization of communications turn the role of information systems into a resource equal in value to the traditionally important resources of property, labor, and capital, according to Drucker's Management Challenges for the Twenty-First Century studies (1993). Nonetheless, Drucker (1993) argued that employees must properly understand the goals of the organization to successfully perform and complete their tasks (2008).

The Deloitte (2012) survey provided results indicating that the trend and speed of innovative technologies will continue as the result of Cloud services, social media, mobile devices, big data, and the Internet of Things (IoT) (Deloitte, 2013). Boss et al. (2009) contended that organizations that do not account for people as a part of

information systems and only gear their investments towards the acquisition of software and hardware were bound to pay the price for not realizing that people, as the weakest link in the information security process could have to be included in the planning and execution phases of innovative technologies to be successful. Deloitte (2012) TMT Global Security Survey findings indicated that the highest number of threats resulted from the adoption of innovative technologies such as the Cloud computing and mobile devices, in addition to threats derived from employee errors, omissions, and abuse of information systems.

What Senior Leadership Needs to Know?

Although variations exist about the risk appetite of public and private organizations and how these translate into policies and procedures for the maintenance of systems, and networks, the advent of the Congress enacted Federal Information Technology Acquisition Act (FITARA) of 2014, has changed how these organizations do business with the government. FITARA through FedRAMP requires that organizations doing business with the government observe the same security guidelines and restrictions for data access, confidentiality, integrity, and accessibility, as their counterparts. FITARA has vested tremendous responsibilities and accountability on the role that the Chief Information Officer (CIO) holds for providing oversight for all IT portfolios, innovations, and changes (FITARA, 2014).

The Federal Information System Management Act (FISMA) of 2002 has influenced information security, governance and cybersecurity in the government using security frameworks such as the NIST Risk Management Framework (NIST, 2016,

Maasberg et al., 2016). Striving a balance between organizational and individual goals may present a challenge during IT implementations because of the way that innovative technologies could affect the employees' working routines and how leadership addresses changes (Denis et al., 2010, 2012).

Ethical Procedures and Data Security

The American Bar Association (2017) affirmed that the ethical rule in information security was the duty to protect the confidentiality of client confidences. The American Psychological Association (2015) also recommended that, while individual practitioners should and do bear the ultimate responsibility for confidentiality and privacy, data storage and communication concerns resulting from poor and/or naïve risk management, it was important that an organization provided constant, up-to-date guidance for practitioners and date users. Because IT departments may work in isolation, opening-up for discussions in a forum such as a Delphi group could increase awareness on how to identify employees who were at high risk for insider threat activities; and develop security policies and standard operating procedures (Abdallah & Gheyas, 2016).

The same was conveyed by FISMA, NIST, and other governance previously mentioned in this study. Innovative technologies and social networking can tempt users to click on links with interesting offers, or those seeming familiar, even when they know it was against organizational policies. This sense of entitlement disregards threats to data stored in the system and information security policy (Bulgurcu et al., 2010). The risks were increased with the utilization of consumer-friendly devices and Cloud computing. Public and private organizations managers providing access from anywhere need to

assure data owners that the confidentiality and integrity of their information is protected to avoid costly lawsuits and damage to their reputations (Nurse et al., 2014b).

Siponen and Iivari (2006) noted that managers have an ethical responsibility for their organizations' IT assets. It was also the responsibility of senior management to protect the organization's assets against involuntary and voluntary harm resulting from employee lack of training, departures, and transfers could be best managed with a knowledgeable workforce (Siponen & Iivari, 2006). Furthermore, a major factor in an employee's decision to stay in an organization may be influenced by the organization's management approach as a key factor in determining the employee's loyalty, and retention (Kuean et al., 2010). In this circumstance, the IT program/project manager's role in delegating and supervising system access becomes critical. The American Bar Association recommended learning from other industries' experiences and lessons learned and to apply industry standards and security frameworks when implementing innovative technologies (ABA Cybersecurity Framework, 2017).

Summary and Conclusions

In Chapter 2, I discussed the increasing problem of insider threats, the research concerning behaviors associated with traits in the dark triad theory; theories, constructs, and concepts formulated for the identification and prevention of insider threats. I also discussed the historical perspective of insider threat classifications, reviewed theoretical and conceptual frameworks that included security awareness, training and the new challenges that innovative technologies present to senior leadership, managers, and users (Assenza et al., 2019). These factors generate a gap for real-time consensus about what to

look for to contain insider threat behaviors, risky actions and how compliance with regulations facilitate innovative technology implementations (Albrechtsen & Hovden, 2010; Adkins, 2015). The findings in this study may shed light on the internal and external factors influencing employee risky behaviors and security practices leading to insider threats in public and private organizations as viewed by the participating SMEs consensus.

In Chapter 3, I provided an overview of the research methodology, design, and rationale, the role of the researcher and the SMEs selection logic; instrumentation, procedures for recruitment using a qualitative Delphi method to illustrate my research methodology, data analysis plan, issues of trustworthiness, ethical procedures, and summary (Hohmann et al., 2018). This study presents an opportunity to narrow the gap in the literature by providing new strategies for managing risks, insider threats, and data breaches as viewed by the SMEs participating in this study. It also presents an opportunity to provide knowledge on areas of threat definition, recognition, avoidance, and individual responsibilities. This study hopes to provide an increased security awareness about insider threat facilitation and prevention and human behaviors under the dark triad theory categories. This study takes the view that SMEs in the field of cybersecurity and data security management were the best-positioned sources to provide new approaches and updated strategies to develop relevant security policies, governance, risk management plans, and employee training and development (NICE, 2016).

Chapter 3: Research Method

The purpose of this qualitative Delphi study was to uncover what real-time consensus existed among 25 IT SMEs in the Washington metropolitan area for managing insider threats and data security in public and private organizations. By identifying real-time reasons and motivators for employees' risky behaviors and insider threat prevention through strategies, policies, and procedures, this study may facilitate early interventions to prevent data breaches (Abdallah & Gheyas, 2016; Amigorena, 2014; Ponemon, 2017). The research methods used to perform the current study are described in this chapter.

In Chapter 3, I outline the research design and rationale for this study, the role of the researcher, SME selection logic, ethics, data collection techniques, analysis, and ethical practices. Also included in this chapter are the logic behind the SMEs' selection, issues of suitability, trustworthiness, and ethics to describe the credibility, transferability, and confirmability of this inquiry. The first section focuses on the research design and rationale, the methodology, and the application of the rationale for employing the dark triad theory as the conceptual framework. Second, the data gathering procedures are provided, as well as information regarding the data. Third, I focus on data analysis for SMEs' consensus and underline the study's operational definitions.

Research Design and Rationale

Billies et al. (2011) noted that the Delphi method is suited to contexts where little academic literature exists, but experiential knowledge is vast. Because one of my goals for this study was to raise awareness and discover the most recent and most successful strategies to prevent insider threats, the information gathered from SMEs using a Delphi method and the dark triad theory conceptual framework may help point to a variety of

human behaviors and security factors for insider threat identification and prevention (Albrechtsen & Hovden, 2010; Kritzinger & Smith, 2008).

The dark triad theory was the conceptual framework of this study for identifying and classifying activities and risky behaviors as viewed by SMEs. Recent qualitative research on data security breaches with a focus on employee behaviors has been lacking in the literature. Instead, research has been heavily focused on insider threats and the impact of financial losses in public and private organizations (Ponemon Institute, 2017). This Delphi study was used to convene a targeted sample, or panel of 25 SMEs in public and private organizations expecting to combine best security practices about innovative technologies, systems management, and strategies for insider threat prevention.

I considered other research methods such as grounded theory and case study, but a Delphi study seemed more suitable to gather real-time information from SMEs on the real-time growing problem of insider threats. Yang et al. (2012) noted that the suitability of a research method such as Delphi is best assessed when it can demonstrate that it is the most suitable approach to address the research problem and answer the research question. Because of the iterative nature of insider threats and the changing requirements for IT professionals, gathering the consensus of SMEs could render better real-time outcomes for identifying toxic employee behaviors, industry best practices, and real-time security countermeasures for data breaches.

In choosing a Delphi method, I was cognizant of the advantages and disadvantages of such a method. In making my final decision, I recognized that the advantages far exceeded the disadvantages of the Delphi method, as I focused on the most relevant aspects of what Joyner and Smith (2015) described as a method that

provides consensus in areas of uncertainty, provides knowledge-sharing opportunities, and presents flexibility and simplicity when using surveys, allowing for freedom of expression, confidentiality, and ease of communications, thus eliminating researcher bias, as there is no face-to-face interaction that could produce likes, dislikes, or favoritism. The anonymity of a survey may open the door to boundaries and cost-effective efforts when compared to face-to-face and phone interviews (Joyner & Smith, 2015).

For this study, I used the Delphi method as the research design. The research rationale for using a qualitative Delphi method with a dark triad conceptual framework was that it allowed a panel of experts to respond in real time, based on their subject matter expertise and the best industry tools and practices that they used in their day-to-day operations (French et al., 2002; Leedy & Ormrod, 2015). Because a Delphi study provides anonymity, SMEs may be able to freely provide feedback without the researcher's influence, or the fear of retribution from their employers (Charmaz, 2014). These real-time findings may help decision makers to plan and assess risks during new hiring, employee departures, and systems access during implementations of innovative technologies, or simply for data security management (NICE, 2017; NIST, 2016). A Delphi method could be useful in the following areas: to develop policy, to develop strategies to address a specific problem, to forecast the future; and to engage in better decision-making processes (Avella, 2016). The 5-point Likert scale classification technique allows SMEs to agree, strongly agree, neither agree nor disagree, disagree, or strongly disagree on a topic. This technique continues to be used to help organize answers in gathering SMEs' consensus findings, or lack thereof (Patton, 2015; Wise, 2015).

This study's survey inquiry for gathering SMEs' data consisted of one overarching question that drove this study and three sub questions, as follows:

RQ1. What is the level of consensus among a panel of SMEs regarding the reasons for insider threats in organizations?

The sub questions included in the study were the following:

SQ1. What are the motivators for insider threats in the workplace?

SQ2. What are the security strategies and early interventions used in organizations to prevent data breaches and insider threats?

SQ3. What policies and procedures can be developed to manage insider threats' access to systems in organizations?

I developed open-ended questions for Round 1 based on the increasing need for qualitative research to demonstrate better prevention and real-time strategies to protect data and identify insider threats' activities and toxic behaviors (Guo, 2013; Hu et al., 2012; NIST, 2016); subsequently, I developed closed-ended questions for Round 2, and upon receipt of Round 2 responses, I developed closed-ended questions for Round 3 that further clarified SMEs' positions and consensus (Habibi et al., 2015). Förster and Von der Gracht (2014) argued that the level of agreement has been a method often used to achieve consensus, that becomes illustrative when used in conjunction with a Likert-type scale.

In this qualitative study, the 25 SMEs' level of agreement for reaching consensus was achieved when at least 60% of them agreed, or strongly agreed, and the combined consensus numbers fell in the *agree*, or *strongly agree* range of the 5-point Likert-type scale used in this study (Habibi et al., 2015). Cleary et al. (2014) noted the importance of

gaining qualitative data from individuals that could provide the potential for exploring a topic in depth within the boundaries of an interpretative, or conceptual framework, or even perspectives. Ultimately, these findings were developed based on SMEs' output and may raise awareness among individuals and organizations about the dark triad theory's identifiable traits and behaviors (Cope, 2013; Habibi et al., 2015).

The feedback from the Round 1 survey provided a baseline of responses for subsequent surveys, as per prior discussion. During this phase, the data gathering process consisted of a laundry list of ideas that were classified and consolidated in an Excel spreadsheet to group a 60% consensus and to develop the Round 2 survey closed-ended questions. At this phase, the goal of Round 1 was not to achieve consensus, because it would have not been realistic, given the magnitude of answers and a lack of maturity in the research process, but also because it would have not followed the guidelines for conducting a Delphi study.

As I gathered raw data on reasons, motivators, strategies, and policies in Round 1, I consolidated similar responses provided by SMEs. For example, money and/or financial gain and revenge, or retaliation were provided simultaneously to depict the reasons (RQ1) and motivators (SQ1) for insider threats in organizations. Other examples, including update software regularly, virus protection, download protection, and using antiviruses such as Bitdefender, were consolidated in one category to depict virus protection. Another consolidation took place for duplicated entries such as limiting access, need to know access, different levels of access, and access controls, under the category for access controls. Lack of knowledge and training were consolidated under training. The same approach was used to present questions about strategies (SQ2) and

policies and procedures (SQ3), that consolidated multiple instances of risk management, and where reference checks and background investigations were used to indicate the same outcome.

For clarity and validation, the questions achieving 60% agreement in Round 1 provided the baseline for questions in the Round 2 survey. The SMEs were asked to make revisions, or validation of the data provided, as follows: "Based on the responses to the first round of interview questions, the following categories were identified by SMEs about insider threats' reasons, motivators … Do you (5) Strongly Agree, (4) Agree, (3) Neutral, (2) Disagree, (1) Strongly disagree?" *Neutral* responses may not have added much value to the research, not that there were any. *Disagree* responses did not yield a minimum of 60%; in fact, the highest rate when it came to religion was 17%, for a motivator of insider threats, as discussed in the study's review. *Strongly disagree* elicited no responses.

The Role of the Researcher

According to my research design and methodology, my role as the researcher consisted of selecting the SME panel, developing the survey questions in SurveyMonkey, submitting the surveys to SMEs, collecting data, categorizing data, analyzing data, developing themes, documenting findings, and maintaining the research schedule. My role also included securing data access and maintaining the highest ethical standards to avoid personal bias, or the perception of unprofessional practices. There were no face-to-face interviews as the design of this Delphi study did not require them. This made it easier to avoid accessibility problems and privacy issues, because many of the SMEs worked on their clients' sites, and many of these sites did not allow visitors, or

interviewing activities. Gaining access could have extended the timelines for data gathering, or jeopardize the data collection (Moustakas, 2015).

Interviews can also put the SME in a difficult position that could defeat the whole purpose of using a Delphi method due to confidentiality issues. Issues of credibility, validity, and reliability are measured against the researcher's knowledge and independence from the SMEs' responses (French et al., 2014). Halpern and Leite (2015) noted that truth, accuracy, transparency, and familiarity of the subjects under study are essential skills in a researcher (Halpern & Leite, 2015). As I observed and assessed the progress of this study, I gathered recent peer-reviewed journals' information on insider threat impacts that might help in understanding security and innovative technologies and/or support the need for additional research on this topic.

My Professional Background

I possess over 30 years of program and project management experience supporting large organizations and the federal government in areas of information assurance, cyber security, FISMA/FISCAM audits, accreditation and certification, and technology business management/capital planning and investment controls. I have achieved several professional certifications such as the Defense Acquisition University's (DAU), Contracting Officer Representative (COR) certification; the Project Management Institute's (PMI), Project Management Professional (PMP), ISACA's Certified in the Governance of Enterprise IT (CGEIT) certification, the Information Technology Infrastructure Library V3 (ITILV3) and ITIL V4 certifications, the Technology Business Management (TBM) Chief Information Officers (CIO) Council's, Certified Technology Business Management Executive (CTBME) certification, and the Scrum Alliance's

Certified Scrum Master (CSM) certification. In addition, I have participated in Delphi studies before. As a federal employee, I held positions as IT project manager, COR, and requisitioner for the intelligence community (IC). As a federal contractor, I performed at the program manager Level III contract labor category, and as a key member of the Cybersecurity Division at one of the largest contracting organizations in the Washington metropolitan area.

As a member of the CIO Council, AFCEA, PMI, and ISACA, I keep abreast with technological changes, IT modernization, and emerging technologies. In that capacity, I may share a similar association and certification status with some SMEs or may possibly share a LinkedIn professional network; however, there has not been any business relationships, or investment participation that could have affected the outcome of these findings.

Having certified members as SMEs was important to me because it added credibility to the study and validated SMEs' knowledge, lessons learned, and positions as industry-recognized experts. Certified SMEs gain status by passing a rigorous 4-hour exam in their field of expertise, having a minimum of 5 years of experience and/or an advanced college degree, and maintaining over 100 hours of continued education (CEU), or risk retaking their certification (ISACA, 2015; PMI, 2015). Participants did not need to use their names when responding to the surveys, as they were coded in the system (Fink, 2000; Habibi et al., 2015; Halpern & Leite, 2015).

Personal Relations, Biases, and Reflexivity

Because I work in environments that use emerging technologies and may share social media connections and training with members of the organizations listed above,

who may or may not be participants in this study, my only personal bias, or favoritism, may be my trust in certified professionals, due to their strict continuing education requirements and my belief that they could provide best IT industry practices. I considered them an elite group. However, the topic of insider threats and the need for better security countermeasures far outweighed my personal consideration for the SMEs participating in this study. The outcomes and responses took a front seat in this journey, far exceeding any personal, or professional consideration.

Personal relations did not present any issues in this study, as the only unforeseen exposure that I could have had with an SME could have been attending a Cybersecurity Summit, PMI evens, or AFCEA Conference. Biases and power relations were not enabled as there were not face-to-face interviews that could have influenced me due to status, culture, or demographics (e.g., race, gender, age, or political status). Visual biases serve as moderators in research, and online surveys do not provide the ability to control cues in people's behaviors, whereas face-to-face interviews can result in rendering judgments easily and before gathering any information (Maddox & Mehta, 2011). In addition to these considerations, I was cognizant of my ethical duty to report accurately and without any influences derived from my own experiences, or personal meaning. Through reflexivity, I was able to use introspection, reflection, intuition, and thinking to channel my strengths and weaknesses (Maslow, 2012; Schneider et al., 2015). Reflecting, intuiting, and thinking are used as primary evidence in qualitative research (Schneider et al., 2015).

Methodology

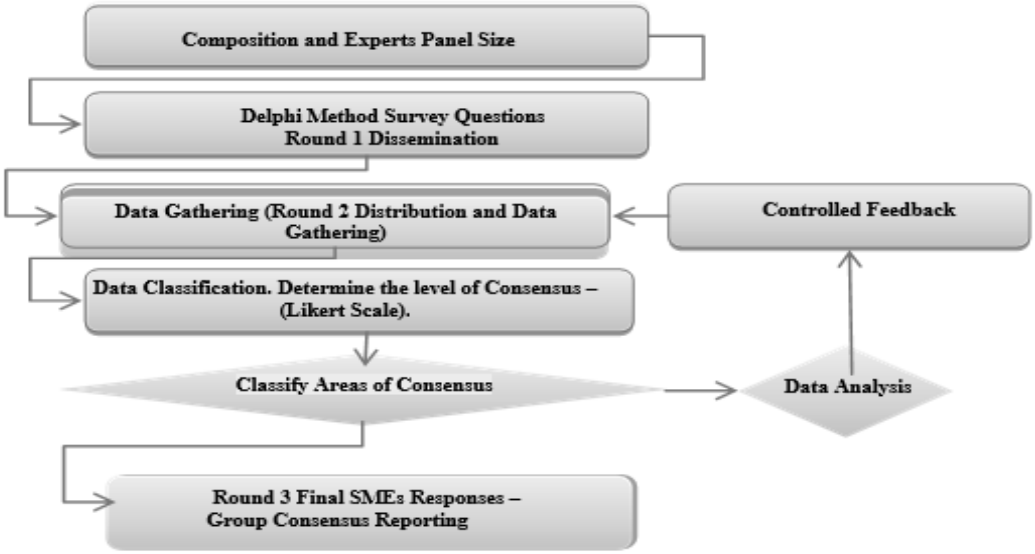
The methodology of a Delphi study was my preferred approach for gathering consensus among SMEs for identifying reasons and motivators for insider threats and risky behaviors in public and private organizations that have become increasingly common with the advent of innovative technologies (Che Ibrahim et al., 2013; Walker, 2012). This Delphi study convened a targeted sample, or panel of 25 SMEs in public and private organizations in the Washington metropolitan area, with the expectation of combining the best security practices and strategies for insider threat management. Applying the conceptual framework of the dark triad theory, I was able to gather reasons, motivators, risky behaviors, social interactions, and security guidelines that served as anchors to classify insider threat behaviors and present options for developing best security strategies and policies that may increase positive outcomes in the workplace. Ludwig (1997) and Nguyen et al. (2013) noted the importance that a Delphi study has for making future predictions; combined with the dark triad, a researcher could introduce a visual analytics system approach and risk framework for insider threat identification, hence reducing systems false threat indicators.

As previously indicated, I used SurveyMonkey to exchange inquiries with 25 certified IT professionals holding IT positions of responsibility in the Washington metropolitan area. I used LinkedIn first, to explore target availability and submit additional information. I administered three surveys in this study; however, a fourth survey was an option, if consensus had not been reached, or if there was a need for further validity. This alternative was noted on the Participants' Consent Form.

The Round 1 survey was submitted in December 2019, receiving a quick 2-week response. I classified SMEs responses to the open-ended questions in the Round 1 survey, using a 5-point Likert-type scale to gather similarities (Wise et al., 2015). Because Round 1 provided similarities on the SMEs responses to the same questions, such as financial gain and money, these responses were consolidated into one category. Then I developed the Round 2 survey, using the information that the SMEs had provided in the open-ended questions in Round 1. The second round of questions provided an opportunity for the SMEs to confirm their previous selections, but also to add additional information. Once Round 2 was sorted out and classified, I developed the final questionnaire for Round 3 that served to confirm and validated SMEs consensus, using 60% *Agree* and *Strongly Agree* ratings as the determinants of consensus. After the three surveys were completed, I shared the findings with the SMEs to ensure that they had an opportunity to comment, make changes, and validate that the surveys had been conducted ethically and in accordance with the original questions, however, I received no subsequent changes. Figure 2 was a composite of the process followed during expert panel composition, survey development, data gathering, classification and final consensus.

Figure 2

Delphi Technique Theoretical Framework



Note. From "Delphi Technique Theoretical Framework in Qualitative Research," by A. Habibi, A. Sarafrazi, and S. Izadyar, 2014, *International Journal of Engineering and Science, 3*(4), p. 13. (https://theijes.com/papers/v3-i4/Version-4/B03404008013.pdf). Adapted with Permission.

Consensus was defined by Skulmoski et al. (2007) as the ability to agree on a subject, or having the majority agreeing, or disagreeing on a subject. In this study, the greater number of *Agree* and *Strongly Agree* answers per questions (i.e., reasons, motivators, type of strategy, policies, procedures) were reflected by the minimum 60% consensus. Although not a quantitative, or mixed study, 60% agreement in this study represents consensus, or the majority totals where SMEs have jointly selected the same options for *Agree* and *Strongly Agree*, or *Disagree* and *Strongly Disagree* (Asselin & Harper, 2014; Habibi, 2014; Vernon, 2009). Contrary to quantitative studies, consensus

can be determined by numbers derived from a mean, or median of responses in the mathematical calculations (Wakefield & Watson, 2014).

During the preparation of the Round 3 survey, I incorporated the closed-ended responses from the Round 2 survey that reached the minimum 60% consensus. The objectives of Round 3 were: (a) to gather additional information to enforce saturation and sufficient consensus through the selection of the same answers; (b) for SMEs to have an opportunity to verify, or change their answers and seek clarification; (c) to use Round 3 as a checkpoint for consensus; and (d) to provide SMEs with opportunities for changes, if they had changed their minds regarding a reason, motive, strategy, policy, or procedure provided in the Round 2 survey responses/findings.

The three Delphi surveys aligned with the problem and purpose statements of this study. These surveys began in December 2019 and concluded in August 2020. Chapter 4 provides the raw data and percentages for each question, an analysis of Rounds 2 and 3 survey responses, a comparison table was presented with explanations, as Round 1 was considered a baseline and a source of free-ranged responses. Responses to Round 1 open-ended questions are addressed under that section (pp. 123-125).

The goal for confidentiality was facilitated by the application of the SurveyMonkey tool. The SurveyMonkey tool's configuration management was standardized to produce consistent options throughout the three surveys. The surveys' cut-off date was automatically set to close upon receipt of 25 completed surveys. Upon receipt of the 25 surveys, I was able to close the surveys. For SMEs' identification, all respondent information (names, e-mail addresses, and custom data) were excluded from the survey results. I set a 5-day reminder notice for those SMEs who had not responded

to the new survey. There were not any IP address restrictions, or blocking of specific IP addresses; that was, a SMEs could take the survey from any computer. However, a "Survey Closed" notice appeared after survey completion. The surveys were password protected to restrict access and maintain the privacy and confidentiality required. Although a feature for sending disqualified respondents to a custom disqualification (URL with an email notification was available, it was not needed and SMEs were able to access their surveys electronically from any location, at their leisure.

Surveys assure privacy, confidentiality, and workable possibilities to complete a functional study (Maxwell, 2013). This qualitative study focused on the discovery of what reasons, motivators and risky behaviors enabled unauthorized access to personal and corporate data creating internal and external threats to individuals and organizations. This Delphi method and dark triad conceptual framework may help systems users to protect their data, and public and private organizations may be able to develop countermeasures and raise awareness regarding toxic and risky behaviors (NIST, 2016).

Participant Selection Logic

I carefully selected a diverse group of SMEs for this study that would reflect the various disciplines in the field of information technology and systems security management. The experts' qualifications for a Delphi panel were critical for the successful outcome of a study and credentials such as certifications in their fields of practice may provide credible, identifiable, and measurable evidence of their expertise (Hasson et al., 2000; PMI, 2015).

The preferred SMEs' selection pool for this study consisted of a purposeful sample of 25 IT certified practitioners, at least 21 years old, working in the Washington

metropolitan area, that was, Maryland, Virginia, and the District of Columbia. Participants who meet the criteria to be called SMEs in a Delphi study meet industry standard criteria from certifying organizations. The logic for this selection was that because these IT practitioners serving as SMEs must have information technology and IT program management certifications, such as IT PM, PMP, CGEIT, CISSP, A+, Security+, CISA, and CISM; and may have responsibilities working as a project manager, database manager, security and/,or system manager, network engineer, chief information officers, chief information security officers, security administrators, security and systems analysts, network engineers, software developers, and database and website administrators, these 25 SMEs meet the criteria to sufficiently provide rich and robust data for reaching saturation (Hancock & Algozzine, 2015). Because these SMEs must follow stringent industry association requirements to maintain active certifications and memberships, and work in the IT environment, they can be considered heterogeneous, their knowledge may provide a quicker saturation for a small number of SMEs given their training and experience on insider threats (Fusch & Ness, 2015; Skulmoski et al., 2007).

Panel Size

I selected a panel size of 25 SMEs with the assumption that the selected sample possessed common characteristics to address the survey questions; that was, they were experts in their field, as can be validated by their active certifications, have at least 5 years of experience in information technology, possess business acumen and accessibility for the researcher. Habibi et al. (2014) noted that a panel size and composition depend on the nature of topics covered, time limitations and money (Habibi et al., 2014). The SMEs

in this study were members of public and private organizations and represented a diverse workforce in the Washington metropolitan area. Given the design of the study, this small Delphi panel was appropriate for purposive sampling (Miles et al., 2014).

Participant Selection Criteria

An expertise screening inquiry took place based on the requirements of this study and the literature review. Certified SME were IT certified and have at least 5 years of experience managing information technology and cybersecurity issues. Industry standards for IT experts include specialized skills and the highest level of experience and training for performing job-related technical tasks (NIST, 2016). Only SMEs holding active industry-certifications, who were at least 21 years old, and have at least 5 years of experience in the IT and cybersecurity fields in the Washington metropolitan area (e.g., D.C., Virginia, and Maryland) were approved to participate in this study. Because certifying organizations have an extensive number of members, recruiting SMEs should not be a risk. This selection criterion represents heterogenous participation, whereas SMEs shared similar backgrounds, experience, training, certifications, and location. Gallego and Bueno (2014) stated that there were two types of expert panels, a heterogeneous, whereas SMEs share similar traits such as gender, culture, age, values, and attitudes, but different levels of knowledge; this study focused on a heterogeneous group that was comprised of SMEs with similar levels of knowledge and expertise in the IT field (Förster & Gracht, 2014).

Instrumentation and Data Collection

The instrument of choice for this study was the electronic survey tool, SurveyMonkey®. The basis for using an electronic survey for collecting data was that

surveys provide an actionable and reliable data access tool that was timely and cost-effective. The electronic survey option was expeditious and accurate when sending, tracking, and analyzing data (Wakefield & Watson, 2014). Surveys have been used for many years as the preferred mode of empirical research (Boone & Boone, 2012). In 1983, Rossi et al. (1983) endorsed the use of surveys for data gathering in the social science disciplines and their associated fields. The authors noted that their application was an important tool for applied purposes in the public and private sectors (Rossi et al., 1983; Tourangeau, 2018).

I engaged a 25 SMEs in this Delphi panel for data collection process using SurveyMonkey questionnaires that provided accessibility, privacy, and confidentiality to SMEs. The SurveyMonkey survey questions were framed within the parameters of the problem statement and purpose statements that were grounded within the dark triad theory conceptual framework.

I developed questions of substance during the open-ended Round 1 inquiry (see Appendix B); however, SMEs had the opportunity to ask any questions needed to clarify the meaning of these questions. Because this study was developed to increase awareness and present real-time best security practices used by SMEs in their daily activities, it was important that the SMEs clearly understood the problem statement and the purpose of the study. The analysis of responses to the Round 1 survey informed development of the Round 2 survey (see Appendix C). The analysis of responses to the Round 2 survey informed creation of the Round 3 survey (see Appendix D).

The purpose of this qualitative Delphi study was to uncover what real-time consensus existed among 25 IT SMEs in the Washington metropolitan area for managing

insider threats and data security in public and private organizations. The purpose statement supported the problem statement of the study (Gallego & Bueno, 2014; Locke et al., 2004; Patton, 2015). Personal preferences and biases were not a part of this study because face-to-face interviews, or physical interactions that could develop biases and issues of perceptions, likes and dislikes did not take place (Jacob & Ferguson, 2012). Content validity was accomplished through SMEs validation of the final responses (Patton, 2015). This verification technique was successful in ensuring the study findings' validity, credibility, dependability, and confirmability (Kornbluh, 2015).

In analyzing the data, neutral responses such as neither agree nor disagree, were not taken into consideration because these could not assist in developing countermeasures, strategies, policies, or in identifying risky behaviors, or support consensus (Boone & Boone, 2012; Wise, 2015). Wise (2015) noted that neither agree nor disagree responses were the result of Likert's 1932 5-point scale response options, or what was called the "Neutral Middle" (Wise, 2015). The "Neutral Middle" does not provide great value to a survey, other than to indicate the number of people who abstained from voting. Neither agree nor disagree represented the same as not responding to a specific question (Wise, 2015). In comparison, in *quantitative* studies the neutral middle receives a scoring number of 3, pulling the means to the middle of the measuring scale that influences the scored responses because it can make responses to appear more similar while hiding the distribution in a standard deviation, thus making statistics misleading (Wise, 2015). In this qualitative study, the level of agreement for reaching consensus was at least 60% if the combined numbers fell in the *Agree/Strongly Agree* range on a 5-point Likert-type scale (Cleary et al., 2014).

Figure 3

5-Point Likert-Type Scale

Agree – Strongly Agree –Neither Agree- nor- Disagree –Disagree – Strongly Disagree				
1	2	3	4	5

Note. From "Likert Scales and Data Analyses," by I. E. Allen and C. A. Seaman, 2007, *Quality Progress, 40*, p. 64-65 (https://asq.org/quality-progress/2007/07/statistics/likert-scales-and-data-analyses.html). In the Public Domain.

Procedures for Recruitment, Participation, and Data Collection

A professional group of 25 (SMEs holding industry-certifications from accredited institutions were recruited for this study. These SMEs were at least 21 years old and had at least 5 years of experience in the IT and cybersecurity fields. In accordance with standard practices for email notification of the study, I submitted SMEs an invitational letter (Appendix E) with information and instructions about the study, their participation, rights for confidentiality, consent, risks, and rights to withdraw at any time as described in the Consent Form.

As to the procedures for data collection, I collected the data from SMEs, within a 2-week interval after each survey round submission and recorded emerging themes and categories using a 5-point Likert-type scale. Emerging themes were comprised of categories such as insider threats' reasons, motivators, behaviors, and security prevention strategies as depicted on Figure 3. Consensus on the data gathered was determined by the minimum 60% frequency and number of responses with the same meaning, or categorization (Yazan, 2015). I analyzed data, formed data segmentation, and developed

direct interpretation, or themes starting at 60% similarities (Talanquer, 2014; Yazan, 2015). Data segmentation, categorization, and analysis were key elements in qualitative studies (Talanquer, 2014).

If consensus was not reached within the specified three rounds of surveys due to issues such as a greater incidence of neutral questions existed, or SMEs withdrew, I reserved the right to develop a fourth closed-ended questionnaire (Round 4), as indicated earlier in the Consent Form. The SMEs were informed of their right to continue or withdraw at any time and for any reason; therefore, they had the final decision to continue, or stop participation. Likewise, SMEs were informed that no compensation could be provided for their participation and that their responses were confidential.

Hsu and Sandford (2007) noted that a Delphi technique allowed for several rounds of questionnaires ending when consensus had been achieved (Hsu & Sandford, 2007). Three rounds of questionnaires are enough to establish consensus, if the qualitative inquiry was trustworthy and met the rigor resulting from a rich data collection (Corbin & Strauss, 2015; Raley et al., 2016; Rosenthal et al., 2015). My standards and familiarity with this form of inquiry as a previous Delphi panel member dictated that I could complete this study in 3 months if I followed the same disciplined method I used as a Delphi SME participant to meet submission deadlines. However, if Round 1 did not render enough responses due to a lack of participation, I kept the option open to recruit more SMEs through LinkedIn, or any other professional organization that could provide SMEs to complete the analysis. According to Che Ibrahim et al. (2013), a Delphi analysis took between 3 and 6 months to complete. As there were no extenuating circumstances, I

was able to process each survey round in a 2-week period (Davies et al., 2016; Raley et al., 2016).

As a part of the data collection process, I emailed reminders to the SMEs 3 days before the expected questionnaires submission. I submitted the Consent Form for Participation to SMEs electronically with a request to return surveys within 10 days after receipt. SMEs received a summary of their responses after the third survey to allow for revisions and clarifications. I sent SMEs thank you notes electronically and will keep all records of these survey material protected for a period up to 5 years at that time, I will delete and destroy these documents. Although a period of 3 years was acceptable for nonacademic IT research's document retention, 5 years will be observed in this study in accordance with the Walden University guidelines.

This research did not include face-to-face interviews, or pilot tests. Before my research proposal was accepted by the Institutional Review Board (IRB), there were no research, or agreements attempts to obtain access to SMEs, or data gathering activities. On December 11, 2019, Walden University granted ethics approval for this study. Contact information at Walden University Research Participant Advocate - USA number 001-612-312- 1210. Email address: IRB@mail.waldenu.edu. Walden University IRB Approval No. 12-11-19-0429821. The research was conducted ethically and respectfully in accordance with the National Institute of Health (NIH) guidelines.

Data Analysis

The data analysis included data visualization, assessment and interpretation based on the feedback from 25 SMEs in Virginia, Maryland, and Washington, D.C. with roles in the public and private sectors as information technology and cybersecurity

professionals. There were three rounds of survey questions in this Delphi study. Excel spreadsheets and tables were used for data visualization to put data into context and provide summaries to SMEs. To provide meaning to the obtained data, I used content analysis for narrative data interpretation. Generalizations and data association were used in the interpretation of findings with the same meaning (e.g., money and financial gain).

The raw data for analysis and subsequent questions came from responses to Round 1 open-ended questions. Data gathered were analyzed through categorization and direct interpretation using a 5-point Likert agreement scale (agree, strongly agree, disagree, and strongly disagree) for responses achieving 60% agreement. The responses to Round 1 questions, as well as any common themes that emerged from those baselines, were used to construct Round 2 questions. In Round 2, SMEs were asked whether they agreed, or disagreed with the Round 1 responses. SMEs were asked to make any necessary adjustments at this point. If more tools existed at the time they received the second survey, extra boxes were supplied to add further reasons, motivators, strategies, policies, and procedures. SMEs had to confirm and agree on the previously verified concepts supplied by the participating group. Round 3 required SMEs to validate and come to consensus with the previously vetted concepts provided by the participating group. In Chapter 4, I used group of tables as a source of information visualization. Hancock and Algozzine (2015) and Hancock et al. (2016) noted that narrative data can be analyzed by individual, grout, or commonalities until reaching saturation.

Data Analysis Process for Round 1 Survey Open-Ended Questions

During the data analysis process, I grouped SMEs open-ended responses into categories and interrelated clusters, summarizing and assigning descriptive, or conceptual

labels using thematic concepts and raw data saved into an Excel spreadsheet (Gale et al., 2013). Brady (2015) noted that a thematic content analysis applies to identify response patterns to open-ended questions. As recommended by Brady (2015), as responses were received from Round 1, I used a thematic content analysis to identify similar themes in Round 1 that could depict employees' risky behaviors, insider threats' motivators, strategies, and early interventions used to prevent data breaches, and recommended policies and procedures issued to prevent insider threats.

Conrad and Schober (2000) found that survey respondents can misunderstand the questions and unintentionally answer in a manner that could produce misalignments in the outcome of a Delphi study. For that reason, I analyzed responses to Rounds 2 and 3 closed-ended questions in a manner that addressed the original survey inquiry and provided SMEs real-time responses that addressed the original problem and purpose of this study. Irrelevant information concerning political views, religion, demographics, or personal information inserted in the questions during this survey, were not be a part of this study (Charmaz, 2014; Patton, 2015). Because this study's survey questions had been designed to gather a diverse number of opinions, my assumption was that three surveys could be enough to achieve consensus, as this Delphi study's conceptual framework supported the overall purpose of raising awareness about insider threats' risky behaviors through SMEs real-time consensus (Habibi et al., 2015; Hoffmann et al., 2018).

Round 1 open-ended questions, as discussed before, provided raw data that was used to inform SMEs of findings and request confirmation during the close-ended Round 2 questions (Cleary et al., 2014). Survey 1 four open-ended questions were not intended to produce consensus, but to gather raw data to develop subsequent survey questions for

Round 2 based on the 5-point Likert scale (agree, strongly agree, disagree. Strongly disagree) until achieving consensus, saturation, and validation. In Round 1, several questions to reasons and motivators rendered the same answers from different SMEs to these questions; therefore, one description (i.e., answer) only was used to inquire SMEs if they agreed during the subsequent Round 2 closed-ended questions. Neutral, or unanswered questions that did not contribute to the goal and purpose of the study, were not included as they did not affect the results of the study, if a 60% majority did not exist. The reasons, motivators, security strategies, and early intervention, policies, and procedures provided by the SMEs are the core elements of consensus in this study (Habibi et al., 2015; Hoffmann et al., 2018). Discrepancies did not occur, making it possible to achieve the overall purpose to identify what real-time consensus existed among SMEs on how to identify and deter the increasing problem of insider threat activities and risky behaviors in public and private organizations (Rosenfeld et al., 2012; Sokolowski et al., 2016; Hampton et al., Pew Research Center Project Survey, 2017).

Data Analysis Process for Round 2 Survey Closed-Ended Questions

Closed-ended questions were drafted from the classification of the responses to the Round 1 survey's open-ended responses. I conducted data segmentation, categorization, analysis, and direct interpretation to incorporate findings into the drafting of the Round 2 survey closed-ended questions. Data interpretation dealt with responses using similar synonyms. Talanquer (2014) noted that data segmentation, categorization, and analysis were key elements in qualitative studies. Consensus was achieved using the data analyzed using content analysis for the overall agreement and disagreement SME feedback provided, using frequency counts and percentages to analyze those category

qualifiers and identify what items met 60% (i.e., 60% of 25 responses), where 25 responses represented 100% agreement and 15 responses represented 60% agreement.

Content analysis examines the pattern of communication in a replicable, systematic, and noninvasive manner (Graneheim & Lundman, 2004; Cleary et al., 2014; Yin, 2010). This analytical framework was comprised of Yin's (2010) analytical generalizations and a path I have designed to group SMEs insider threats' consensus for reasons, motivators, outcomes, and impacts. Yin (2010) described analytical generalizations as projections from the transferability of findings in qualitative data evaluation. These generalizations were based on the theoretical analysis and evaluations of the reasons, or consideration that produce a certain outcome in research (Birko et al., 2015; Yin, 2010). Miles et al. (2014) described an analytical framework as summarizing what was known in theory to what was empirically investigated. To update the analytical framework of this study, I included other descriptions resulting from the SMEs responses to the survey questions. This scale guided me through the data analysis and conclusions. Developing an analytical framework in qualitative research was important because qualitative research pursues exploration and discovery (Charmaz, 2014). Miles et al. (2014) noted that to help identify the main data needed for saturation, particularly during data interpretation, an analytical framework helps qualitative researchers to organize data findings and differences, developing themes as the researcher's analysis goes from a broad to detailed analysis. Data analysis did not include statistical, or multivariate data analysis, as this was a qualitative study based on 60% consensus approval (Hair et al., 2010). References to demographic information, income, race, age, gender. Irrelevant data that did not apply to this inquiry was disregarded.

Because SMEs could have become distracted by their own opinions and interests, upon achieving the first series of qualifiers for reasons, motivators, strategies and policies and procedures from grouping similar responses in Round 1, topics and themes were incorporated into Round 2 closed-ended questions for controlled feedback (Hsu & Sandford, 2007). Controlled feedback was an integral part of the Delphi method that facilitates group dynamics and interactions limiting negative effects on data validity (Hsu, 2007).

The analytical strategies were important for this research because they could account for real time, real life contemporary phenomena and, the boundaries between phenomena, context relevant events unclear, or unavailable for direct observation (French et al., 2002). Comparisons among SMEs' common responses could help in developing thematic frameworks and narrative analyses (Janesick, 2011). Data analysis included three main categories to include data reduction through consolidation, data display and data verification (Adler & Clark, 2015). No demographic data were requested from SMEs that could include race, gender, or national origin. Data gathered were analyzed through categorization and direct interpretation (Yazan, 2015).

Data Analysis Process for Round 3 Survey Closed-Ended Questions

In this phase of the study, the integration of SurveyMonkey and Excel spreadsheets supported my analysis of the extensive data collected from 41 questions and real-time answers provided by the SMEs. I used frequency counts and percentages to analyze categories and identify what items met 60% agreement (i.e., 60% of 25 responses), where 25 responses represented 100% agreement and 15 responses represented 60% agreement. I used this set of responses for validation and final analysis.

The Round 3 closed-ended questions included any validation in the responses from Round 2 where SMEs had an opportunity to validate, add, or change their prior answers. This approach served to provide summaries of the SMEs consensus and to resolve any misunderstandings that may have taken place due to different interpretations of the questions and that there was no bias on my reporting of the research findings (Onwuegbuzie et al., 2012).

Determining Final Consensus

During the final Round 3, I paid greater attention to changes, relevance and validity for achieving consensus. There are several forms and measures used when achieving consensus. These include several rounds, post group consensus, the coefficient of variation, subjective percentage agreement, and subjective analysis (de Loë et al., Diamond et al., 20142016; Von der Gracht, 2014). The level of agreement was also a recognized method for identifying consensus that becomes illustrative when used in conjunction with a Likert scale (Förster & Von der Gracht, 2014). In this qualitative study, I used frequency counts and percentages to analyze categories and identify what items met 60% agreement for reaching consensus in every entry requiring a minimum of 60% SMEs agreement on a 5-point Likert-type scale showing agreements; (i.e., 60% of 25 responses), where 25 responses represented 100% agreement and 15 responses represented 60% agreement (Cleary et al., 2014).

A contingency approach was to extend a fourth survey, if consensus was not reached within the specified three rounds of surveys, due to a greater incidence of neutral questions, that was, neither agree, nor disagree themes, or SMEs withdrawal. I reserved the right to administer four surveys, as noted in the Informed Consent, if additional data

were required. The SMEs were informed of a potential Round 4 survey and their right to continue or withdraw from the study.

Optional Round 4 Survey Closed-Ended Questionnaire

Upon receipt of the SMEs validation of Round 3 findings, it seemed clear that a fourth survey was not needed, unless the findings indicated a lack of stability, or similarities (e.g., less than 60% agreement). A fourth survey could have been an alternative (Fusch & Ness, 2015). Kalaian and Rafa (2012) theorized that the stability of results over several rounds of questioning could lead to consensus, hence the flexibility for a fourth survey, if needed.

Issues of Trustworthiness

Trustworthiness is the term used for validity and reliability in qualitative studies; it is the pillar for all other terms of credibility, dependability, conformability, transferability, and authenticity (Gallego & Bueno, 2014). The four elements applied to this study for ensuring unbiased qualitative results were credibility, transferability, dependability, and confirmability (Lincoln & Guba, 2000). Although different opinions were found in research about what works best for qualitative studies, or if there was not much variation in Delphi studies' design, researchers must try to clearly define how rigor in research was established (Diamond et al., 2014). Trustworthiness in this study was established by the responses received from SMEs during their final survey. I ensured that the information provided by SMEs provided value and that the findings were based on SMEs experiences and viewpoints (Lincoln & Guba, 2000). The SMEs assessed if the questions were credible and appropriate to discourage biases and if the findings described fully described their answers. As the researcher, I made sure that the questions aligned

with the problem statement and purpose of the study identifying real-time consensus and best practices from SMEs. As insider threats continue to rise, increased awareness about risky behaviors and real-time strategies needed to be gathered from SMEs, who could share their experiences and consensus on the subject on insider threats' reasons, motivators strategies, policies, and procedures for the identification and prevention of insider threats, thus allowing no room for personal preferences and biases (Jacob & Ferguson, 2012).

Credibility

The survey analysis recognized trends surrounding insider threats' identifiers and red flags, compliance with regulatory mandates, policies, and procedures; emerging technologies, knowledge sharing, and management of information technology systems and applied a 5-point Likert scale to classify feedback provided by SMEs in the first survey questionnaire, that is, *Agree, Strongly Agree, Disagree, Strongly Disagree*. Neutral answers provided no value to the study and were not incorporated into the results (Dang-Pham, 2014; Kirlappos et al., 2014; Willison & Warkentin, 2013). Strategies available to assure credibility included saturation, triangulation, and peer review (Charmaz, 2014; Hancock & Algozzine, 2015). Saturation was the preferred method to ensure survey findings credibility, quality and validity from the methods listed above (Fusch & Ness, 2015). Billups (2014) noted that credibility establishes believable results on the part of the researcher and an understanding of the SMEs' perspectives and viewpoints (Billups, 2014). Because the final findings were presented to the SMEs for their confirmation and verification, any perception of reflexivity, that was, my own

personal views, beliefs and professional experiences did not affect the answers of the SMEs.

Transferability

I accomplished transferability to the extent that it achieved external validity, or the ability to apply data that had been gathered into a new study to enhance the research process (Janesick, 2011). Houghton et al. (2013) noted that to achieve transferability, the researcher must provide detailed information of the findings, explain the methodology used and why, explain the data collection and analysis process, findings and summaries that could provide value to the body of knowledge and enhance further research (Fusch & Ness, 2015; Houghton et al., 2013). Chapter 3 depicts the research method and rationale.

Dependability

A study is dependable when a different set of researchers can perform an inquiry and obtain similar outcomes based on the study design, rationale, and interpretative judgment (Houghton et al., 2013). One exception to that dependability may be the result of changes in conditions and views about the subject under study on the part of the SMEs participating in the new study (Billups, 2014). Billups (2014) argued that for data collection dependability, consistent themes must align with the original data collection methods indicated at the beginning of the study (Billups, 2014). The flexibility and freedom of the Delphi study facilitated the study's dependability, and separation from any bias (Fusch, 2015).

Neutrality

The concept of neutrality refers to the social researcher's obligation and responsibility to overcome personal biases while doing any research. The goal of

neutrality is to separate fact from emotion and to make individuals less stereotyped. Neutrality is fundamental not only in sociology, but also in many other fields because it explains basic ethics. This Delphi study was based solely on the SMEs' consensus, feedback, and responses, and not on my personal motivations, biases, or interests. Researchers are responsible for striving for objectivity and eliminating prejudices while doing research.

Confirmability

A Delphi study provides the privacy for SMEs to speak freely and without fear of retaliation. Kornbluh (2015) noted that in such settings, SMEs could provide feedback freely and without external influences on their viewpoints. Billups (2014) noted that confirmability was used to determine if results were accurate, can be corroborated and depict actual findings. In this study, I validated SMEs responses with them before concluding the reporting of findings for my dissertation. Participant validation was a well-accepted practice in Delphi studies to validate SMEs' responses and reduce the perception of reflexivity if any (Kornbluh, 2015). Reflexive journaling and auditing also provide the transparency that can be reviewed by others to judge the methods and approaches of this study (Cope, 2013).

Ethical Procedures

In compliance with the Walden University's human SMEs and ethics data collection practices, all research began upon the Walden University's Institutional Review Board's (IRB) approval and receipt of the IRB Informed Consent form. No minors could participate in this study. SMEs participation was voluntary, and these must be over the age of 21, and able to respond to questions without feeling coerced, forced, or

uncomfortable. Participants can withdraw at any time and for any reason. SMEs voluntary participation, anonymity, confidentiality, and goal clarity were the drivers of this study. SMEs have an opportunity to revise answers to reflect their real-time points of view (Janesick, 2011).

Data gathered in this study was password-protected and maintained in confidentiality for 5 years using a Cloud service. Participants were identified by a number versus a name to protect confidentiality and SMEs opinions. Given the topic and the nature of this study, ethical issues and conflicts of interest do not appear as issues that could jeopardize the completion of this study.

Summary and Transition

In Chapter 3, the research rationale, design, role of the researcher and methodology were introduced. The SMEs rights were clearly outlined along with issues of trustworthiness. Three rounds of surveys were done, the first survey provided SMES an opportunity to freely provide descriptions for reasons, motivators, strategies and policies and procedures for handling insider threats; while the second and third surveys used closed-ended questions to validate and achieve a 60% consensus. No pilot studies, or interviews took place in this study. This study provided the selection logic for SMEs participation, instrumentation, data collection and the data collection plan describing how issues of trustworthiness encompassed areas of ethics, credibility, transferability, dependability, confirmability. The results from this Delphi study were classified from an analysis of the SMEs' responses classified using the themes, patterns, and relationships gathered from three surveys from SMEs. In this qualitative study, I gathered the perspectives of those IT experts, or SMEs managing data security and insider threat

issues in public and private organizations within the Washington metropolitan area. Real-time awareness and best practices to manage insider threats and data security were needed, and this Delphi study provided the opportunity to gather real-time consensus among SMEs on a current topic where the existing scholarship needed updating to increase security awareness.

In Chapter 4, I presented the consensus results from the data collection and analysis process for this Delphi study, using a dark triad theory conceptual framework to explain risky behaviors offered by the SMEs that could lead to insider threats in public and private organizations. The focus of Chapter 4 is on the characteristics of the panel of SMEs and results.

Chapter 4: Results

The purpose of this Delphi study was to identify what consensus existed among IT SMEs regarding insider threats and data security in organizations. Specifically, 25 SMEs in the Washington, DC metropolitan area were asked to participate in three rounds of iterative online surveys to address the following research question:

RQ1. What is the level of consensus among a panel of SMEs regarding the reasons for insider threats in organizations?

Sub questions included in the study were as follows:

SQ1. What are the motivators for insider threats in the workplace?

SQ2. What are the security strategies and early interventions used in organizations to prevent data breaches and insider threats?

SQ3. What policies and procedures can be developed to manage insider threats' access to systems in organizations?

This Delphi study was targeted for completion within the Walden University Institutional Review Board (IRB) approved schedule in the IRB application form. On December11,2019, I received IRB approval to commence study (No. 12-11-19-0429821). I set the SurveyMonkey tool to close after 25 responses from the 50 survey invites sent to SMEs were received. According to the Ponemon Institute (2014), survey response rates can range from 33% to 45% or less; for this reason, I decided to double the number of survey invitations sent to SMEs to meet or exceed my survey's 25 participation requirement. My initial contact with the prospective participants included an email notification indicating that they would be receiving an invitation to participate in the survey, so that my emails would be whitelisted. Whitelisting is a process where

computer users can create an authorization to receive emails only from known sources only. My recruiting approach included presenting the objectives of the study in the survey invitational letter and a consent to participate form that clarified the SMEs' roles, responsibilities, any risk, and the right to withdraw at any time.

In this chapter, I describe the study results, setting, demographics, data collection and analysis, evidence of trustworthiness, and final consensus. The chapter ends with a summary, followed by a transition to Chapter 5.

Research Setting

I developed the SurveyMonkey administered survey questions within the parameters of the problem statement and the purpose statement. As per the approved IRB consent form and ethics approval, the term to conduct this Delphi study was 3 months. Using SurveyMonkey and LinkedIn, I made follow-up calls and sent reminders to participants during Round 2. Responses were expected in 7–10 days, with a total time spent of no more than 60 minutes for all three surveys (20 minutes per survey x 3 = 60 minutes total spent time) over a 3-month span, or less, as agreed on the IRB-approved schedule.

The panel of SMEs provided timely responses concerning the reasons, motivators, security strategies, and early interventions needed to recognize and prevent insider threats in organizations and the policies and procedures needed to protect the confidentiality, integrity, and availability of personal and organizational data. The SMEs received an automatic thank-you note when completing the surveys within 7-10 days, or a follow-up reminder email if the survey was not accessed within 5 days. I used electronic messages

on LinkedIn to follow up with SMEs on the status of, or delays in the submission of Rounds 2 and 3.

Although Round 1 open-ended questions were submitted during the month of December 2019, responses were received within a 2-week period after survey dissemination. The coronavirus (COVID-19) and mandatory social distancing may have had the greatest effect on the study's outcome; either the SMEs simply raised the importance of this insider threats' Delphi study, or as good project managers, they understood the significance of adhering to a schedule. The obligation to remain at home may have made it easier for SMEs to complete the surveys in a timely manner; this was not a possibility that I could have anticipated, and data collection was unaffected. The SMEs reacted positively to the survey even though this killer virus had a direct impact on their lives, job availability and location, and the health of neighbors, family, and friends.

Demographics

A selected group of 25 IT professionals in the Washington metropolitan area with a minimum of 5 years of IT experience consented to participate in this study. Members of organizations such PMI, ISACA, and NIST who were certified members of PMI, ISACA, ISO, SANS, Global Information Assurance Certification (GIAC), ISC, or a similar technology/security organization comprised the SMEs in this study. I did not conduct face-to-face, or phone call interviews, onsite observations, or focus groups; therefore, a visual method did not exist to gather the SMEs' age, or race. Given the educational requirements and education required to obtain a professional certification, no minors participated in this study. Demographic questions were not included in any of the three

survey rounds; the only information gathered was that tied into the requirements for participation as indicated in the informed consent document.

Data Collection

I used online surveys for data collection. Upon SMEs' decision to participate in the study, 25 surveys were delivered using the SurveyMonkey tool; reminders and updates were disseminated using private emails at LinkedIn. The data collection process did not include interviews to eliminate the perception of any personal bias during this study. This fast and inexpensive method was enhanced by the flexibility, privacy, and freedom offered by a Delphi study. I collected data from 25 SMEs in the public and private sectors of the Washington metropolitan area using three survey questionnaires: one survey for open-ended questions and two surveys for close-ended questions. The data were analyzed using frequency counts and percentages to analyze category qualifiers and identify what items met 60% (i.e., 60% of 25 responses), where 25 responses represented 100% agreement and 15 responses represented 60% agreement. Content analysis examined the pattern of communication in a replicable, systematic, and noninvasive manner (Graneheim & Lundman, 2004). In this qualitative study, how many times SMEs responded with the same answers, or synonyms (e.g., number of repetitions) to reasons, motivators, strategies, policies, and procedures was used to analyze themes pertinent to real-time insider threats for risky behaviors, security, and data vulnerabilities, remediations, and training.

To make the data easier to classify, I first integrated the survey results from Round 1 open-ended questions into an Excel spreadsheet. I broke down the data into categories and looked for commonalities before I was satisfied with the data and reached

saturation. Hancock and Algozzine (2015) noted that consensus was based on the concept of response stability and consistency for greater saturation and transparency. I applied an analytical framework previously presented in this dissertation for the analysis and categorization of closed-ended questions in Rounds 2 and 3, along with a 5-point Likert scale. An analytical framework is a set of organized categories, or codes developed by researchers to create a new structure to organize and manage data (Gale et al., 2013). I preferred the analytical framework rather than referencing the full original accounts provided by SMEs to support the research answers (Gale et al., 2013). In December 2020, I finished my final data analysis using a 5-point Likert scale. In my final data review, I aimed to better understand the SMEs' consensus on insider threat characteristics, risk attitudes, prevention measures, and policies and procedures.

Analysis

The three key categories of data analysis in this study for data reduction were consolidation, data display, and data verification (Adler & Clark, 2015). No demographic information, such as race, gender, or country of origin, was requested of the SMEs. Reasons, motivators, security strategies, policies, and procedures in the management of insider threats' behaviors and data security management strategies as provided by SMEs in their SurveyMonkey answers were added under the corresponding themes (e.g., reasons, motivators, security strategies, policies, and procedures) for the management of insider threats' behaviors and data security management strategies.

Round 1 Open-Ended Questions

The overarching research question (RQ1) was used as a frame for the open-ended questions that aligned with the sub questions (SQ1, SQ2, SQ3) in the open-ended Round

1 survey. Responses to these open-ended questions were completed within a 10-day period and submitted for academic review within the next 5-10 days after the analysis and classifications of findings were completed. The SMEs often provided the same response for reasons and motivators. However, the survey answers reached over 100 entries for all four questions. I condensed these responses within the study's analytical framework and the 5-point Likert scale, to construct closed-ended questions for the Round 2 survey using SMEs' real-time responses reaching at least a 60% agreement. In analyzing the data, neutral responses such as *neither agree nor disagree* were not taken into consideration because these responses would not have provided meaningful input in uncovering the reasons, motivators, strategies, policies, and procedures for managing insider threats in private, or public organizations, or to support SMEs' consensus (Boone & Boone, 2012; Wise, 2015).

Miles et al. (2014) noted that to help identify the main data needed for saturation, particularly during data interpretation, an analytical framework helps qualitative researchers to organize data findings and differences, developing themes as the analysis goes from a broad to detailed analysis. The responses to the data themes gathered were analyzed through categorization and direct interpretation (Yazan, 2015). The analysis of the data from the open-ended questions in the Round 1 survey aligned with the categories of the study's analytical framework in the following category for the dark triad theory constructs. The raw data categories were closely linked to the analytical framework to begin the process of abstraction needed to gather findings in a meaningful manner (Gale et al., 2013). Because this was a qualitative research study, statistical, or multivariate data analysis was not included in the analysis of narrative findings (Hair et al., 2010).

Round 2 Closed-Ended Questions

In Round 2, SMEs were asked if they agreed with, or disagreed with the responses provided in the open-ended Round 1 survey and to make revisions as needed. In Round 2, the SurveyMonkey tool included drop-down boxes to add additional reasons, motivators, strategies, policies, and procedures if changes were required at the time that SMEs received their second survey. With each round of surveys, the categories were updated to reflect real-time inputs and present accurate categorization, thus eliminating any redundancies in findings (e.g., money vs. financial gain).

The main areas for reasons and motivators were found under the following categories: money/financial gain, retribution/revenge, political/religious affiliation, and dislike for management/organization. The top security strategies and early interventions used in organizations to prevent data breaches and insider threats were found under control access, such as "need-to-know systems access," or granting access necessary to do a person's job; security training; background investigations; nondisclosure agreements (NDAs); and controlled access/logs. The top categories for policies and procedures were focused on risk management policies, security training, reference checking, polygraphs, NDAs, and background checks. Because the survey in Round 2 allowed for changes, as further disclosed in Round 3, a greater number of reasons, motivators, strategies, policies, and procedures resulted from Survey Round 2 findings (see the Glossary for a better understanding of these categories).

Round 3 Closed-Ended Questions

In survey Round 3, I asked the SMEs to validate and come to consensus with the previously provided reasons, motivators, strategies, policies, and procedures provided in

response to the Round 1 and Round 2 surveys. Following the completion of Round 2 data collection and review, I presented findings in the Round 3 survey for validation and consensus. I introduced the survey findings to allow an opportunity to comment, make changes, and confirm that the surveys had been performed ethically and in compliance with the original questions. The general method that I followed during the administration of this study's three rounds of surveys is depicted in the Habibi's (2017) Delphi technique framework.

Lessons Learned

One comment received from an SME indicated that Round 2 had been too long. This comment was part of my lessons learned for conducting a Delphi study. Perhaps revisiting data reduction could have rendered a shorter survey, but it was my intent to be as transparent as possible when providing SMEs' responses to a survey. As a qualitative study, the survey did not include a calculation for a margin of error.

Evidence of Trustworthiness

The four elements of trustworthiness applied to this study for ensuring unbiased qualitative results were credibility, transferability, dependability, and confirmability (Lincoln & Guba, 2000). The responses obtained from SMEs during their final survey were used to determine the study's trustworthiness. I made sure that the information presented by SMEs was relevant to the problem and purpose statements of the study. The conclusions were founded on SMEs' responses, experiences, and viewpoints (Lincoln & Guba, 2000). To avoid prejudices, the SMEs evaluated whether the questions were credible and relevant, as well as whether the results described accurately reflected their responses.

Credibility

Credibility in this study was recognized by the trends provided and the degree of consensus achieved throughout the study by the participating SMEs, who had the opportunity to change their answers and/or confirm previous responses surrounding insider threats' reasons, motivators, strategies, policies, and procedures. Neutral answers provided no value to the study and were not incorporated into the results (Dang-Pham, 2014; Kirlappos et al., 2014; Willison & Warkentin, 2013). Saturation was the preferred method to ensure survey findings' credibility, quality, and validity from the methods listed above (Fusch & Ness, 2015). Billups (2014) noted that credibility establishes believable results on the part of the researcher and an understanding of the SMEs' perspectives and viewpoints.

Transferability

I accomplished transferability in this study to the extent that it achieved external validity, or the ability to apply data that had been gathered into a new research process (Janesick, 2011). Transferability of findings was reviewed by my dissertation committee as a part of their dissertation approval process regarding the approaches and activities that took place to gather findings. To achieve transferability, I provided detailed information on the findings, explained the methodology used and why, and explained the data collection and analysis processes, findings, and summaries that could provide value to the body of knowledge and enhance further research (Fusch & Ness, 2015; Houghton et al., 2013). In Chapter 3, I demonstrated the research method and rationale for this study.

Dependability

A study is dependable when a different set of researchers can perform an inquiry and obtain similar outcomes based on the study design, rationale, and interpretative judgment (Houghton et al., 2013). I addressed dependability through presenting the study's consistent findings and how these findings connected to the need for a real-time qualitative study using the dark triad theory as the conceptual framework. In this Delphi study, I relied solely on the SMEs' consensus, feedback, and responses, and not on my personal motivations, biases, or interests. For data collection dependability, consistent themes must align with the original data collection methods indicated at the beginning of the study (Billups, 2014). The flexibility and freedom of a Delphi study were factors that facilitated the dependability and separation from any bias during this study (Fusch, 2015).

Confirmability

A Delphi study is recognized for its privacy (Fusch, 2015). In this study, SMEs were able to respond freely and without fear of retaliation, providing real-time opinions and findings. Billups (2014) noted that confirmability was used to determine if results were accurate, could be corroborated and depicted actual findings. In this study, SMEs validated responses before concluding the reporting of findings for my dissertation. Participant validation was a well-accepted practice in Delphi studies to legitimize SMEs' responses and reduce the perception of reflexivity if any (Kornbluh, 2015). Reflexive journaling and auditing also provided the transparency that can be reviewed by others to judge the methods and approaches of this study (Cope, 2013).

Study Results

This section includes the study's findings as well as responses to the research questions. Results from this study are qualitative and derived from the SMEs' real-time given answers to the overarching question RQ1 Reasons for insider threats in organizations; SQ1 Motivators for insider threats in organizations; SQ2 Strategies and early interventions to prevent insider threats; and SQ3 Policies, and procedure used to manage insider threats and protect data. This study is valuable because it presents the readers with options when exploring the topic of insider threats' identification, prevention, and securing the integrity, accessibility, and confidentiality of the data. I presented closed-ended questions for Round 2 after grouping responses from Round 1 that had achieved a minimum of 60% consensus (i.e., 60% of 25 responses), where 25 responses represented 100% agreement and 15 responses represented 60% agreement.

Survey Question Round 1

The purpose of the Round 1 open-ended survey questions was to create a collection of baseline responses in a manner that would allow SMEs to freely express their opinions on the subject while also providing input based on their knowledge and experience. A Delphi panel had the benefit of allowing participants to respond to questions at any time, from any place, and in any way they wanted. The benefit of open-ended questions is that the SMEs could answer in a variety of ways.as evidenced by the raw data SMEs provided in Round 1.

The overarching topic for this study was depicted as research question 1 (RQ1). The raw data and percentages displayed in Tables 4-7 were derived from the SMEs' responses to the open-ended survey questions I used to start the study. Round 1 was an

opportunity for SMEs to respond to a question with several credible responses, allowing them to have complete control of what they said rather than being influenced by my opinions, interests, and/or previous experiences.

Reasons for Insider Threats in Organizations

The SMEs' top reason for insider threats in was a lack of training, followed by a lack of knowledge about insider threats that can be a byproduct of a lack of training, political views, political affiliation/ideology, and a lack of knowledge about insider threats that can be considered a byproduct of a lack of training. Subsequent categories included: Foreign influences; social media (this percentage decreased drastically, possibly due to the pandemic related telework mandates and the need to use social media to advertise and recruit new employees). Dislike of peers/coworkers, dislike of management, and company culture, intentional, or unintentional access to systems. Discontent with the culture of the organization, a sense of entitlement, and resentment. Employers can use the National Initiative for Cybersecurity Education (NICE) framework to train their employees on insider threat awareness (NICE, 2020).

Table 4

Reasons for Insider Threats in Organizations

Answer choices	*n*	%
employees with no regard for the organization	12.0	48.0
fraudulent activities on the part of the organization	1.0	4.0
insufficient guidelines and security	14.0	56.0
lack of training	23.0	92.0
hiring of chronic rule violators	1.0	4.0
lack of behavioral screening (negative social patterns)	1.0	4.0
personal recognition	0.0	0.0
employees sent by competitors	1.0	4.0
intentional,or unintentional access to systems	15.0	60.0
manager's treatment of employees	11.0	44.0
discontent with the culture of the organization	15.0	60.0
political affiliation/ideology	18.0	72.0
foreign influences	18.0	72.0
lack of knowledge about insider threat	20.0	80.0
careless recruiting	10.0	40.0
lack of background investigations and reference checking	10.0	40.0
sense of entitlement	15.0	60.0
resentment	15.0	60.0
social media	17.0	68.0
dislike of management and company culture	16.0	64.0
personal recognition	11.0	44.0
political views	20.0	80.0
dislike of peers/coworkers	17.0	68.0
unknown	1.0	4.0

Motivators for Insider Threats

The top motivators for insider threats were money, personal gain, revenge and/or ideology; entry level employees wanting to do social networking at work; bad intentions, emotional, financial, or politically based motivators driving the intent, dislike of management; disregard for authority; pushing boundaries; hackers wanting to sell your information/ransomware (Table 5 depicts these findings). These findings align with prior studies and insider threat motivators events such as the one previously mentioned of Ames Aldrich, a 31- year veteran of the Central Intelligence Agency, where he was a case officer, fluent in Russian, and an expert in foreign intelligence. He spied for Russia from 1985 until the day of his arrest in February 1994. Like the previous insider threats, Aldrich had accumulated excessive debt and lived beyond his means. He was paid over $1.88 million of dollars by his treason. Aldrich showed arrogance, greed and financial need that transferred to a sense of entitlement by selling national security secrets; he also showed a lack of conscience (Maasberg et al., 2016). This is just one example among the many stated in Chapter 2.

Table 5

Responses to the Motivators for Insider Threats

Answer choices	*n*	%
pushing boundaries	15.0	60.0
financial gain	5.0	20.0
hackers wanting to sell your information/ ransomware	17.0	68.0
greed	12.0	48.0
power centric	14.0	56.0
money	20.0	80.0
mental illness	1.0	4.0
immaturity	1.0	4.0
disrupting economies of scale	7.0	28.0
personal gain, revenge and/,or ideology.	20.0	80.0
depression	1.0	4.0
entry level employees want to do social networking at work	20.0	80.0
disregard for authority	17.0	68.0
retribution	2.0	8.0
dislike of management	18.0	72.0
bad intentions, emotional, financial, or politically based motivators drive the intent	20.0	80.0

Security Strategies and Early Interventions

To be successful and effective as a security professional, it is important to understand what security strategies and early interventions work best in other

organizations. You can accomplish this through benchmarking, reading dissertations such as this one, or reviewing NICE and NIST publications. You should be knowledgeable of the main security terms and tools used by other security specialists. Security systems are built from essential building pieces in the same way that a large building is built from individual bricks. Your insider threats awareness would also be built as you become familiar with the top real-time strategies and early interventions used by SMEs in the Washington metropolitan area to protect and safeguard personal and corporate data.

The top security strategies and early interventions for insider threats and data security management the SMEs provided included: Audits and network scanning, user activity monitoring, training, multi-factor identification, need to know access, security logs, effective oversight, coordinated multi-disciplinary coordination, analysis, separation of duties and mandatory training, firewalls, cybersecurity training, change management policies, using antiviruses such as Bitdefender, security indoctrination, shielding sensitive information from all employees, buddy system, and insider threat impact training.

Data are not just static assets that need to be checked on only when needed, on the contrary, the confidentiality, integrity and authorized accessibility of data requires careful access control guidelines. Integrating new data security strategies and early interventions with innovative technologies activities requires to be cognizant of the behaviors that may jeopardize security as highlighted in this study. Awareness of the dark triad theory's traits and behaviors may help organizations to reinforce their data management strategy. A more detailed explanation of this study's terminology will be observed in the analysis of Survey Round 3 individual responses that validate this study.

Table 6 depicts SMEs responses. These findings aligned with previous research findings from the Ponemon Institute, the National Institute of Standards and Technology and peer-reviewed quantitative and qualitative studies (NIST, 2016; Ponemon, 2016).

Table 6

Strategies and Early Interventions

Answer choices	*n*	%
limited access controls	20.0	80.0
update virus protection regularly	20.0	80.0
using antiviruses/bitdefender	15.0	60.0
shielding sensitive information	15.0	60.0
cybersecurity training	13.0	52.0
change management policies	17.0	68.0
limiting administrative rights	19.0	76.0
audits and network scannings	23.0	92.0
user activity monitoring, separation of duties, and training.	23.0	92.0
buddy system	15.0	60.0
access controls, one administrator per site	10.0	40.0
background checks	5.0	20.0
firewalls	20.0	80.0
polygraphs	12.0	48.0
cybersecurity training	17.0	68.0
Nondisclosure agreements (NDAs)	12.0	48.0
training, multiple factor authentication	23.0	92.0
ID Cards, dual sign on/multifactor	13.0	52.0
effective oversight, multidisciplinary coordination, analysis	22.0	88.0
need to know access	23.0	92.0
mandatory training	20.0	80.0
security indoctrination	15.0	60.0
insider threat impact training	15.0	60.0
security logs	23.0	92.0

Policies and Procedures

Employees must learn how to utilize Information technology securely and safely, as well as be aware of their duties, as a critical component of a company's Information Technology (IT) infrastructure security. To help employees understand and carry out their duties, as well as follow proper procedures, the organization must generate policies and procedures. Adopting an effective security posture may be difficult and costly for an organization because it involves disruption of normal operations at practically every level with no instant results. Security compliance necessitates the collaboration and assistance of all employees in the organization.

Policies and procedures are used to demonstrate how senior management leads and manages the organization, to achieve compliance from all stakeholders, external agreements with partners, suppliers, and customers may also be required to articulate these policies and procedures. See Table 7. The top policies and procedures the SMEs provided to manage insider threats in organizations included: Separation of duties, enforcement of least privileged access, training and oversight policy, (this answer was an example of how SMEs responded with multiple options to one question), logs and need to know policy, log analysis, SOP, background screening at hiring policy, risk management plans, controlled access Policy, training procedures, Pulseway policy, polygraphs policy, conflict resolution plan, training policy, and rewards and recognition for following rules practice.

Table 7

Policies and Procedures

Answer choices	*n*	%
limit third party usage policy/social networks	3.0	12.0
pulseway policy	15.0.	60.0
controlled access policy	20.0	80.0
log analysis SOP	23.0	92.0
background screening at hiring policy	20.0	80.0
logs and need to know areas policy	23.0	92.0
risk management activities	20.0	80.0
separation of duties, enforcement of least privileged access,		
training policy	25.0	100.0
polygraphs policy	15.0	60.0
conflict resolution plan	15.0	60.0
training policy	15.0	60.0
nondisclosure agreements	10.0	40.0
references checking procedure	12.0	48.0
internal referrals	8.0	32.0
training procedures	18.0	72.0
regularly monitoring, access controls, technology hardening, interval training	5.0	20.0
risk management plan	5.0	20.0
audits/compliance	6.0	24.0
rewards and recognition	15.0	60.0
reference checking practice	13.0	52.0
hiring the right people for the right jobs	13.0	52.0
limited access SOP	13.0	52.0
different levels of access	20.0	80.0
physical security	8.0	32.0
system security plan	12.0	48.0
change control plan	5.0	20.0

Survey Question Round 2

The preparation of the inquiries in the Round 2 survey closed-ended questions consisted of themes arranged in accordance with the study's framework that were derived from the SMEs baselined responses in Round 1. While categories in an analytical framework were closely linked to the raw data, developing these categories and codes were a way to begin with the process of abstraction of the data and a confirmation of initial consensus (Gale et al., 2013). With open-ended questions, I was able to delve into SMEs' perspectives, experiences, and thoughts, gaining useful insight into the subject at hand. Open-ended questions can be considered an essential component of a qualitative research framework. For Round 2 of this qualitative Delphi study, the baseline for consensus categorization was based on the 60% agreement among SMEs as evidenced by their responses to reasons, motivators, strategies, policies, and procedures for managing insider threats in organizations. Themes with consistent categorizations were those where the grouping of responses achieved the preestablished level of consensus (Förster & von der Gracht, 2012). Hsu and Sandford (2007) noted that the option, or criterion for narrowing down responses, or consolidation may be applied to present single themes. Additional measures, or conditions could have been used to focus on a much larger grouping of responses, such as an 80% or 90% consensus using only a higher percentage of discriminating factors; however, I did not find it necessary to use additional criteria to present the full scope of the study due to saturation (Hsu & Sandford, 2007). Round 2, the consensus was based on the concept of responses, or theme stability, and consistency that provided greater transparency and saturation (Hancock & Algozzine, 2015).

The findings were gated at a 60% minimum consensus, and in cases where the SMEs indicated disagreement, the number of disagreeable responses did not reach the minimum 60% necessary to have a significant impact in this study. Although the word disagree has been included in the finding tables, these responses did not provide consistency and were only added for transparency purposes as they did not reach criteria for inclusion, or the minimum 60%. SMEs mainly chose not to answer questions in the negative knowing that the goal of the survey was to achieve agreement, or consensus.

Reasons for Insider Threats in Organizations

In Round 2 closed-ended questions, neutral, or unanswered questions that did not contribute to the goal and purpose of the study were not included, as they did not affect the results of the study if a 60% majority did not exist (i.e., 60% of 25 responses), where 25 responses represented 100% agreement and 15 responses represented 60% agreement. In Table 8, I demonstrated the number of SMEs who agreed, strongly agreed, and disagreed, and the percentages for the main reasons for insider threats in organizations. These numbers are indicative of the real-time level of consensus among SMEs in this category. No panelists strongly disagreed.

The top SMEs' responses to the survey Round 2 closed-ended questions for reasons for insider threats in organizations confirmed previously identified traits and behaviors in the NIST, NICE and Ponemon studies, as follows: Lack of background investigations and reference checking, insufficient guidelines and security, lack of training, employees with no regard for the organization, sense of entitlement, lack of knowledge about insider threats, political views, political affiliation/ideology, foreign

influences combined, personal recognition, social media, dislike of peers/co-workers, and dislike of management.

One the most crucial categories in this survey question deals with background checks and investigations. Background checks are used to assess a person's fitness for work, whether, or not that person is who he, or she claims to be, and whether, or not that person is hiding criminal behavior, bankruptcy, or ties that might put him, or her at risk. Employees operating in high-security workplaces, or with access to high-value transactions will undoubtedly need to be scrutinized more closely. Background checks are required for some employment, particularly federal jobs that require a security clearance. Some background checks are carried out internally, while others are carried out by a third party.

Employees with no regard for their organizations have been observed in past insider threats reports such as those who sold corporate intellectual property and trade secrets, or employees who have stolen confidential, secret, or top-secret information without regard to their organization’s loss of customer trust, financial losses, falling share prices and regulatory fines (Ponemon, 2020).

Table 8

Round 2 Survey (RQ1), Reasons for Insider Threats in Organization

Answer choices	Agree	Strongly agree	Disagree	
	n	*n*	*n*	%
employees with no regard for the organization	12.0	11.0	2.0	92.0
fraudulent activities on the part of the organization	1.0	0.0	0.0	4.0
insufficient guidelines and security	14.0	11.0	0.0	100.0
lack of training	23.0	2.0	0.0	100.0
hiring of chronic rule violators	1.0	0.0	0.0	4.0
lack of behavioral screening (negative social patterns)	1.0	0.0	0.0	4.0
personal recognition	0.0	18.0	0.0	72.0
employees sent by competitors	1.0	0.0	0.0	4.0
resentment	15.0	0.0	0.0	60.0
social media	17.0	0.0	0.0	68.0
intentional, or unintentional access to systems	15.0	0.0	0.0	60.0
manager’s treatment of employees	11.0	0.0	0.0	44.0
discontent with the culture of the organization	15.0	0.0	0.0	60.0
political affiliation/ideology	18.0	0.0	0.0	72.0
foreign influences	18.0	0.0	0.0	72.0
lack of knowledge about insider threat	20.0	0.0	0.0	80.0
careless recruiting	10.0	0.0	0.0	40.0
lack of background investigations and reference checking	10.0	15.0	0.0	100.0
sense of entitlement	15.0	7.0	0.0	88.0

Motivators for Insider Threats in Organizations

Many motivators were mentioned in the SMEs responses, and previous research on insider risks has focused on human motivation to break the rules and jeopardize security guidelines to satisfy personal wants and needs, leaving the door open to inadvertent insider threats. Cyberstalking, digital piracy, trolling, online deceit, internet addiction, social and sexual networks, and vandalism are among the individual activities described for accessing unauthorized sites. These activities have been associated to the dark triad's psychopathic traits and behaviors often observed in social media activities (Golden, 2014).

There are many motivators provided by the SMES, but top identifiers were: Financial gain, retribution, money, foreign influences, personal gain, revenge and/or ideology; entry level employees want to do social networking at work, money, bad intentions, emotional, financial, or politically based motivators drive the intent, revenge, politics, dislike of management, hackers wanting to sell your information/ransomware, disregard for authority, and pushing boundaries. The themes and categories related to motivators for insider threats aligned with previous studies conducted by the Ponemon Institute (Ponemon, 2020) about insider threats and data security worldwide.

Table 9

Round 2 Survey (SQ1), Motivators for Insider Threats in Organizations

Answer choices	Agree *n*	Strongly agree *n*	Disagree *n*	%
financial gain	5.0	20.0	0.0	100.0
hackers wanting to sell your information/ ransomware	17.0	0.0	0.0	68.0
pushing boundaries	15.0	0.0	0.0	60.0
greed	12.0	0.0	0.0	48.0
power centric	14.0	0.0	0.0	56.0
revenge	20.0	0.0	0.0	80.0
greed	12.0	0.0	0.0	48.0
power centric	14.0	0.0	0.0	56.0
money	20.0	0.0	0.0	80.0
mental illness	1.0	0.0	0.0	4.0
showing others what one can do; show off	3.0	0.0	0.0	12.0
foreign influences	20.0	0.0	0.0	80.0
disrupting economies of scale	7.0	0.0	0.0	28.0
personal gain, revenge and/or ideology	20.0	0.0	0.0	80.0
depression	1.0	0.0	0.0	4.0
new employees/social net at work	20.0	0.0	0.0	80.0
disregard for authority	17.0	0.0	0.0	68.0
retribution	2.0	20.0	0.0	88.0
dislike of management	18.0	0.0	0.0	72.0
money	5.0	15.0	0.0	80.0
bad intentions, emotional, financial, or politically based motivators drive the intent	20.0	0.0	0.0	80.0
revenge	20.0	0.0	0.0	80.0
religion views	6.0	0.0	0.0	17.0
politics	20.0	0.0	0.0	80.0
arrogance	14.0	0.0	0.0	56.0
religious affiliation	1.0	0.0	0.0	4.0

Table 10

Round 2 Survey (SQ2), Security Strategies and Early Interventions to Manage Insider Threats

Answer choices	Agree *n*	Strongly Agree *n*	Disagree *n*	 %
limited access controls	20.0	0.0	0.0	80.0
update software regularly (virus protection)	20.0	0.0	0.0	80.0
using antiviruses such as Bitdefender	15.0	0.0	0.0	60.0
shielding sensitive information from all employees	15.0	12.0	0.0	60.0
cybersecurity training	13.0	0.0	0.0	100.0
change management policies	17.0	0.0	0.0	68.0
limiting administrative rights	19.0	0.0	0.0	76.0
audits and network scannings	23.0	0.0	0.0	92.0
user activity monitoring, SoD, and training	23.0	0.0	0.0	92.0
buddy system	15.0	5.0	0.0	60.0
access controls, one administrator per site	10.0	0.0	10.0	60.0
background checks	5.0	0.0	0.0	2.0
firewalls	20.0	0.0	0.0	80.0
polygraphs	12.0	0.0	0.0	48.0
cybersecurity training	17.0	0.0	0.0	68.0
nondisclosure agreements (NDAs)	12.0	0.0	0.0	48.0
effective oversight, coordinated multidisciplinary coordination, analysis	22.0	0.0	0.0	88.0
need to know access	23.0	0.0	0.0	92.0
security indoctrination	15.0	0.0	0.0	60.0
mandatory training	20.0	0.0	0.0	80.0
insider threat impact training	15.0	0.0	0.0	60.0
security logs	23.0	0.0	0.0	92.0
religion views	6.0	0.0	0.0	24.0
religious affiliation	1.0	0.0	0.0	4.0
politics	20.0	0.0	0.0	80.0
arrogance	14.0	0.0	0.0	56.0
foreign influences	20.0	0.0	0.0	80.0
money	20.0	0.0	0.0	80.0
mental illness	1.0	0.0	0.0	4.0
immaturity	1.0	0.0	0.0	4.0
disrupting economies of scale	7.0	0.0	0.0	28.0
personal gain, revenge, and/or ideology	20.0	0.0	0.0	80.0

Policies and Procedures to Manage Insider Threats and Data Security

Policies and procedures are critical in decreasing the risk of data theft, or loss by internal, or external threats. Enforcing rigorous data regulations may be the results of legal, or compliance regulations. For example, many areas for preventing data breaches were provided by the SMEs in this survey (Table 11). This awareness can help prevent the disclosure of healthcare and credit card information, regulated by law. If an organization does not comply with regulations, it could risk significant fines and be denied entry to the market. Employees who fail to perform their duties properly may be consistently punished up to criminal charges if applicable. SMEs validated responses follow: Controlled access policy, (different levels of access), background screening at hiring policy, risk management plans, training procedures, polygraph's policy, Pulseway policy, conflict resolution plan, training policy, logs and need to know areas policy, oversight policy; download protection policy, nondisclosure agreements, and rewards and recognition for following rules. Procedures can be established with Audits/compliance, physical security, system security plan. change control plan, regularly monitoring, implementation of access controls, technology hardening, and regular interval training for all on how to protect data, risk management plan; Separation of duties (SoD), enforcement of least privileged access, training, limit third party usage policy/social networks, log analysis SOP, and hiring internal referrals. Results for Policies and Procedures to manage insider threats and data security management.

Table 11

Round 2 Survey (SQ3, Policies and Procedures to Manage Insider Threats Access)

Answer choices	Agree *n*	Strongly agree *n*	Disagree *n*	%
download protection policy	23.0	0.0	0.0	92.0
limit third party usage policy/social networks	3.0	20.0	0.0	92.0
Pulseway security policy	15.0	0.0	0.0	60.0
controlled access policy	20.0	0.0	0.0	80.0
log analysis SOP	23.0	0.0	0.0	92.0
background screening at hiring policy	20.0	0.0	0.0	80.0
logs and need to know areas policy	23.0	0.0	0.0	92.0
risk management activities	20.0	0.0	0.0	80.0
separation of duties, enforcement of least privileged access, training, oversight policy	25.0	0.0	0.0	100.0
polygraph policy	15.0	0.0	0.0	60.0
conflict resolution plan	15.0	0.0	0.0	60.0
training policy	15.0	0.0	0.0	60.0
nondisclosure agreements	10.0	5.0	0.0	60.0
reference checking practice	13.0	0.0	0.0	52.0
references checking procedure	12.0	0.0	0.0	48.0
internal referrals	8.0	15.0	0.0	92.0
training procedures	18.0	0.0	0.0	72.0
regularly monitoring, implementation of access controls, technology hardening, and regular interval training for all on how to protect data.	5.0	20.0	0.0	100.0
risk management plan	5.0	20.0	0.0	100.0
audits/compliance	6.0	19.0	0.0	100.0
rewards and recognition for following rules practice	15.0	0.0	0.0	60.0
hiring the right people for the right jobs	13.0	0.0	0.0	52.0
limited access SOP	13.0	0.0	0.0	53.0
different levels of access	20.0	0.0	0.0	80.0
physical security	8.0	17.0	0.0	100.0
system security plan	12.0	13.0	0.0	100.0
change control plan	5.0	20.0	0.0	100.0

Survey Question Round 3

After completing Round 2 and analyzing the survey results, I synthesized the information from the SMEs to construct the Round 3 closed-ended questions. Survey Round 3 confirmed the consensus reached in Survey Round 2 on the reasons, motivators, strategies an early interventions, policies, and procedures for identifying, classifying, and managing insider threats in public and private organizations. I completed Survey Round 3 closed-ended questions in December 1, 2020. The Round 3 closed-ended questions sought consensus from the 25 participating SMEs completing the study to gained final consensus on insider threats' behaviors and data security management strategies as stated in the problem and purpose statements of the study. The Round 3 survey consisted of 42 questions because the Round 2 survey allowed for changes; therefore, SMEs added additional comments, or changes to their prior responses. No diminishing returns occurred during Round 3 because of SMEs' steady participation that remained a constant throughout the study. The survey findings validation using a 5-point Likert scale follow.

Survey Question Round 3

Survey Question 1. Please rate to what extent you agree/strongly agree that employees with no regard for the organization are a reason for insider threats in organizations.

Eighty-four percent of participating SMEs agreed that employees with no regard for the organization are a reason for insider threats in organizations. This finding was consistent with the findings in Round 2.

Table 12 depicts the percentages of *Agree* and *Strongly Agree* among SMEs' responses to Round 3, Survey Question 1.

Table 12

Round 3—Survey Question 1—Consensus: Employees with No Regard for the Organization

Answer choices	*n*	%
Strongly agree	6.0	24.0
Agree	15.0	60.0
Neither agree nor disagree	2.0	8.0
Disagree	1.0	4.0
Strongly disagree	1.0	4.0

Employees with no regard for the organization who become insider threats are not a new phenomenon (Thoroughgood & Padilla, 2013). The history of insider threats has shown that there was not a single industry, or business line that has not been affected by insider threats. The list of examples included insider threats within the CIA, the FBI, the Defense Intelligence Agency, the National Democratic Convention, the Office of Personnel Management, the Internal Revenue Service (IRS), EQUIFAX Credit, Bank of America, the military services, law firms, medical and pharmaceutical organizations.to mention a few (FBI, 2016c). Some insider threats have shown compensatory behaviors for low self-esteem and even dyslexia, as it was the case of agents who lacked impulse control and showed symptoms of paranoia (Maasberg et al., 2016; FBI, 2016c).

A lack of care for one's organization may be the result of perception, cultural bias, religious beliefs, financial need, and demographic differences. Awareness of these

differences are important in organizational behavior and leadership management because this awareness can help incorporate methods to decrease ill feelings and resentment on the part of employees; therefore, knowing that people with different perceptions may have unique characteristics and needs that should be considered by managers is key to avoiding, or diminishing negative feelings towards the coworkers and the organization (Padilla et al., 2007).

Round 3: Survey Question 2

Survey Question 2: Please rate to what extent you agree/strongly agree that insufficient guidelines and security training are a reason for insider threats in organizations.

Eighty-four percent of participating SMEs agreed that a lack of cyber security training was a reason for insider threats in organizations. This finding was consistent with the finding in Round 2. Table 13 depicts the percentages of *Strongly Agree* and *Agree* among SMEs' responses to Survey Question 2.

Table 13

Survey Question 2—Consensus: Insufficient Guidelines and Security Training

Answer choices	*n*	%
Strongly agree	6.0	24.0
Agree	15.0	60.0
Neither agree nor disagree	2.0	8.0
Disagree	1.0	4.0
Strongly disagree	1.0	4.0

Insufficient guidelines and security awareness training are reasons and motives for insider threats in organizations. IT Managers attempting to avoid insider threats activities and the misappropriation of organizational assets, and senior management may benefit from a real-time, in-depth understanding of the impact that guidelines and security training have on employee buy-in and behavior when it comes to embracinig emerging technologies and enhancing data security countermeasures for insider threats. This in-depth knowledge of the need for security training can support senior leadership efforts for continued development and training budgets that tie into the total cost of ownership to build and maintain a safer working environment (NIST/NICE, 2017).

Different types of risk management and security training exist to ensure physical, environmental, internal, and external risks are identified and manage before these interfere with mission essential functions. For example, a lack of cyber security training was consistently chosen by SMEs in Surveys Round 2 and Round 3 as reasons for insider threats.

Round 3: Survey Question 3

Survey Question 3. Please rate to what extent you strongly agree/strongly disagree that a lack of cybersecurity training was a reason for insider threats in organizations.

Eighty-four percent of participating SMEs agreed that a lack of cybersecurity training was a reason for insider threats in organizations. This finding was consistent with the finding in Round 2. Table 14 details SMEs' responses to Survey Question 3.

Table 14

Survey Question 3—Consensus: Cybersecurity Training

Answer choices	*n*	%
Strongly agree	9.0	36.0
Agree	12.0	48.0
Neither agree nor disagree	1.0	4.0
Disagree	3.0	12.0
Strongly disagree	0.0	0.0

Cybersecurity training programs will help to reduce the risks of cyber-attacks (NIST, 2016; Ponemon, 2017). While employee knowledge may not be a panacea for protecting all risks, a cybersecurity training program will demonstrate (a) employers' commitment to data protection and (b) that employers are taking the necessary steps to fix vulnerabilities and intrusions. Cybersecurity training is not simply having people follow the rules; rather, security involves empowering people to be proactive when presented with threat situations. Cybersecurity training enables the principles of data availability, confidentiality, and integrity (CIA). Twenty-one SMEs concurred with these findings in both surveys, achieving a total consensus of 84%.

Round 3: Survey Question 4

Survey Question 4: Please rate to what extent you strongly agree/strongly disagree that personal recognition was a reason for insider threats in organizations.

Although personal recognition has been related to the dark triad personality traits, it did not achieve the necessary 60% consensus needed to provide a substantial input to

this survey. Personal recognition was described by 44% of SMEs as a *Neither Agree nor Disagree* category for insider threats in organizations. (See Table 15).

Table 15

Survey Question 4: Personal Recognition Responses

Answer choices	*n*	%
Strongly agree	1.0	8.0
Agree	7.0	28.0
Neither agree nor disagree	11.0	44.0
Disagree	5.0	20.0
Strongly disagree	0.0	0.0

Maslow's hierarchy of needs (1954), or an individual's needs to excel in his, or her performance, accomplishments, rank, or education may be linked to the need for personal recognition, as there have been both welcomed and problematic outcomes in community, school, and families. Psychologists, in contrast, have become interested in what motivates people and how people can better understand each other. Balik (2014) noted that what motivates individuals, has changed through the years. Social media for example, has served as the battle ground for students, presidents, and players to exchange accomplishments. Balik affirmed that social media such as Facebook with more than 800 million active users, Twitter with more than one billion users and LinkedIn®, were examples of our technological need for personal recognition, as value assigned to the individual was directly linked to who has more friends, followers, members, posts, groups, lists, events, likes, and dislikes (Balik, 2014; Palfrey & Gasser, 2008).

Round 3: Survey Question 5

Survey Question 5: Please rate to what extent you strongly agree/strongly disagree that intentional,or unintentional access are a reason for insider threats in organizations. Table 16 details SMEs' responses to Survey Question 5.

Eighty-four percent of participating SMEs agreed, or strongly agreed that intentional, or unintentional access was one of the reasons for insider threats in organizations in Round 3. This finding represented an increase from 15 to 21 SMEs in agreement in Round 2 (see Table 16).

Table 16

Survey Question 5—Consensus: Intentional and Unintentional Access

Answer choices	*n*	%
Strongly agree	4.0	16.0
Agree	17.0	68.0
Neither agree nor disagree	2.0	8.0
Disagree	2.0	8.0
Strongly disagree	0.0	0.0

Unintentional access occurs when untrained employees click on links and go to sites that appear familiar to them, it may also occur when employees forget to remove the identification cards from the system or allow others to view their passwords. As survey findings confirmed, intentional access to unauthorize users can be the result of retaliation, revenge, sabotage, or espionage. Innovation and modernization brought this unknown ingredient and bugs into the systems that could take training to counter intentional, or

unintentional unauthorized access to sensitive, confidential, and personally identifiable information (ABA, 2017; NIST, 2016; Ponemon, 2017).

One example of unintentional, or accidental leakage can be observed with medical records, personally identifiable information, and health records). All unauthorized disclosures must be reported to those affected by this type of breach. All personally identifiable information and health records releases must be preauthorized by patients only.

Round 3: Survey Question 6

Survey Question 6: Please rate to what extent you strongly agree/strongly disagree that discontent with the culture of the organization was a reason for insider threats in organizations.

Eighty-eight percent of participating SMEs agreed, or strongly agreed that discontent with the culture of the organization was a reason for insider threats in organizations (see Table 17).

Table 17

Survey Question 6—Consensus: Discontent with the Culture of the Organization

Answer choices	*n*	%
Strongly agree	11.0	44.0
Agree	11.0	44.0
Neither agree nor disagree	3.0	12.0
Disagree	0.0	0.0
Strongly disagree	0.0	0.0

In Round 3, the number of responses to Survey Question 6 showed an increase in consensus from 15 to 21 SMEs. Discontent with the culture of an organization may be the result of not understanding the organization's leadership, culture, mission, and goals for innovative changes, or simply a lack of communication from leader (Padilla et al., 2007). One important factor in information security implementation was to gain employee buy-in through awareness and training to create a security culture within the organization (Mallery, 2009). D'Arcy et al. (2009) established the need for ongoing research on security awareness and noticed that current research mostly covers the relationship between behavioral intentions and security awareness, thus indicating the need for researchers to examine the relationship between the former and the actual information security-related behaviors and compliance with information security policies (The Impact of Cybersecurity, 2018).

Round 3: Survey Question 7

Survey Question 7: Please rate to what extent you strongly agree/strongly disagree that ideology, foreign influence are reasons for insider threats in organizations.

Seventy-two percent of participating SMEs agreed, or strongly agreed that ideology and foreign influence are reasons for insider threats in organizations. This finding was consistent with Round 2 findings (see Table 18).

Table 18

Survey Question 7—Consensus: Ideology, Foreign Influence

Answer choices	*n*	%
Strongly agree	4.0	16.0
Agree	14.0	56.0
Neither agree nor disagree	4.0	16.0
Disagree	3.0	12.0
Strongly disagree	0.0	0.0

The FBI Director, Christopher Wray described in 2017, that foreign influences are activities that may include covert actions by foreign governments, or individuals trying to influence the United States' political and/or public sentiment; and that this association of citizens around the world, was enabled by the anonymity that the Internet provides. Through the years, foreign influence has taken many forms and used many tactics hoping to reach Americans secretly from outside of the United States. Foreigner influences often use false personas and fabricate stories on social media platforms to discredit U.S. individuals and institutions (FBI, Wray, 2017). Organizational leaders should be aware of

social media information to help their organization avoid becoming a target (Padilla et al., 2007).

Round 3: Survey Question 8

Survey Question 8: Please rate to what extent you strongly agree/strongly disagree that lack of knowledge about insider threats was a reason for insider threats in organizations.

Eighty percent of participating SMEs agreed that a lack of knowledge about insider threats was a reason for allowing insider threats in organizations (See table 19).

Table 19

Survey Question 8—Consensus: Lack of Knowledge

Answer choices	*n*	%
Strongly agree	4.0	16.0
Agree	14.0	56.0
Neither agree nor disagree	4.0	16.0
Disagree	3.0	12.0
Strongly disagree	0.0	0.0

A lack of knowledge about insider threats can be observed when new employees join an organization and are not fully trained on identifying insider threat behaviors, thus enabling voluntary, or involuntary unauthorized access to the organization. A lack of knowledge about the risks of insider threats was exacerbated by the Internet of Things (IoT) and social media that often can threaten assets. Organizational knowledge, security and legal departments must secure ways of sharing knowledge across geographical

boundaries. Employers can use the National Initiative for Cybersecurity Education (NICE) framework to train their employees on insider threat awareness through the granting of industry certifications and academic credentials that provide employees with greater opportunities in the workplace (NICE, 2020).

Round 3: Survey Question 9

Survey Question 9: Please rate to what extent you agree/strongly agree that lack of background investigations and reference checking are a reason for insider threats in organizations.

Eighty percent of participating SMEs agreed/strongly agreed that a lack of background investigations and reference checking are reasons for insider threats in organizations. This finding was consistent with Round 2 findings. Table 20 details SMEs' responses to Survey Question 9.

Table 20

Survey Question 9—Consensus: Lack of Background Investigations and Reference Check

Answer choices	*n*	%
Strongly agree	6.0	24.0
Agree	14.0	56.0
Neither agree nor disagree	3.0	12.0
Disagree	2.0	8.0
Strongly disagree	0.0	0.0

A background investigation was a review of your life history that includes credit, criminal, checks, and citizenship verification, including verification of family members

depending on the organization. A background investigation includes (a) an interview with the investigator, (b) a request for original documents such as birth certificates, diplomas, employment, and (c) education and military history. Supervisors, neighbors, and family may be interviewed to corroborate facts. A background investigation was generally conducted by the Office of Personnel Management, or the U.S. Customs and Border Protection Office that is the largest federal law enforcement agency of the United States, Department of Homeland Security (U.S. Custom and Border Protection, n.d.; www.cbp.gov/faqs/what-does-background-investigation-involve). A reference check was less intrusive than a background investigation; a reference check includes the verification of the applicant's past performance from employers, schools, colleges, and other sources to assess of an applicant possesses the qualifications for the job (www.Opm.gov).

When organizations do not conduct a background investigation, or reference check, they may engage in risky hiring and engage in extensive retention problem that may include hiring inexperienced workers, undocumented employees, outlaws, or people with a history of poor performance.

Round 3: Survey Question 10

Survey Question 10: Please rate to what extent you strongly agree/strongly disagree that a sense of entitlement was a reason for insider threats in organizations.

Sixty percent of participating SMEs agreed that a sense of entitlement was a reason for insider threats in organizations. This finding achieved the minimum consensus of 60%, an increase from the 50% consensus gathered in Round 2. Table 21 details SMEs' responses to Survey Question 10.

Table 21

Survey Question 10—Consensus: Sense of Entitlement

Answer choices	*n*	%
Strongly agree	3.0	12.0
Agree	12.0	48.0
Neither agree nor disagree	7.0	28.0
Disagree	3.0	12.0
Strongly disagree	0.0	0.0

Individuals who believe to be deserving of recognition, or additional privileges and praises could display a sense of entitlement according to Jonason et al. (2017). A sense of entitlement was one of the personality traits closely aligned with Narcissism and the dark triad theory and Narcissism has been identified as one of the traits exhibited by insider threats in organizations, as agreed by SMEs in Survey Question 1. Jonason et al. (2017) noted that these traits allow holders to portray a changeable approach to interpersonal influence and create a sense of entitlement in individuals (Jonason et al., 2017).

Round 3: Survey Question 11

Survey Question 11: Please rate to what extent you strongly agree/strongly disagree that resentment was a reason for insider threats in organizations.

Eighty-eight percent of participating SMEs agreed that resentment may be a reason for insider threats in organizations. This finding was consistent with the Round 2 findings. Table 22 depicts SMEs' consensus.

Table 22

Survey Question 11—Consensus: Resentment

Answer choices	*n*	%
Strongly agree	8.0	32.0
Agree	14.0	56.0
Neither agree nor disagree	3.0	12.0
Disagree	0.0	0.0
Strongly disagree	0.0	0.0

Round 3: Survey Question 12

Survey Question 12: Please rate to what extent you strongly agree/strongly disagree that social media was a reason for insider threats in organizations.

Survey Question 12 did not achieve the minimum 60% consensus required in this study to indicate that social media was a reason for insider threats in organizations. Table 23 depicts SMEs' number of responses to Survey Question 12.

Table 23

Survey Question 12 Responses

Answer choices	*n*	%
Strongly agree	3.0	12.0
Agree	1.0	44.0
Neither agree nor disagree	8.0	32.0
Disagree	2.0	8.0
Strongly disagree	1.0	4.0

Fifty-six percent was only three answers short of 60%, or the minimum requirement for discussion; thus, the role of social media should be researched further to determine the impact of social media as an enabler of insider threats. Because social media has created accessibility of innovative and emerging technologies, particularly during the Covid-19 pandemic and the extensive telework in place (IBM_Security_Work_From_Home_Study.pdf; Kirkwood & Price, 2013; Panetta, 2017).

Social media has proven to be a valuable tool in communications and has opened the doors to academic learning, collaboration, increased business, and family communications among individuals and organizations; however, social media has not always safeguarded accessibility and file transferability; nor was it known how well it keeps up with firewalls and security guidelines to protect personal identifiable information. The extent that social media pervades government sites and causes accessibility issues was one that was not well understood; however, it was apparent that

third party accessibility and a lack of insider threats, or cybersecurity training can increase data security risks (IBM/Ponemon, 2016, 2017; Sonnenberg, 2020).

Round 3: Survey Question 13

Survey Question 13: Please rate to what extent you strongly agree/strongly disagree that dislike of management, company culture, and coworkers are a reason for insider threats in organizations.

Ninety-two percent of participating SMEs agreed that dislike of management, coworkers, or company culture was a reason for insider threats in organizations. This finding was inconsistent with previous findings in Round 2 where consensus only achieved a total of 64%. Table 24 shows SMEs responses to Survey Question 13.

Table 24

Survey Question 13—Consensus: Dislike of Management, Coworkers, Culture

Answer choices	*n*	%
Strongly agree	10.0	40.0
Agree	13.0	52.0
Neither agree nor disagree	2.0	8.0
Disagree	0.0	0.0
Strongly disagree	0.0	0.0

An organization's management and leadership can be contributing factors to culture in the workplace, and how employees adapt, and perceive their environments (Schein, 2017). Edgar Schein (2017), a renowned professor at the MIT Sloan School of Management, argued that culture in organizations was not built in a single day, instead

culture was formed in due course of time as employees go through various changes, solve problems, and adopt to the internal (peers) and external (vendors, customers) communications. Schein (2017) noted that the culture of an organization could become the newly learned behavior for employees' daily interactions in the workplace, thus forming, or enforcing the culture of the organization. The new employees who fail to comprehend the current organizational culture, or those who do not feel included may develop a dislike for their peers, managers, and environment in general (Schein, 2017). Organizations must engage in proactive leadership and employee engagements by providing proper orientations and training to counter the effect of early negative perceptions (Borkowski et al., 2011).

Edgar Schein (2017) described three levels in an organization's culture. The first level was artifacts; that was, the dress code of the employees, office furniture, facilities, behavior of the employees, and the mission and vision of the organization. The second level was values: the ethics, morals, beliefs, and principles of the decision-makers and individuals working in the organization. The third level was assumed values that included the inner aspects of upbringing and human nature, or what can be construed in current times as political correctness rather than real beliefs (Schein, 2017).

Round 3: Survey Question 14

Survey Question 14: Please rate to what extent you strongly agree/strongly disagree that pushing boundaries was a motivator for insider threats in organizations.

Only 40% of SMEs viewed pushing boundaries as a motivator for insider threats in organizations. Therefore, this category did not meet the 60% minimum consensus

required for this study. This finding was consistent with Round 2. Table 25 depicts the SMEs' responses to Question 14.

Table 25

Survey Question 14: Pushing Boundaries

Answer choices	*n*	%
Strongly agree	3.0	12.0
Agree	7.0	28.0
Neither agree nor disagree	8.0	32.0
Disagree	7.0	28.0
Strongly disagree	0.0	0.0

Pushing boundaries can be viewed negatively as part of one's personality trait, or positively during an organizational change. In this study, pushing boundaries did not achieve the minimum 60% consensus among SMEs as a motivator for insider threats in organizations.

Round 3: Survey Question 15

Survey Question 15: Please rate to what extent you strongly agree/strongly disagree that financial gain/money was a motivator for insider threats in organizations.

Ninety-two percent of participating SMEs agreed that financial gain and money was a motivator for insider threats in organizations. This finding was consistent with the Round 2 findings. Table 26 details SMEs' responses to Survey Question 15.

Table 26

Survey Question 15—Consensus: Financial Gain/Money

Answer choices	*n*	%
Strongly agree	10.0	40.0
Agree	13.0	52.0
Neither agree nor disagree	2.0	8.0
Disagree	0.0	0.0
Strongly disagree	0.0	0.0

Financial gain has been identified in prior research on insider threats as both the reason and the motivator for insider threats in organizations (IBM/Ponemon, 2016, 2017). Money and financial gain have been a factor in one's reason and motivation to grant unauthorized access to systems, or data as previously discussed in Chapter 2 (The Ponemon Institute, 2015, 2016). Financial gain through the unauthorized access of credit card numbers and banking accounts has led to drug trafficking, kidnapping, and other illegal activities in the form of identity theft (Skillings, 2020; Willison, 2009; Willison & Warkentin, 2013).

Round 3: Survey Question 16

Survey Question 16: Please rate to what extent you strongly agree/strongly disagree that disregard for authority was a motivator for insider threats in organizations.

Sixty-eight percent of participating SMEs agreed that disregard for authority was a motivator for insider threats in organizations. This finding was consistent with the Round 2 findings. Table 27 details SMEs' responses to Survey Question 16.

Table 27

Survey Question 16—Consensus: Disregard for Authority

Answer choices	*n*	%
Strongly agree	6.0	24.0
Agree	11.0	44.0
Neither agree nor disagree	6.0	24.0
Disagree	2.0	8.0
Strongly disagree	0.0	0.0

The disregard for authority behavioral trait has been linked to evidence of behaviors observed in insider threats and the dark triad traits as previously indicated in this study. Offenders have been people with problems with the law, parents, managers, or anyone in a position of authority (Abdallah & Gheyas, 2016). Disregard for authority was a factor that Abdallah and Gheyas (2016) introduced as a predisposition to malicious behaviors that seemed to indicate that wrongdoers were inclined to disobey laws and regulations, and even have delinquent behaviors (Abdallah & Gheyas 2016).

This finding ties into the conceptual framework of the dark triad for behaviors observed in insider threats in organizations (Abdallah & Gheyas, 2016; Dang-Pham, 2014).

Round 3: Survey Question 17

Survey Question 17: Please rate to what extent you strongly agree/strongly disagree that revenge/retribution was a motivator for insider threats in organizations.

Ninety-six percent of participating SMEs agreed that revenge and retribution (retaliation) were reasons and motivators for insider threats in organizations. This finding was consistent with the Round 2 findings. Table 28 depicts the findings for Question 17.

Table 28

Survey Question 17—Consensus: Revenge/Retribution

Answer choices	*n*	%
Strongly agree	11.0	44.0
Agree	13.0	52.0
Neither agree nor disagree	1.0	4.0
Disagree	0.0	0.0
Strongly disagree	0.0	0.0

Revenge resulting from perceived, or factual victimization involves adverse work-related actions that purposely have a negative impact on the target's job performance and are intended by the instigator or perceived by the target to be a reprisal for the target's behavior (Cortina & Magley, 2003; Ghazzawi, 2010). Employees who seek revenge may resort to retaliation if they perceive unfairness on the part of management, or if they perceived unfair treatment (Yoshimura, 2007). Acts of retaliation in the workplace can be work-related, or socially related retribution (Cortina & Magley, 2003). Actions that affect one's work outcomes can be concrete and addressed by senior management. Outcomes resulting from revenge activities may lead to demotions, poor performance, and terminations depending on the severity of the acts (Yoshimura, 2007).

Round 3: Survey Question 18

Survey Question 18. Please rate to what extent you strongly agree/strongly disagree that hackers wanting to sell information was a motivator for insider threats in organizations.

Eighty-eight percent SMEs agreed that hackers wanting to sell information was a motivator for insider threats in organizations. This finding confirms consensus in Round 2. Table 29 depicts the answers to Question 18.

Table 29

Survey Question 18—Consensus: Hackers

Answer choices	*n*	%
Strongly agree	6.0	24.0
Agree	16.0	64.0
Neither agree nor disagree	1.0	4.0
Disagree	2.0	8.0
Strongly disagree	0.0	0.0

The name hacker was often reference with there was a network breach, or data loss in organizations. The definition of a hacker has ranged from that of a caring to a vindictive actor. The term hacker was first coined in the 1960s to describe highly skilled computer programmers. In the 1990s, the term changed to describe anyone using their computer skills to break into computers (Skillings, 2020). Hackers' four main motives for breaking into computers and networks have been identified as follows:

- financial gain (credit card numbers and banking accounts access leading to identity theft)
- showing off to others what they can do, or increasing their reputation among hackers
- intellectual property through corporate espionage and the theft of trade secrets
- state-sponsored attacks that provide nation states with both wartime and intelligence collection options (Ponemon, 2017; Skillings, 2020).

Round 3: Survey Question 19

Survey Question 19. Please rate to what extent you strongly agree/strongly disagree that bad intentions, emotional, financial, or political reasons are motivators for insider threats in organizations.

Eighty-eight percent of participating SMEs agreed that bad intentions, emotional, financial, or political reasons are motivators for insider threats in organizations. This finding was consistent with the findings in Round 2 (see Table 30).

Table 30

Survey Question 19—Consensus: Bad Intentions, Emotional, Financial, and Political Reasons

Answer choices	*n*	%
Strongly agree	6.0	24.0
Agree	16.0	64.0
Neither agree nor disagree	1.0	4.0
Disagree	2.0	8.0
Strongly disagree	0.0	0.0

The consensus in Survey Question 19 has overlapping, or overarching effects into other areas of this Delphi Study, but ultimately represents an overwhelming agreement ranging from 84% in Round 2 to 92% in Round 3, for bad intentions, emotional, financial, or political reasons as motivators of insider threats in organizations. These motivators may fall within Baughman's dimensions that describe socially malicious behaviors. Baughman et al. (2014) stated that traits and dimensions were applicable to socially malicious behaviors. Traits such as bad intentions, emotional, financial, and political associations have been associated with socially malicious behaviors in the dark triad theory, to include emotional coldness, duplicity, self-promotion, and aggressiveness (Baughman et al., 2012; Baughman et al., 2014; Paulhus & Williams, 2002). These traits may also be aligned to a low conscientiousness attitude, a sense of entitlement, superiority, privilege, lack of remorse, lack of empathy, and a tendency to exploit others (Paulhus & Williams, 2002).

Round 3: Survey Question 20

Survey Question 20: Please rate to what extent you strongly agree/strongly disagree that entry level employees wanting to access social networks are motivators for insider threats in organizations.

Survey Question 20 only achieved a 28% response and did not meet the minimum consensus requirement of 60% needed for providing solutions to this study. This finding was consistent with the finding in Round 2 (see Table 31).

Table 31

Survey Question 20 Responses

Answer choices	*n*	%
Strongly agree	5.0	20.0
Agree	2.0	8.0
Neither agree nor disagree	10.0	40.0
Disagree	7.0	28.0
Strongly disagree	1.0	4.0

Although Survey Question 20 did not achieve the minimum 60% consensus as it relates to entry-level employees wanting to access social networks, the topic of social media was extensively covered under Survey Question 12 due to the importance that social media in social networks has in the community. Social media has been used in politics, important announcements, recruiting, and social interaction. Boss et al. (2009) argued that organizations that do not account for people as a part of information systems active players are bound to pay the price for not realizing that people—as the weakest

link in the organization—could have to be included in the planning, risks, and execution phases of innovative technologies to be successful, including the organization's mandatory security training (Boss et al., 2009; NICE, 2017).

Round 3: Survey Question 21

Survey Question 21: Please rate to what extent you strongly agree/strongly disagree that limited access controls are a main security strategy and early intervention to prevent insider threats in organizations.

Ninety-two percent of participating SMEs agreed that having limited access controls was a main security strategy and early intervention to prevent insider threats in organizations. This finding was consistent with the findings in Round 2. Table 32 depicts the how consensus was achieved in Question 21.

Table 32

Survey Question 21—Consensus: Limited Access Controls

Answer choices	*n*	%
Strongly agree	10.0	40.0
Agree	13.0	52.0
Neither agree nor disagree	1.0	4.0
Disagree	1.0	4.0
Strongly disagree	0.0	0.0

The importance of having limited access controls was reaffirmed with the responses to Survey Question 31, whereas 88% of the SMEs agreed that having a controlled access policy was a main procedure to manage insider threats access to the

organization and 92% agreed to this measure in Round 3. The National Institute of Standards (NIST) 800-100, NIST 800-12 Technical Access Control AC-2 recommends having an access control policy as a for developing an information security program for the organization (Bulgurcu et al., 2010). An organizational risk management strategy was a key factor in the development of the access control policy (NIST 800-100; NIST 800-12. Related control: PM-9. Access controls require authentication to verify the identity of the user trying to access a resource, or a control process. A system administrator was generally the authority that can grant access within an application domain (e.g., custodian). Policies determine how authorizations could be granted based on the principle of least privilege. In other words, an organization limits its risks and insider threats' opportunities to disclose information by providing users with the minimum access the job requires (NIST, 2018).

Round 3: Survey Question 22

Survey Question 22: Please rate to what extent you strongly agree/strongly disagree that updating software regularly (virus protection) was a main security strategy and early intervention to prevent insider threats in organizations.

Eighty-eight percent of participating SMEs (88%) agreed that updating software regularly (virus protection) was a main security strategy and early intervention to prevent insider threats in organizations. This finding was consistent with findings in Round 2. Table 33 depicts the SMEs responses to Question 22.

Table 33

Survey Question 22—Consensus: Updating Software Regularly/Virus Protection

Answer choices	*n*	%
Strongly agree	14.0	56.0
Agree	8.0	32.0
Neither agree nor disagree	1.0	4.0
Disagree	1.0	4.0
Strongly disagree	1.0	4.0

Updating software and virus protection are two recommendations SMEs have offered in this study to prevent data breaches and software vulnerabilities. A software vulnerability was a security hole, or weakness found in a software program, or operating system due to a lack of virus protection (NIST, 2018). Cyber and physical threats are real and can expose sensitive information and lead to identity theft; thus, updating software was key to avoid compromises. People, or companies that fail to update software expose personal information and their clients' information to criminals, simply by leaving loopholes and failing to do software updates. An antivirus software provides protection against the following types of malicious software:

- Computer viruses: A computer virus was a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be infected with a computer virus (NIST, 2018).

- Spyware: Spyware was a type of malware that gathers information about a person, or an organization without their knowledge and sends such information to hack another entity without the user's permission, or awareness (NIST, 2018).
- Rootkits: A rootkit was a collection of computer software that was typically malicious and designed to gain unauthorized access to a computer, or an area of its software. A Rootmask often masks its existence, or the existence of other software (Dang-Pham, 2014).
- Trojan horses: A Trojan horse, or Trojan, was any malware program that misleads users with the goal of breaching the security of a computer system. The term was used to depict deception and was derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy (Chondros, 2015; Azizli et al., 2016). Norton (2016), among others, created a series of software protection security solutions aimed to protect their customers.

Round 3: Survey Question 23

Survey Question 23: Please rate to what extent you strongly agree/strongly disagree that shielding sensitive information from all employees and separation of duties (SoD) are main security strategies and early interventions to prevent insider threats in organizations.

Eighty-four percent of participating SMEs agreed that shielding sensitive information from all employees, and separation of duties (SoD) are main security strategies and early interventions to prevent insider threats in organizations. This finding

was consistent with the findings in Round 2. Table 34 depicts SMEs consensus on Question 23.

Table 34

Survey Question 23—Consensus: Shielding Sensitive Information/Separation of Duties

Answer choices	*n*	%
Strongly agree	14.0	56.0
Agree	7.0	28.0
Neither agree nor disagree	3.0	12.0
Disagree	0.0	0.0
Strongly disagree	1.0	4.0

Shielding information and separation of duties are two strong components of network and systems security. This answer presents two categories that align with the National Institute of Standards and Technology ([NIST], 2016) security concept of the least privileged and zero trust, a process for granting permissions and access to network assets of the organization at the most essential level. The least privileged access means that employees have the minimum access, or the access required to perform their duties (Herold, 2010; NIST, 2016).

Shielding sensitive information from all employees aligns with the government's Privacy Act (1974). The Privacy Act (1974) applies to the records keeping practices on records of every U.S. citizen, or lawfully admitted resident of the United States and applies to the records held by any agency, or organization (Privacy Act, 1974, United States Code, Chapter 5, Sections 552a, and amendments).

The goal of the Zero-Trust architecture was to protect all resources in addition to network segments. This new architecture aims to provide network security in response to the new trends arising from remote users and off-boundaries, cloud-based technologies (NIST, 2018). The Zero Trust strategies are already a part of the government's cybersecurity policies and programs guided by the NIST Risk Management Framework, including the execution of a gap analysis to identify loopholes in security (Spear et al., 2018).

Separation of duties (SoD) also known as segregation of duties—has its roots in the financial accounting systems, whereas a funds requestor, or receiver cannot be the approver. IT departments share SoD requirements due to the increased number of IT audits and the repercussions arising from a lack of transparency in IT spending under the Federal Information Technology Acquisition Reform Act (FITARA; NIST, 2016). FITARA was responsible for the ways the U.S. federal government buys and manages computer technology (National Defense Authorization Act for Fiscal Year 2015 Title VIII, Subtitle D, H.R. 3979).

NIST recommends internal controls to prevent intentional, or unintentional errors, fraud, and theft. Internal controls facilitate control over employees having too much control, or influence over business assets and data (NIST, 2018).

Round 3: Survey Question 24

Survey Question 24: Please rate to what extent you strongly agree/strongly disagree that cybersecurity training was the main security strategy and early intervention to prevent insider threats in organizations.

Eighty percent of participating SMEs agreed that cyber security training was a main security strategy and early intervention to prevent insider threats in organizations. This finding was consistent with the finding in Round 2. Table 35 depicts SMEs responses to Question 24.

Table 35

Survey Question 24—Consensus: Security Training

Answer choices	*n*	%
Strongly agree	9.0	36.0
Agree	11.0	44.0
Neither agree nor disagree	4.0	16.0
Disagree	1.0	4.0
Strongly disagree	0.0	0.0

The Department of Homeland Security (DHS; 2019), pointed out that, as a part of the preparation of the cybersecurity workforce of tomorrow, training was essential. DHS was committed to providing the nation with access to cybersecurity training and a secure workforce development effort to create a more resilient and capable cyber nation (Gelles et al., 2012). Additional information on cyber security training can be obtained by accessing the NIST/NICE Communities of Practice (NIST/NICE, 2019).

Round 3: Survey Question 25

Survey Question 25: Please rate to what extent you strongly agree/strongly disagree that a change management policy was main security strategy and early intervention to prevent insider threats in organizations.

Sixty percent of participating SMEs agreed that having a policy for change management was a main security strategy and early intervention to prevent insider threats in organizations. This finding was consistent with the finding in Round 2. Table 36 details SMEs' responses to Survey Question 25.

Table 36

Survey Question 25—Consensus: Policy for Change Management

Answer choices	*n*	%
Strongly agree	5.0	20.0
Agree	10.0	40.0
Neither agree nor disagree	9.0	36.0
Disagree	0.0	0.0
Strongly disagree	1.0	4.0

A change management policy for Information Technology has been used by organizational leaders and IT managers to control IT changes, upgrades, purchases and unauthorized changes to processes and network systems throughout their lifecycle. A change management policy may also be used to administer administrative and operational changes that could shed clarity during organizational change and to counter change resistance. In 1996, Kotter developed an eight-step change model for implementing organizational change across many industries. presented an important framework, or model for understanding how employees perceive changes. Kotter's 8 Step Change Model presents great alternatives for leading change.

In mature organizations, a change management policy alleviates the burden of acceptability because the policy was managed by a change advisory board and senior management. Change management policies are designed to manage upgrades, new IT purchases for modernization, and to handle emergency and scheduled changes. Change management policies minimize impact to organizations while monitoring risks and conflicts during innovative technologies and IT disruptions (Panetta, 2017).

Round 3: Survey Question 26

Survey Question 26: Please rate to what extent you strongly agree/strongly disagree that audits and network scanning are main security strategy and early intervention to prevent insider threats in organizations.

Ninety-two percent of participating SMEs agreed that audits and network scans are a main security strategy and early intervention to prevent insider threats in organizations. This finding was consistent with the finding of Round 2. Table 37 depicts SMEs' responses to Survey Question 26.

Table 37

Survey Question 26

Answer choices	*n*	%
Strongly agree	13.0	52.0
Agree	10.0	40.0
Neither agree nor disagree	1.0	4.0
Disagree	1.0	4.0
Strongly disagree	1.0	4.0

The function of an audit was to uncover risks and threats that could jeopardize performance in an organization (NIST, 2019). Audits support business objectives by providing an opportunity for risk identification, classification, and mitigation according to the organization's risk tolerance. Risks can be managed through the development and implementation of policies, procedures, and security measures to decrease vulnerabilities and intrusions (FISMA, NIST, ISO 27001 Compliance Assessments). Early interventions are those risk management techniques put into place from the beginning of a project, business, or activity.

Network scanning can detect network intrusion attempts to every possible destination in a network, or a port on a given location. Early detection by such scans can help identify more dangerous threats to a network (Muelder et al., 2005). Several methods of scan detection exist, but these may only be familiar to a savvy attacker. The effectiveness of network scanning depends on the thresholds that an attacker could possibly avoid crossing (Muelder et al., 2005).

Round 3: Survey Question 27

Survey Question 27: Please rate to what extent you strongly agree/strongly disagree that a buddy system was main security strategy and early intervention to prevent insider threats in organizations.

Only 41% of SMEs agreed that a buddy system was a main security strategy and early intervention to prevent insider threats in organization. The responses to Survey Question 27 did not achieve the minimum 60% required in this study to provide consensus or add real-time value to the study. Table 38 depicts survey answers.

Table 38

Survey Question 27 Responses

Answer choices	*n*	%
Strongly agree	3.0	12.0
Agree	7.0	29.0
Neither agree nor disagree	11.0	45.0
Disagree	2.0	8.0
Strongly disagree	1.0	4.0

A buddy system in organizations may facilitate team performance and enhance communications by reducing professional isolation, augmenting the effectiveness of training, encouraging a shared approach to problem solving, and by providing a proxy for supervision and self-direction (Brown & Gilbert, 2014).

Round 3: Survey Question 28

Survey Question 28: Please rate to what extent you strongly agree/strongly disagree that security logs are a main security strategy and early interventions to prevent insider threats in organizations.

Seventy-six percent of participating SMEs agreed that security logs are a main security strategy and early intervention to prevent insider threats in organizations. This finding was consistent with the finding in Round 2. Table 39 details SMEs' responses to Survey Question 28.

Table 39

Survey Question 28—Consensus: Security Logs

Answer choices	*n*	%
Strongly agree	7.0	28.0
Agree	12.0	48.0
Neither agree nor disagree	4.0	16.0
Disagree	2.0	8.0
Strongly disagree	0.0	0.0

System security logs can help trace abnormal activities identified as attacks to the data, unauthorized logs on operating systems, faulty applications, new routers, malfunctioning firewalls, and infrastructure that create their own logs. This activity can be observed with the increased use of mobile devices and Internet-of-Things (IoT) creates a staggering number of activities that generate event logs. Once an event log information was received by the IT specialist, the data are analyzed and used for security incidents and to create profiles of normal network and user activities (Kuman & Morarjee, 2014). This baseline log information can help security professionals identify suspicious activity that falls outside of expected norms (Panetta, 2017).

Round 3: Survey Question 29

Survey Question 29: Please rate to what extent you strongly agree/strongly disagree that download protection policy was a main policy and procedure to manage insider threats' access in organizations.

Ninety-six percent of participating SMEs agreed that having a download protection policy was a main procedure to manage insider threats' access in organizations. Table 40 depicts the results for Survey Question 29.

Table 40

Survey Question 29—Consensus: Download Protection Policy

Answer choices	*n*	%
Strongly agree	8.0	32.0
Agree	16.0	64.0
Neither agree nor disagree	1.0	4.0
Disagree	0.0	0.0
Strongly disagree	0.0	0.0

The response to Survey Question 29 showed consistent consensus with findings in Round 2. Having a download protection policy may be for some organizations a part of their IT Policy, or vendor management policy. The protection policy was closely aligned with the purchase of firewalls and other computer security tools and software.

Round 3: Survey Question 30

Survey Question 30: Please rate to what extent you strongly agree/strongly disagree that limiting third party usage/social networks was a main policy and procedure to manage insider threats' access in organizations.

Seventy-six percent of participating SMEs agreed that having a policy limiting third party usage and social networks access was a main procedure to manage insider threats' access in organizations. This finding was consistent with Survey Question 4

answers regarding social networks access and Survey Question 35 regarding least privileged access presented in Round 2. Table 41 details SMEs' responses to Survey Question 30.

Table 41

Survey Question 30—Consensus: Limiting Third Party Usage/Social Networks Access

Answer choices	*n*	%
Strongly agree	7.0	28.0
Agree	12.0	48.0
Neither agree nor disagree	5.0	20.0
Disagree	0.0	0.0
Strongly disagree	1.0	4.0

Limiting third party access and preventing employee access to social networks, for improved performance and for security reasons, are common practices in many organizations, but especially among federal agencies. Preventing downloads and popup boxes that may carry viruses, are best industry practices to control unauthorized changes to networks and systems. Adhering to the principle of least privilege creates a protected, and traceable environment by clearly defining high-level functions, and actively controlling user access (Frank, 2011).

Round 3: Survey Question 31

Survey Question 31: Please rate to what extent you strongly agree/strongly disagree that having a controlled access/physical security was a main policy and procedure to manage insider threats' access in organizations.

Eighty-eight percent of participating SMEs agreed that having a policy for controlled access and physical security was a main procedure to manage insider threats' access in organizations. This finding was consistent with the findings in Round 2. Table 42 depicts SMEs' responses to Survey Question 31.

Table 42

Survey Question 31—Consensus: Controlled Access/Physical Security

Answer choices	*n*	%
Strongly agree	1.0	44.0
Agree	11.0	44.0
Neither agree nor disagree	2.0	8.0
Disagree	1.0	4.0
Strongly disagree	0.0	0.0

A controlled access policy was a part of physical security and information security policies for selective and secure access, consumption, and entering, or using information assets. Such permission to access a resource was called authorization (Borgatti et al., 2013). After the 9-11 attacks in New York, Pennsylvania and Washington, DC, organizations have imposed the requirement for individuals to self-identify upon entry/exit of buildings and to carry a badge, or identification document (ID).

Round 3: Survey Question 32

Survey Question 32: Please rate to what extent you strongly agree/strongly disagree that a Standard Operating Procedures (SOPs) was a main policy and procedure to manage insider threats' access in organizations.

Sixty-eight percent of participating SMEs agreed that having a policy for preparing standard operating procedures (SOPs) was a main procedure to manage insider threats' access in organizations. This was consistent with the finding in Round 2. Table 43 details SMEs responses to Survey Question 32.

Table 43

Survey Question 32—Consensus: Standard Operating Procedures

Answer Choices	*n*	%
Strongly agree	4.0	16.0
Agree	13.0	52.0
Neither agree nor disagree	6.0	24.0
Disagree	1.0	4.0
Strongly disagree	1.0	4.0

An SOP was designed to describe an organization's activities and operations needed for conducting business. An SOP was used to depict activities that align with an organization's business needs (Taylor, 2012).

Round 3: Survey Question 33

Survey Question 33: Please rate to what extent you strongly agree/strongly disagree that background screening at hiring was a main policy and procedure to manage insider threats' access in organizations.

Eighty-four percent of participating SMEs agreed that having a policy for background screenings at hiring was a main policy and procedure to manage insider threats access' in organizations. Table 44 depicts SMEs' responses to Survey Question 33.

Table 44

Survey Question 33—Consensus: Background Screening at Hiring

Answer choices	*n*	%
Strongly agree	7.0	28.0
Agree	14.0	56.0
Neither agree nor disagree	3.0	12.0
Disagree	1.0	4.0
Strongly disagree	0.0	0.0

A background screening was an investigation of a prospective candidate, or a review of employee's information provided in an application for employment, or when undergoing a security clearance. In this process, the company, or agency verifies that the person was who they claim to be by validating education, employment history, and other activities from their past, such as criminal records. Different methods can be used to

conduct a background screening at hiring depending on the position and location of the job. Credit organizations conduct similar background screenings (Bauman, 2017).

Round 3: Survey Question 34

Survey Question 34: Please rate to what extent you strongly agree/strongly disagree that having a risk management plan a main policy and procedure to manage insider threats access' in organizations.

Seventy-two percent of participating SMEs agreed that having a policy for a risk management plan was a main procedure to manage insider threats' access in organizations. This finding was consistent with the findings in Round 2. Table 45 details SMEs' responses to Survey Question 34.

Table 45

Survey Question 34—Consensus: Risk Management Plan

Answer choices	*n*	%
Strongly agree	8.0	32.0
Agree	10.0	40.0
Neither agree nor disagree	5.0	20.0
Disagree	1.0	4.0
Strongly disagree	1.0	4.0

A risk management plan was a document that addresses how risks could be identified, categorized, and managed. The risk management plan also details what levels of risk (high, medium, and low) and risk responses are acceptable to the organization (NIST, 2019). The risk management process was conducted through a rigorous risk

assessment, sometimes using a risk matrix, or a checklist. Risk management plans should be periodically reviewed by the project team to avoid having the analysis become stale (PMI, 2015).

Round 3: Survey Question 35

Survey Question 35: Please rate to what extent you strongly agree/strongly disagree that having a standard operating procedure (SoD), enforcement of least privileged access and training oversight are a main policy and procedure to manage insider threats' access in organizations.

Ninety-two percent of participating SMEs agreed that having a policy on standard operating procedures, enforcement of the least privileged, and access and training oversight are a main procedure to manage insider threats' access in organizations. This finding aligns with the Round 2 consensus. Table 46 details SMEs' responses to Survey Question 35.

Table 46

Survey Question 35—Consensus: Standard Operating Procedures, Enforcement of the Least Privileged, Access, and Training

Answer choices	*n*	%
Strongly agree	9.0	36.0
Agree	14.0	56.0
Neither agree nor disagree	0.0	0.0
Disagree	1.0	4.0
Strongly disagree	1.0	4.0

Survey Question 35 was one of the few questions in Round 3 that carried out multiple answers to a specific open-ended question during Round 1. The level of consensus that sustained such answers was consistently maintained through Rounds 2 and 3. Survey Question 35 aligns with responses in Round 2, Question 23 regarding SoD as a main security strategy and early intervention to prevent insider threats in organizations.

Round 3: Survey Question 36

Survey Question 36: Please rate to what extent you strongly agree/strongly disagree that having a conflict resolution plan was a main policy and procedure to manage insider threats' access in organizations.

Seventy-six percent of participating SMEs agreed that having a policy for conflict resolution was a main procedure for regulating insider threats' access in organizations. This finding was consistent with the finding in Round 2. Table 47 details SMEs' responses to Survey Question 36.

Table 47

Survey Question 36—Consensus: Conflict Resolution

Answer choices	*n*	%
Strongly agree	6.0	24.0
Agree	13.0	52.0
Neither agree nor disagree	5.0	20.0
Disagree	1.0	4.0
Strongly disagree	0.0	0.0

Conflict resolutions aims to decrease conflict. Conflict arises from disagreement and day-to-day situations. Wallensteen (2018) defined conflict resolution as the agreement between two parties in conflicting positions to solve their disagreements and central incompatibilities, accept each other's existence, and cease all negative actions against each other (Wallensteen, 2018). An organization's best gathering of such agreements was through a conflict resolution plan (Wallensteen, 2018; Jerko et al., 2019).

Round 3: Survey Question 37

Survey Question 37: Please rate to what extent you strongly agree/strongly disagree that having a polygraph policy was a main policy and procedure to manage insider threats' access in organizations.

Only 36% of participating SMEs agreed that having a polygraph policy was a main policy and procedure to manage insider threats' access in organizations. Thus, this consensus did not meet the minimum 60% majority responses for solutions to manage insider threats in organizations. Table 48 details SMEs' responses to Survey Question #37.

Table 48

Survey Question 37 Responses

Answer choices	*n*	%
Strongly agree	3.0	12.0
Agree	6.0	24.0
Neither agree nor disagree	9.0	36.0
Disagree	3.0	12.0
Strongly disagree	4.0	16.0

The results of this Delphi study reaffirmed the polygraphs' lack of popularity among prospective employees. A polygraph was also called a lie detector test. This device measures physiological indicators such as blood pressure, pulse, respiration, and skin conductivity while a person was asked to answer a series of questions (Bell & Grubin, 2010). One example for the polygraph's lack of trust and popularity can be attributed to examples such as that of spy Aldridge Ames, who betrayed his country by providing classified information to a foreign nation for many years, and yet, he was able to provide the right answers to the polygraph administrator, who cleared him because his answers were perceived as truthful enough during his first polygraph. After administering a second polygraph, Mr. Ames was cleared of any illegal activity. He spied for Russia from 1985 until the day of his arrest in February 1994 (FBI, 2016a).

Round 3: Survey Question 38

Survey Question 38: Please rate to what extent you strongly agree/strongly disagree that having an NDA was a main policy and procedure to manage insider threats' access in organizations.

Only 52% of SMEs agreed that having a policy on nondisclosure agreements, or confidentiality agreement was a main procedure to manage insider threats' access in organizations. This percentage was lower than needed for consensus. Table 49 details SMEs' responses to Survey Question 38.

Table 49

Survey Question 38 Responses

Answer choices	*n*	%
Strongly agree	3.0	12.0
Agree	10.0	40.0
Neither agree nor disagree	6.0	24.0
Disagree	4.0	16.0
Strongly disagree	2.0	8.0

Many government agencies and scientific organizations rely on Non-Disclosure Agreements (NDAs) to ensure that their intelligence secrets, patents, and trademarks are protected from disclosure to the enemy, or competition. An NDA was a binding confidential agreement that one party agrees to keep secret information (such as trade secrets to competitors) from being released to a third party (Radack, 1994).

Round 3: Survey Question 39

Survey Question 39: Please rate to what extent you strongly agree/strongly disagree that having a conflict resolution plan was a main policy and procedure to manage insider threats' access in organizations.

Sixty-four percent of SMEs agreed that having a conflict resolution plan was a main policy and procedure to manage insider threats' access in organizations. Table 50 details SMEs' responses to Survey Question 39.

Table 50

Survey Question 39—Consensus: Conflict Resolution Plan

Answer choices	*n*	%
Strongly agree	5.0	20.0
Agree	11.0	44.0
Neither agree nor disagree	7.0	28.0
Disagree	2.0	8.0
Strongly disagree	0.0	0.0

Conflict arises whenever a change occurs, or something different from the norm appears to create an unbalance. Having a policy becomes instrumental to organizations needing to set a standard for maintain a fair working environment, thus diminishing the perception of preferential treatment. Because conflict resolution may be the result of misunderstandings and plain disagreements between coworkers, or between supervisors and subordinates, service providers, contractors, subcontractors, and clients, a well though policy seems to be the only reliable guidance.

The Harvard University (2014) defined Conflict Resolution as "the informal, or formal process that two, or more parties use to find a peaceful solution to their dispute" Conflict resolution may be parallel to the severity of the conflict and how it was resolved. Three components of conflict resolution are (a) cognitive resolution, or how partiers understand the conflict based on their beliefs; (b) emotional resolution, or how the parties could feel about a conflict, and (c) behavioral resolution, or how the parties act about a conflict (Mayer, 2012).

Round 3: Survey Question 40

Survey Question 40: Please rate to what extent you strongly agree/strongly disagree that having an internal referral policy was a main policy and procedure to manage insider threats' access in organizations.

Only 52% of participating SMEs agreed that having a policy on internal referrals was a main procedure to manage insider threats access' in organizations. The number of responses did not meet the 60% minimum standard to be included as a solution in this Delphi study. Table 51 details SMEs' responses to Survey Question 40.

Table 51

Survey Question 40: Responses

Answer choices	*n*	%
Strongly agree	3.0	12.0
Agree	10.0	40.0
Neither agree nor disagree	10.0	40.0
Disagree	1.0	4.0
Strongly disagree	1.0	4.0

An internal referral policy establishes ways that an organization can capitalize on employee referrals by providing a referral fee and customizing training. An internal referral program was structured to help find reliable personnel resources because referrals could be known by existing employees who could receive a monetary incentive, and with whom the organization could be familiar (Irving & Montes, 2010).

Round 3: Survey Question 41

Survey Question 41: Please rate to what extent you strongly agree/strongly disagree that having a physical security plan, system security plan, and a change control plan was a main policy and procedure to manage insider threats' access in organizations.

Eighty-eight percent of participating SMEs agreed that having a policy to develop physical security plans, security plans and change control plans was a main procedure to manage insider threats' access in organizations. This finding was consistent with the finding in Round 2. Table 52 details SMEs' responses to Survey Question 41.

Table 52

Survey Question 41—Consensus: Physical Security Plans, Security Plans, and Change Control Plans

Answer choices	*n*	%
Strongly agree	8.0	32.0
Agree	14.0	56.0
Neither agree nor disagree	3.0	12.0
Disagree	0.0	0.0
Strongly disagree	0.0	0.0

A physical security plan was a plan that describes how to secure buildings, data networks, environmental controls, and security technology (Sennewald & Baillie, 2016). A system security plan was a detailed narrative of a security control implementation, system components, and inventories. A system security plan provides a systematic method for protecting computers from unauthorized users, viruses, and system authorization boundaries (General Services Administration, FedRAMP). A change control plan documents the processes for ensuring that changes are introduced in a controlled and coordinated manner while minimizing risks and tracing approvals (Marshak, 2005).

Round 3: Survey Question 42

Survey Question 42: Please list any additional information that you think could enhance the previously stated categories.

No additional feedback was provided, or answers were submitted during Round 3 completion. All 25 SMEs completed the survey in its entirety within the expected time.

Final Consensus

The overarching research question pertained to the reasons for insider threats. According to the final consensus of the SMEs, the most common reasons for insider threats in organizations were (a) insufficient guidelines and training; (b) a lack of background investigations; and (c) financial gain and money. The first sub-question pertained to motivators for insider threats. The final consensus on the most common motivators for insider threats in organizations was (a) pushing boundaries; (b) financial gain; (c) hackers wanting to sell your information/ ransomware; (d) money; (e) personal gain; (f) revenge and/or ideology; (g) entry-level employees wanting to do social networking at work; (h) disregard for authority; (i) retribution; (j) dislike of management; (k) bad intentions, emotional, financial, or politically based motivators driving the intent; and (l) foreign influences. The second sub-question pertained to security strategies and early interventions. The final consensus on the most common security strategies and early interventions for insider threats in organizations was: (a) audits and network scannings; (b) separation of duties and training; (c) implementing multiple factor authentication to reduce data breaches; (d) ID cards, dual sign in, and multi-factor identification; (e) need to know access; and (f) security logs and cybersecurity training. The third sub-question pertained to policies and procedures for managing insider threats. The final consensus on the most common policies and procedures to manage insider threats in organizations was: (a) separation of duties, enforcement of the least privileged access; (b) regular monitoring

and access controls implementation; (c) logs and need-to-know policy; (d) apply log analysis as a part of your standard operating procedures; (e) limit third party access and social networks; and (e) include download virus protection in your policy.

Summary and Transition

In Chapter 4, I described the study findings and the ramifications of each response and provided supporting literature references to expand on SMEs answers. These findings and discussions of the impact of insider threats in organizations and what SMEs described as reasons, motivators, security strategies and early interventions are considered real-time industry practices. In Chapter 4, tabulated results, and associated explanations for achieving a 60% consensus were presented. This chapter includes the findings that SMEs described as real-time best security practices when handling insider threats in organizations. In Chapter 5, I discuss conclusions and interpretations of the study findings, where they converge with, or diverge from the body of literature, limitations, recommendations for future research, and the contribution of this research on social changes.

Chapter 5: Discussion, Conclusions, and Recommendations

This chapter includes a summary of the findings from this study on insider threats and data security management strategies, the overall research objectives, implications for research, industry best practices, limitations of the study, and recommendations for future research. In Chapter 4, I described the study findings and the ramifications of each response and provided supporting literature to explain the SMEs' answers. These findings and discussions of the impact of insider threats in organizations and what SMEs described as reasons, motivators, security strategies, early interventions, policies, and procedures are considered real-time best industry practices for this study.

Specifically, this study focused on these reasons, motivators, strategies, policies, and procedures for insider threat identification, prevention, and data security management to lead IT practitioners and new managers towards sustainability and secure working environments (Castellion & Markham, 2013; Stalla-Bourdillon, 2014; Talke & Snelders, 2013). This Delphi study included a purposeful sample of 25 IT SMEs' opinions in the Washington metropolitan area. The nature of the Delphi study facilitated the privacy of the SMEs, who were able to openly provide answers and offer feedback on the use of security and other aspects of risk management. In this study, I aimed to include a cross-sectional discussion of best industry practices and provide new knowledge about strategies for privacy and security to protect data and detail how SMEs manage insider threats from a global perspective, rather than from an individualized organizational perspective.

Interpretation of Findings

The results of this research on reasons for insider threats in private and public organizations are consistent with the peer-reviewed literature review. The results are also consistent with other best industry practices established by the NIST and NICE as common best practices for insider threat and risk management in general. The findings of this study align with previous research findings and other security practices issued by the NIST and NICE as recommended practices for insider threat management and data security administration, enabling opportunities to develop tailored security programs and employees' skill levels relevant to asset protection depending on each organization's risk baseline.

Reasons for Insider Threats

The SMEs agreed that the following were among the most common reasons for insider threats in organizations: (a) insufficient guidelines and training, (b) a lack of background investigations, and (c) financial gain and money (Jakobwitz & Egan, 2006; Maasberg, 2015; Ponemon, 2020). Overall, training took a predominant place in all areas of the three study rounds. These real-time findings confirmed the need for organizations to increase the stature of training on their priority list (Anderson, 2006; NICE, 2016; Society for Human Resource Management [SHRM], 2020). Training is frequently reduced or canceled during budget cuts due to a lack of an adequate return on investment metric; however, training benefits new employees and employees with tenure who can acquire new skills, sharpen outdated ones, and adjust to the ever-changing world of innovative technologies presenting a long-term benefit to individuals and organizations (NICE,2016; SHRM,2020). Background investigations are a necessity for organizations

doing business with the federal government, and after September 11, 2001, the private sector began tightening recruiting practices and onboarding to ensure transparency in the hiring process (NIST, 2016; OPM, 2020). Financial gain and money are self-explanatory, as they represent not only a reason, but also a motivator for insider threats in public and private organizations.

Motivators for Insider Threats

The SMEs agreed that the following were among the most common motivators for insider threats in organizations: (a) pushing boundaries; (b) financial gain; (c) hackers wanting to sell your information/ransomware; (d) money; (e) personal gain; (f) revenge and/or ideology; (g) entry-level employees wanting to do social networking at work; (h) disregard for authority; (i) retribution; (j) dislike of management; (k) bad intentions, emotional, financial, or politically based motivators driving intent; and (l) foreign influences (Maasberg et al., 2016).

Pushing boundaries can be viewed negatively as part of an individual's personality traits, or positively during an organizational change given an individual's aptitude to adjust and excel during the change process (Gheyas & Abdallah, 2016; Jouini, 2009; Zhao, 2016). The rest of the categories in this response group align with previous literature, research, and surveys, such as those of the Ponemon Institute (2017, 2018, 2019). However, in the interest of transparency of findings, they are presented without changes. The results of this study on motivators for insider threats in private and public organizations are consistent with the literature review and other best industry practices established by the NIST and NICE as common best practices for insider threats and risk management in general (NICE, 2016; NIST, 2016).

Security Strategies and Early Interventions

The SMEs agreed that the following were among the most common security strategies and early interventions for insider threats in organizations: (a) audits and network scannings; (b) separation of duties and training; (c) implementing multiple factor authentication to reduce data breaches; (d) ID cards, dual sign in, and multifactor identification; (e) need-to-know access; and (f) security logs and cybersecurity training.

In this category, several answers could have been grouped, as they are ultimately closely related, or applied to the same family tree. For example, separation of duties was related to need to know, as individuals are only given access to what they need to know to do their jobs. Implementing multifactor authentication and dual sign in were in the same control tree, but in the interest of transparency of findings and the number of responses, these remained as stand-alone answers (Arping & Sautner, 2012). The results of this study on security strategies and early interventions for insider threat prevention in private and public organizations and data security management are consistent with the literature review and other best industry practices established by the NIST, the NICE, and survey findings conducted by IBM and the Ponemon Institute (2017-2020) as common best practices for insider threats and data security management in general (NIST, 2016; NIST, 2016).

The relationship between access to information systems and human behavior is undeniable. This means that users need to be authenticated and authorized to access networks, data in any form, and facilities (NIST, 2016). Insider threats can be motivated by a variety of factors, including profiting from the activity or overuse of services via high-speed workplace computers, web portals, the Cloud, and peer-to-peer apps, all of

which increase dangers and accessibility to internal and external threats (Spitzner, 2013). Modernization and e-commerce have forced organizations to explore innovations to become more competitive, or to get best products, or services, making that access very tempting to users who feel motivated to access purchasing sites, movies, music, and other forms of social media and entertainment, leading to data breaches (Heilbrun & Brown, 2011; Schubert & Leimstoll, 2007). This excessive use of the Internet needs to be controlled through mandatory and discretionary access control policies, training, and standard operating procedures to prevent malware attacks from occurring on targeted systems, if users are not properly authenticated (NIST, 2016; Sastry, 2016; Spitzner, 2003).

Giving access to external unauthorized users may occur when outsiders provide credentials belonging to another user, or when internet transmissions are intercepted by someone else using an authorized user's credentials that may lead to malware and viruses that propagate from system to system if the proper security is not updated according to the vendor's recommendations (Gregory, 2017; Kui et al., 2012; Ziegeldorf et al., 2014).

Policies and Procedures to Manage Insider Threats

Policies and procedures defining standards of authorization for access requests and approvals, or separation of duties, ensure that no one person has too much power to exercise authorizations that may lead to ethical concerns and conflicts of interest (NIST, 2016, 2017). Additional government cyber security legislation was reviewed in Chapter 2. This legislation often rules the development of organizational policies and procedures. Policies and procedures that regulate employee access to facilities, networks, systems, and data are pivotal for the success of individuals and organizations. Employees only

need access to the equipment and systems they need to execute their jobs, according to NIST (2016)'s "least privileged access" policy. All further authorizations would require administrator access escalation and approval outside of this scope.

A comprehensive policy's value comes from the fact that it eliminates any doubt that employees may have about what to do in each situation. For example, if an organization has a policy that all visitors to the workplace must be always escorted, it will be much easier for employees to restrict access in this situation (Meyers, 2018). An organization that implements a separation of duties (SoD) policy not only complies with the Sarbanes-Oxley Act (SOX, 2002), but establishes checks and balances against the risk of breaches to the financial side of the company, and prepares the organization for FISMA audits, financial accuracy, and security controls. The expectation for separation of duties under the SOX Act of 2002, outlined requirements for IT departments regarding electronic records, or procedures that can be compromised by insider threats (Arping & Sautner, 2012; NIST, 2016).

A corporate security policy should serve to support security awareness, and outline in general terms, the procedures, roles, and responsibilities within the organization. The creation and enforcement of a security policy also demonstrate the organization's maturity level and compliance. In this study, the SMEs agreed that the following policies and procedures were the most commonly used for access control and manage insider threats in organizations: (a) separation of duties, and enforcement of the least privileged access, (b) regular monitoring and access controls implementation, (c) logs and need-to-know policy, (d) application of log analysis as a part of standard

operating procedures, (e) limitation of third party access and social networks, and (f) inclusion of download virus protection (firewalls) in the policy.

The SMEs' agreement contained in this study could aid in the introduction and advancement of security-related initiatives, as well as the enhancement of a positive working environment and the support of IT security policies. The study's findings may contribute to the body of knowledge regarding the return on investment derived from innovative technologies and training in organizations in the future. The results of this survey on policies and procedures to manage insider threats in private and public organizations are consistent with the literature review and other best industry practices established by the NIST and NICE as common best practices for insider threats and risk management in general.

Limitations of the Study

Because I only targeted 25 SMEs in the Washington metropolitan area (Washington, DC; Virginia; and Maryland), this survey had a limited sample, that could be seen as a limitation, or disadvantage. The size and composition of a panel are determined by the nature of the topics discussed, time constraints, and financial constraints (Habibi et al., 2014). The SMEs in this study came from both public and private sectors, and they represented a diverse workforce in the Washington metropolitan area. This small Delphi panel was suitable for purposive sampling given the study's nature (Miles et al., 2014).

While design, or methodological limitations may affect a research study, including issues of transferability and dependability, some limitations may represent possible flaws that go beyond the researcher's control (Kirkwood & Price, 2013). Experts

with the same level of knowledge and experience regarding insider threats were sought in this Delphi study that may have resulted in limitations (Grisham, 2009). However, this was not a concern because I had a LinkedIn network of over 750 accredited IT professionals as well as memberships in professional organizations such as the PMI, ISACA, and AFCEA, to name a few. Another limitation could have been attributed to conflicting schedules for gathering SMEs' responses, teleworking due to COVID-19, and continued commitment to go through the survey process within the allocated time. The availability of SMEs could have been affected due to loss of work, relocations, change of jobs, promotions, apathy, and internet accessibility. These limitations could have caused SMEs to drop out of the study at any time. However, 25 SMEs responded to the survey invitations, and 100% of those who responded participated in the duration of the study.

Recommendations for Future Research

The findings in this Delphi study suggest that cybersecurity and training play a pivotal role in the development of security awareness and safe working environments. The toxic behaviors that participating SMEs identified, as viewed through the lens of the dark triad theory, suggested that a relationship existed between toxic behaviors and insider threats (Albrechtsen & Hovden, 2010; Deloitte Center for Financial Services, 2014; Goodboy & Martin, 2015). These findings may be beneficial for organizations seeking to improve their organizational culture and employee engagement. The findings on employees' disregard for the organization is one that may require a root-case analysis to uncover how management, culture, and peer relation can curtail negative feelings fostered, or influenced by workplace behaviors (Schultz, 2014). Researchers should study

the relationship between employee personality, attitude, retention, and work satisfaction in future quantitative studies (Schultz, 2014).

This Delphi study results may or may not be applicable to all areas of the United States due to the small sample size; therefore, I recommend replicating this Delphi study in regions outside the Washington metropolitan area using a larger sample. Nonetheless, the issues of insider threats in organizations and data security management are considered a global problem for individuals and organizations (Ponemon, 2017). Quantitative studies on the return on investment (ROI) for hasty hiring decisions without the benefit of a full background investigation, or references, onboarding of employees without training, and offboarding of employees without proper debriefing or exit interviews may represent a risk that organizations should consider during their human capital planning. Because the need to raise awareness about insider threats grows with rapid innovation and changes in the way we manage projects, the inquiry for continuous research, both quantitative and qualitative becomes necessary. Real-time findings become outdated and the need for continuous education remains a constant in our day-to-day lives; therefore, a need for further research becomes imperative to gather best industry practices for safeguarding personally identifiable information, data security, and the integrity of the cybersecurity process that could prevent insider threats in organizations.

Implications of the Study

This qualitative Delphi study has provided SMEs opinions and best practices on reasons, and motivators for insider threats, and security strategies, policies, and procedures for the prevention and identification of risky behaviors and risks avoidance that could help public and private organizations when hiring, firing, developing policies,

procedures, and training. This Delphi study represents 8 years of research and analysis of peer-reviewed journals, recent research, IT surveys, and cases studies related to insider threats, compounded by the SMEs real-time responses based on their experiences and training that may provide a solid foundation for a better understanding of the new challenges and opportunities derived by innovative technology, the importance of training and positive working environments in the organization.

The dark triad theory was used to gather real-time information on how SMEs viewed this insider threats in the workplace. Some subproducts of the dark triad theory, such as narcissistic attitudes, a sense of superiority, and a desire for recognition and to impress others, were first presented in Round 1 open-ended questions in one variation, or another, aligning with characteristics studied by the FBI while examining insider threats' behaviors (see Tables 1 and 2).

The final consensus provided tools for new practitioners, academics, researchers, and IT managers responsible for employee hiring, onboarding, development, training, and offboarding. The managers leading new systems implementation, security, and data management may take advantage of this research to develop baseline countermeasures and prevent unauthorized physical and virtual access to organizational assets, hence, preserving the confidentiality, integrity, and accessibility of the data (NIST, 2016; NICE, 2016). Federal contractors who manage the government agency's IT environments need to safeguard data and maintain adequate levels of trained personnel, often certified personnel who possess the network, systems, and cybersecurity skills specified in contract requirements. The results of this study may facilitate the path for the creation of access controls concepts and models for their incident response plans and compliance

(ABA, 2017; NICE, 2017). Based on the results of this Delphi study, managers should strongly consider the application of a zero-trust policy when granting access to their physical and intellectual property in public and private organizations (Tables 7, 10). Employees in the least privileged group only have access to network/system assets needed to perform their jobs (Herold, 2010; NIST, 2016).

Social Change

Employee empowerment leads to social change. Employees who are empowered experience a risk-free environment that their employers trust and respect them (PMI, 2015). Public and private organizations' managers that implement effective security countermeasures create less stressful working conditions and boost employees' morale, productivity, and retention, promoting positive social change (NIST, 2016). Furthermore, creating a real-time deeper awareness of the impact that corporate culture, habits, security training, best industry practices, and employee buy-in play in strengthening data security management could help minimize insider threats and asset misuse. Prior case studies provided a historical pattern of the similarities in behavior that lead to insider threats' activities (Baughman et al., 2014).

In this chapter, I presented the SMEs' validation of the reasons, motivators, security strategies, early interventions, policies, and procedures for identifying and deterring insider threats in public and private organizations with the goal of protecting the confidentiality, integrity, and availability of personal and organizational data. The fulfillment of the purpose of this study for gathering real-time feedback from credentialed SMEs in the Washington metropolitan area for reasons, motivators, security strategies, early interventions, policies, and procedures has been satisfied. Additionally, increasing

awareness on cyber and insider threats provides managers, supervisors, and researchers with tools to develop their own security programs. The 25 participating SMEs' level of consensus seemed to support the implementation and development of training programs that could lead to professional activities enhancing positive social change that may support IT security policies. The dark triad theory portrayed a picture of how insider threats may respond to management policies and procedures and to external motivational factors influencing their behaviors in the workplace (Baughman et al., 2014). Recognizing the motivators for insider threats may increase an organization's opportunity to develop early countermeasures (Beck & Harter, 2015; Cohen, 2015).

The social change implications of the study may be that a greater awareness could be achieved about what security training programs and knowledge sharing are relevant to develop mandatory training, as a perspective for the survival of public and private organizations (Spector et al., 2005). The deterrence of potential insider threats, the enhancement of risk management strategies, the potential to decrease system sabotage, and the creation of new policies that could enhance individual and organizational safety and performance are prime functions in the prevention of intrusions, identity theft, and misuse of organizational assets (Hoffmann et al., 2012).

Understanding the dark triad behaviors can aid managers and senior leadership in reducing insider risks, fostering healthy working environments, managing employee dissatisfaction, and instilling honest and ethical behaviors at all levels of the organization (Sokolowski et al., 2016). Individuals who are aware of the dark triad theory may find it easier to interact with peers, and safely work with diverse groups creating enriched interactions, culture, and working environments. Lastly, private, and public organizations

can benefit from the National Institute of Standards and Technology (NIST) Security, Education, Training, Awareness (SETA) programs for managing social engineering risks, insider threats, remote multi-factor and password policies to manage insider threats in their organizations (NIST, SP 800-50).

This study included a cross-sectional discussion of real-time best business practices and security strategies for protecting the confidentiality, integrity, and accessibility of data, as presented by the SMEs' individual perspectives, rather than a company-funded overarching viewpoint. With the increasing challenges and risks that teleworking and emerging technologies presented to systems users and organizations in 2020, due to the COVID-19 pandemic, this study combined insider threats' awareness and security solutions from 25 certified IT participants from various organizations and industries, including government, private, public, and academia. This research could, in theory, result in a road map for new hires, supervisors, managers, researchers, and security administrators.

Conclusions from these findings could contribute to narrowing the gap in the literature regarding how to (a) more effectively recognize and prevent insider threats' activities and behaviors, (b) implement best industry practices, and (c) develop new training programs that could support professional development and enhance the profession. The study may also raise awareness of strategies to identify, detect, and prevent insider threats' activities and toxic behaviors.

Significance to Practice

Because of the increased use of IT in everyday operations, information systems have become vulnerable to insider attacks (NIST, 2016). As the need for faster

communications grows, IT systems have allowed expedited electronic communications for companies, education, and medical records access, opening the door to insider threats' mishaps (NIST, 2016). The use of the Cloud and Big Data present many opportunities for data loss (American Psychological Association, 2015; Clarke, 2016; Hashem et al., 2015). Insider breaches are user-centric; therefore, continuous monitoring and controls are needed for early prevention (Glasser & Lindauer, 2013). The SMEs' feedback may provide real-time preventive strategies and controls to identify and decrease insider threat behaviors and data breaches, as well as consensus about best practices among SMEs (Greitzer et al., 2013; NIST, 2016). Table 6 depicts the major categories used in this study's analytical framework for insider threats strategies and early interventions.

Significance to Theory

This qualitative Delphi study provides the SMEs unique perspective on real-time preventive strategies and controls for identifying and reducing insider threats' behaviors and data breaches. Future researchers may use the dark triad theory as a conceptual framework to gain new insights into real-time traits and behaviors, potentially enhancing the body of knowledge. The feedback from SMEs presented in this study may lead to better deterrence strategies and improved recruitment and training practices (Greitzer et al., 2013; NIST/NICE, 2016). There are implications for theory and practice that offer methods for defining dark triad characteristics in the workplace, as well as indicators for handling negative workplace behaviors. Unless the SME is a qualified psychologist, labeling a person under any of the dark triad categorizations for dark behaviors, or insider threat should be done with caution, and handled very carefully in collaboration with a trained human factors practitioner in the human resources department of the affected

organization. According to the results of this Delphi study, managers should take responsibility for managing the effects of negative attitudes in the workplace and fostering healthy working conditions to achieve the organization's mission and goals. Another crucial recommendation is that managers should not label, or stereotype workers based on a misunderstanding of what the dark triad categories mean.

IT practitioners and managers that exercise conflict resolution, emotional intelligence, constructive feedback, and provide insider threats training are using best practices to address situations where there is individual, or team conflict, or when there is a perception that the current organizational culture may foster insider threats' toxic behaviors. Consistent with best practices, managers should engage their human resource departments in any personnel action.

The results of this qualitative Delphi study could help companies improve their return on investment by preventing data breaches, increasing employee productivity and retention, and reducing dissatisfaction and costly departures. Pinder (2008) found a correlation between employee loyalty and dedication, as well as turnovers; employee departures could leave an organization vulnerable (Evans & Reeder, 2010; Kramer et al., 2011; Mahoney, 2011). Maasberg (2016) argued that, while the proposed relationship between dark triad personality traits, related constructs, and external process antecedents was derived from past literature, further empirical research was needed.

Conclusions

This Delphi study identified real-time reasons, motivators, strategies, and best industry practices in generating policies and procedures as recommended by 25 SMEs in the public and private sectors of the Washington metropolitan area during the period

2019-2020 and raised awareness about what traits and behaviors employees could display at work that align with the dark personality traits and behaviors of insider threats as depicted in the dark triad theory, prior studies and peer-reviewed literature.

Because of the demands, stressors, and challenges that new technology, system implementations, human resource management, and business requirements place on individuals, these findings may aid new managers, supervisors, students, system users, and academics in preventing intentional or unintentional data breaches that may be the result of toxic behaviors in the workplace. IT managers are responsible for leading their employees, and for providing training, development, and upward mobility opportunities while maintaining the integrity and quality of their programs. The findings of this study contribute to positive social change and the body of knowledge by recommending job-related training, cybersecurity training, mandatory training, and activities leading to professional development to manage the increasing demands of emerging technologies, insider threats, and data security management.

References

Abdallah, A. E., & Gheyas, I. A. (2016). Detection and prediction of insider threats to cybersecurity: A systematic literature review and meta-analysis. *Big Data Analytics, 1,* Article 6. https://doi.org/11.0186/s41044-016-0006-0

Adkins, A. (2015, May 7). *U.S. employee engagement holds steady at 31.7%.* Gallup Poll. https://news.gallup.com/poll/183041/employee-engagement-holds-steady.aspx

Adler, E. S., & Clark, R. (2015). *An invitation to social research: How it's done* (5th ed.). Cengage Learning. https://www.cengage.com/c/an-invitation-to-social-research-how-it-s-done-5e-adler/9781285746425PF/

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection: An intervention study. *Computers & Security, 29*(4), 432–445. https://doi.org/11.0016/j.cose.2009.12.005

Allen, I. E., & Seaman, C. A. (2007). Likert scales and data analyses. *Quality Progress, 40,* 64-65. http://asq.org/quality-progress/2007/07/statistics/likert-scales-and-data-analyses.html

American Bar Association (ABA). (2017). *Privacy, Cybersecurity & Digital Rights Committee.* ABA Journal. http://www.abajournal.com/

American Psychological Association (APA). (2015). Emerging ethical threats to client privacy in cloud communication and data storage. *Professional Psychology: Research and Practice, 46*(3), 154–160. https://doi.org/11.0037/pro0000018

Amigorena, F. (2014). The threat from within: How to start taking internal security more seriously. *Computer Fraud & Security, 2014*(7), 5–7. https://doi.org/11.0016/S1361-3723(14)70510-X

Anderson, R., & Moore, T. (2006). The economics of cybersecurity. *Science, 314*(5799), 610–613. https://doi.org/11.0126/science.1130992

Arping, S., & Sautner, Z. (2012). Did SOX Section 404 make firms less opaque? Evidence from cross-listed firms. *Contemporary Accounting Research*, *30*(2013), 1133–1165. https://doi.org/10.2139/ssrn.1561619

Assante, M., & Tobey, D. (2011). Enhancing the cybersecurity workforce. *IT Professional, 13*(1), 12–15. https://doi.org/11.0109/MITP.2011.6

Asselin, M., & Harper, M. (2014). Revisiting the Delphi technique: Implications for nursing professional development. *Journal for Nurses in Professional Development, 30*(1), 11–15. https://doi.org/11.0097/01.NND.0000434028.30432.34

Assenza, G., Chittaro, A., De Maggio, M. D., Mastrapasqua, M., & Setola, R. (2019). A review of methods for evaluating security awareness initiatives. *European Journal for Security Research, 5,* 259–287. https://doi.org/11.0007/s41125-019-00052-x

Avella, J. R. (2016). Delphi panels: Research design, procedures, advantages, and challenges. *International Journal of Doctoral Studies, 11,* 305–321. http://www.informingscience.org/Publications/3561

Avery, A., & Ranganathan, C. (2016, March). *Financial performance impacts of information security breaches* [Paper presentation]. WISP America

Ayofe, A., & Irwin, B. (2010). Cyber security: Challenges and the way forward. *Computer Science & Telecommunications*, *29*(6), 56–69.

Azizli, N., Atkinson, B. E., Baughman, H., Chin, M. K., Vernon, P. A., Harris, E., & Veselka, L. (2016). Lies and crimes: Dark triad, misconduct, and high-stakes deception. *Personality and Individual Differences*, *89*, 34–39. https://doi.org/11.0016/j.paid.2015.09.034

Bai, B. Y., Liu, X. X., & Kou, Y. (2014). Belief in a just world lowers perceived intention of corruption: The mediating role of perceived punishment. *PLoS ONE*, *9*(5), Article e97075. https://doi.org/11.0371/journal.pone.0097075

Balik, A. (2014). *The psychodynamics of social networking: Connected-up instantaneous culture and the self.* Routledge.

Baughman, H. M., Dearing, S., Giammarco, E., & Vernon, P. A. (2012). Relationships between bullying behaviours and the dark triad: A study with adults. *Personality and Individual Differences*, *52*(5), 571–575. https://doi.org/11.0016/j.paid.2011.11.020

Baughman, H. M., Jonason, P. K., Vernon, P. A., & Lyons, M. (2014). Liar liar pants on fire: Cheater strategies linked to the dark triad. *Personality and Individual Differences*, *71*, 35–38. https://doi.org/11.0016/j.paid.2014.07.019

Bauman, K. (2017). A twenty-first-century social contract between employers and job candidates. *Employment Relations Today*, *44*(2), 13–19. https://doi.org/11.0002/ert.21620

Beck, R., & Harter, J. (2015, April 21). Managers account for 70% of the variance in employee engagement. *Gallup Business Journal*. https://news.gallup.com/businessjournal/182792/managers-account-variance-employee-engagement.aspx

Beebe, N. L., & Rao, V. S. (2010). Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process. *Communications of the Association for Information Systems*, 26(1), 329–358. https://doi.org/11.07705/1CAIS.02617

Bell, B. G., & Grubin, D. (2010). Functional magnetic resonance imaging may promote theoretical understanding of the polygraph test. *Journal of Forensic Psychiatry and Psychology*, *21*(1), 52–65. https://doi.org/11.0080/14789940903220676

Bennett, J. (2016, August 21). Apparent Army Opsec brief lists Hillary Clinton, David Petraeus as examples of insider security threats. *Daily Caller*. http://dailycaller.com/2016/08/21/apparent-army-opsec-brief-lists-hillary-clinton-david-petraeus-as-examples-of-insider-security-threats/#ixzz4Pul3QJoT

Bharati, P., & Chaudhury, A. (2009). SMEs and competitiveness: The role of information systems. *International Journal of E-Business Research, 5*(1), i–ix. https://www.academia.edu/3657555/Bharati_P._and_Chaudhury_A._2009_SMEs_and_Competitiveness_The_Role_of_Information_Systems_International_Journal_of_E-Business_Research_Vol._5_No._1_pp._i-ix

Billies, M., Francisco, V., Krueger, P., & Linville, D. (2011). Participatory action research. *International Review of Qualitative Research, 3*(3), 277–286. https://doi/10.1177/160940691401300101

Billups, F. (2014). The quest for rigor in qualitative studies: Strategies for institutional researchers. The NERA Researcher, 1-5. https://www.airweb.org

Birko, S., Dove, E. S., & Özdemir, V. (2015). Evaluation of nine consensus indices in Delphi foresight research and their dependency on Delphi questionnaire characteristics: A simulation study and debate on Delphi design and interpretation. *PLoS ONE, 10*(8), Article e0135162. https://doi.org/11.0371/journal.pone.0135162

Boone, H., Jr., & Boone, D. A. (2012). Analyzing Likert data. *Journal of Extension, 50*(2), Article 2TOT2. https://archives.joe.org/joe/2012april/pdf/JOE_v50_2tt2.pdf

Borgatti, S. P., & Foster, P. C. (2003). *The network paradigm in organizational research: A review and topology.* Department of Organizational Studies. Carrol School of Management. https://journals.sagepub.com/doi/10.1016/S0149-2063_03_00087-4

Borgatti, S. P., Everett, G., & Johnson, J. C. (2013). *Analyzing social networks.* SAGE.

Borkowski, N., Deckard, G., Weber, M., Padron, L. A., & Luongo, S. (2011). Leadership development initiatives underlie individual and system performance in a U.S. public healthcare delivery system. *Leadership in Health Services, 24*(4), 268–280. https://doi.org/11.0108/17511871111172321

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone was watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151–164. https://doi.org/11.0057/ejis.2009.8

Brady, S. R. (2015). Utilizing and adapting the Delphi method for use in qualitative research. *International Journal of Qualitative Methods, 14*(5), 1–6. https://doi.org/11.0177/1609406915621381

Brenner, J. F. (2010). Privacy and security: Why isn't cyberspace more secure? *Communications of the ACM, 53*(11), 33–35. https://doi.org/11.0145/1839676.1839688

Brown, A., & Gilbert, B. (2014). The Pacific Medical Supply Workers Buddy Network: A regional professionalization activity. *Journal of Pharmacy Policy and Practice, 7,* Article O10. https://doi.org/11.0186/2052-3211-7-S1-O10

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548. http://131.08.86.27/faculty/warkentin/BIS9613papers/MISQ_SpecialIssue/BulgurcuCavusogluBenbasat2010_MISQ34_RationalityAwareness.pdf.

Burris, T., Rempel, J. K., Munteanu, A. R., & Therrien, P. A. (2013). More, more, more: The dark side of self-expansion motivation. *Personality and Social Psychology Bulletin, 39*(5), 578–595. https://doi.org/11.0177/0146167213479134

Cappelli, D. M., Trzeciak, R. F., & Moore, A. P. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (Theft, sabotage, fraud).* Addison-Wesley.

Carmichael, S. W. (2007). *True believer: Inside the investigation and capture of Ana Montes, Cuba's master spy.* Naval Institute Press.

Castellion, G., & Markham, S. K. (2013). Perspective: New product innovation failure rates: Influence of argumentum ad populum and self-interest. *Journal of Product Innovation Management, 30*(5), 976–979. https://doi.org/11.0111/j.1540-5885.2012.01009.X

Chang, T. S. (2010). *Handbook of research on computational forensics, digital crime, and investigation: Methods and solutions.* Information Science Reference.

Charmaz, K. (2014). *Constructing grounded theory* (2nd ed.). SAGE.

Che Ibrahim, C. K. I., Costello, S. B., & Wilkinson, S. (2013). Development of a conceptual team integration performance index for alliance projects. *Construction Management and Economics, 31*(11), 1128–1143. https://doi.org/11.0080/01446193.2013.854399

Chen, C. P., & Zhang, C. Y. (2014). Data-intensive applications, challenges, techniques, and technologies: A survey on big data. *Information Sciences, 275,* 314–347. https://doi.org/11.0016/j.ins.2014.01.015

Chondros, T. G. (2015). The Trojan Horse reconstruction. *Mechanism and Machine Theory, 90,* 261–282. https://doi.org/11.0016/j.mechmachtheory.2015.03.015

Ciampa, M. (2010). *Security awareness: Applying practical security in your world* (3rd ed.). Course Technology.

Clarke, R. (2016). Big data, big risks. *Information System Journal, 26*(1), 77–90. https://doi.org/11.0111/isj.12088

Claycomb, W. R., & Nicoll, A. (2012). *Insider threats to Cloud computing: directions for new research challenges* [Paper presentation]. IEEE 36th Annual Computer Software and Applications Conference. https://doi:10.1109/COMPSAC.2012.113

Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: Does size mater? *Journal of Advanced Nursing, 70*(3), 473–475. https://doi.org/11.011/jan.12163

Cohen, A. (2015). Are they among us? A conceptual framework of the relationship between the dark triad personality and counterproductive work behaviors (CWBs). *Human Resource Management Review, 26*(1), 69–85. https://doi.org/11.0016/j.hrmr.2015.07.003

Conrad, F. G., & Schober, M. F. (2000). Clarifying question meaning in a household telephone survey. *Public Opinion Quarterly, 64,* 1–28. https://doi.org/11.0086/316757

Cope, D. G. (2013). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum, 41*(1), 89–91. https://doi.org/11.0188/14.ONF.89-91

Corbin, J. M., & Strauss, A. (2015). *Basics of qualitative research*: *Techniques and procedures for developing grounded theory* (4th ed.). SAGE.

Cortina, L., & Magley, V. (2003). Raising voice, risking retaliation: Events following interpersonal mistreatment in the workplace. *Journal of Occupational Health Psychology, 8*(4), 247–265. https://doi.org/11.0037/1076-8998.8.4.247

Crysel, L. C., Crosier, B. S., & Webster, G. D. (2013). The dark triad and risk behavior. *Personality and Individual Differences, 54*(1), 35–40. https://doi.org/11.0016/j.paid.2012.07.029

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98. https://10.1287/isre.1070.0160

Dang-Pham, D. P. T. (2014, May). *Predicting insider's malicious security behaviours: A general strain theory based conceptual model* [Paper presentation]. 2014 International Conference on Information Resources Management. https://www.academia.edu/11630556/Predicting_Insider_s_Malicious_Security_Behaviours_A_General_Strain_Theory_Based_Conceptual_Model

Davies, E., Martin, J., & Foxcroft, D. (2016). Development of an adolescent alcohol misuse intervention based on the Prototype Willingness Model: A Delphi study. *Health Education, 116*(3), 275–291. https://doi.org/11.0108/HE-01-2015-0006

de Loë, R. C., Melnychuk, N., Murray, D., & Plummer, R. (2016). Advancing the state of policy Delphi practice: A systematic review evaluating methodological evolution, innovation, and opportunities. *Technological Forecasting and Social Change, 104*, 78–88. https://doi.org/11.0016/j.techfore.2015.12.009

Deloitte Center for Financial Services. (2014). *Transforming cybersecurity: New approaches for an evolving threat landscape.* https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/dttl-fsi-TransformingCybersecurity-2014-02.pdf

Deloitte TMT Survey Security. (2013). *Deloitte 2013 TMT global security survey.* https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/dttl_TMT_

Denis, J. L., Langley, A., & Rouleau, L. (2010). The practice of leadership in the messy world of organizations. *Leadership, 6*(1), 67–88. https://doi.org/11.0177/1742715009354233

Denis, J. L., Langley, A., & Sergi, V. (2012). Leadership in the plural. *The Academy of Management Annals, 6*(1), 211–283. https://doi.org/10.5465/19416522.0012.667612

Department of Homeland Security. (2013). Cybersecurity: What every CEO should be asking. https://www.us-cert.gov/security

Diamond, I. R., Grant, R. C., Feldman, B. M., Pencharz, P. B., Ling, S. C., Moore, A. M., & Wales, P. W. (2014). Defining consensus: A systematic review recommends methodologic criteria for reporting of Delphi studies. *Journal of Clinical Epidemiology, 67*(4), 401–409. https://doi.org/11.0016/j.jclinepi.2013.12.002

Diller, J. W., & Nuzzolilli, A. E. (2012). The science of values: The moral landscape by Sam Harris. *The Behavior Analyst, 35*(2), 265–273.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), Article 23. https://doi.org/11.07705/1jais.00133

Drucker, P. F., Collins, J., Kotler, P., Kouzes, J., Rodin, J., Kasturi, R., & Hesselbein, F. (2008). *The five most important questions you will ever ask about your organization.* Leadership to Leader Institute. Jossey-Bass.

Equifax. (2017). *Consumer notice.* Retrieved November 19, 2017, from https://www.equifaxsecurity2017.com/consumer-notice/

Evans, K., & Reeder, F. (2010). *A human capital crisis in cybersecurity: Technical proficiency matters: A report of the CSIS commission on cybersecurity for the 44th presidency.* Center for Strategic & International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101111_Evans_HumanCapital_Web.pdf

Federal Bureau of Investigation. (2016a). *Aldrich Ames.* https://www.fbi.gov/history/famous-cases/aldrich-ames

Federal Bureau of Investigation. (2016b). *Brian P. Regan espionage.* https://www.fbi.gov/history/famous-cases/brian-p-regan-espionage

Federal Bureau of Investigation. (2016c). *Law enforcement enterprise portal (LEEP).* https://www.fbi.gov/services/cjis/leep

Federal Bureau of Investigation. (2016d). *Robert Hanssen.* https://www.fbi.gov/history/famous-cases/robert-hanssen

Federal Bureau of Investigation. (2017). *Naval espionage: Stopping a dangerous threat.* https://www.fbi.gov/news/stories/naval-espionage-stopping-a-dangerous-insider-threat

Federal Information Security Management Act (FISMA). (2002), 44 U.S.C. Ch. 35, 40 U.S.C., §11331, & 15 U.S.C., §278. https://www.congress.gov/bill/107th-congress/house-bill/3844

Federal Information Technology Acquisition Reform Act (FITARA*).* (2014). Pub. L. No. 113-291, div. A tit. VIII, subtitle D, 128 Stat. 3292, 3438-50. https://www.congress.gov/bill/113th-congress/house-bill/1232

FedRAMP. (2017). *FedRamp marketplace.* Retrieved February 26, 2021, from https://marketplace.fedramp.gov/#!/products?sort=productName

FedRAMP. (2017). U.S. General Services Administration, OMB Max: A guide for Agencies (2017). https://www.fedramp.gov/

Ferreira, A., & Otley, D. T. (2009). The design and use of management control systems: An extended framework for analysis. *Management Accounting Research, 20*(4), 263–282. https://doi.org/11.0016/j.mar.2009.07.003

Figueredo, A. J., Gladden, P., Sisco, M., Patch, E., & Jones, D. (2015). The unholy trinity: The dark triad, coercion, and Brunswik-Symmetry. *Evolutionary Psychology, 13*(2), 435–454. https://doi.org/11.0177/147470491501300208

Financial Services Modernization Act. (1999). Publication L, 106–102, 113 Stat., 1333.

Fink, A. S. (2000). The role of the researcher in the qualitative research process. A potential barrier to archiving qualitative data. *Forum: Qualitative Social Research, 1*(3), Article 4. https://www.qualitative-research.net/

Firmin, M., Bouchard, V., Flexman, J., & Anderson, D. (2014). A qualitative analysis of students' perceptions of pursuing pharmacy as a potential vocation. *The Qualitative Report, 19*(40), 1–12. https://nsuworks.nova.edu/tqr/vol19/iss40/2/

Flaherty, A., Day, C., & Yen, H. (2016, July 24). *Hacked emails overshadow Democratic National Convention*. Public Broadcasting Service. http://www.pbs.org/newshour/rundown/hacked-emails-overshadow-democratic-nationalconvention/

Förster, B., & Von der Gracht, H. (2014). Assessing Delphi panel composition for strategic foresight — A comparison of panels based on company-internal and external SMEs. *Technological Forecasting and Social Change, 84*, 215–229. https://doi.org/11.0016/j.techfore.2013.07.012

Frank, O. (2011). Survey sampling in networks. In J. Scott & P. Carrington (Eds), *The Sage handbook of social network analysis.* SAGE.

French, P., Yin Yu, H., & Lee, L. S. (2002). A Delphi survey of evidence-based nursing priorities in Hong Kong. *Journal of Nursing Management, 10*(5), 265–273. doi: http://dx.doi.org/10.1046/j.1365-2834.2002.00314.x

Furnham, A., Hyde, G., & Trickey, G. (2014). The dark side of career preference: Dark side traits, motives, and values. *Journal of Applied Social Psychology, 44*(2), 106–114. https://doi.org/11.0111/jasp.12205

Fusch, P. L., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20,* 1408–1416. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2281&context.

Gale, N. K., Heath, G., Cameron, E., Rashid, S., & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology, 13,* Article 117. http://doi.org/11.0186/1471-2288-13-117

Gallego, D., & Bueno, S. (2014). Exploring the application of the Delphi method as a forecasting tool in information systems and technologies research. *Technology Analysis & Strategic Management, 26*(9), 987–999. https://doi.org/11.0080/09537325.2014.941348

Gansler, J., Lucyshyn, W., & Rigilano, J. (2012). *Toward a valid comparison of government and contractor costs.* Calhoun: Institutional Archive of the Naval Postgraduate School. https://calhoun.nps.edu/bitstream/handle/10945/54492/UMD-CE-11-209.pdf?sequence=1&isAllowed=y

Gelles, M. G., & Mahoutchain, T. (2012). *Mitigating the insider threat: Building a secure workforce* [Conference session]. FISSEA 25th Annual Conference, Gaithersburg, Maryland. https://csrc.nist.gov/CSRC/media/Presentations /Mitigating-the-Insider-Threat-Building-a-Secure/images-media/fissea-conference-2012_mahoutchian-and-gelles.

General Services Administration, FedRAMP. (August 31, 2020). https://www.gsa.gov/technology/government-it-initiatives/fedramp

Ghazzawi, I. (2010). Job satisfaction among information technology professionals in the U.S. An empirical study. *Journal of Organizational Culture, Communications and Conflict, 14*(2), 1–34.

Giammarco, E. A., & Vernon, P. A. (2015). Interpersonal guilt and the dark triad. *Personality and Individual Differences, 81,* 96–101. https://doi.org/11.0016/j.paid.2014.10.046

Glasser, J., & Lindauer, B. (2013). *Bridging the gap: A pragmatic approach to generating insider threat data* [Paper presentation]. 2013 IEEE Security and Privacy Workshops, San Francisco, CA, United States.

Golden, E. (2014). *Internet stalking 101: The dos and don'ts of internet creeping*. Thought Catalog. http://thoughtcatalog.com/emma-golden/2014/02/the-dos-and-donts-of-internet-creeping/

Goodboy, A. K., & Martin, M. M. (2015). The personality profile of a cyberbully: Examining the dark triad. *Computers in Human Behavior, 49,* 1–4. https://doi.org/11.0016/j.chb.2015.02.052

Gottschalg, O., & Zollo, M. (2007). Interest alignment and competitive advantage. *Academy of Management Review*, *32*(2), 418–437. https://doi.org/10.5465/amr.2007.24351356

Graneheim, U. & Lundman, B. (2004). "Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness." *Nurse Education Today*. *24* (2): 105–112. https://doi.org/11.0016%2Fj.nedt.2003.10.001

Green, D. (2014). Insider threats and employee deviance: developing an updated typology of deviant workplace behaviors. *Issues in Information Systems 15*(2), 185–189. https://doi.org/10.48009/2_iis_2014_185-189

Gregory, P. H. (2017). *CISA: Certified information systems auditor* (3rd ed.). McGraw-Hill.

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. R., & Ferryman, T. (2013). Psychological modeling of insider threat risk based on behavioral, and word use analysis. *e-Service Journal*, *9*(1), 106–110. https://doi.org/12.0979/eservicej.9.1.106

Grisham, T. (2009). The Delphi technique: A method for testing complex and multifaceted topics. *International Journal of Managing Projects in Business, 2*(1), 112–130. https://doi.org/11.0108

Guo, K. (2013). Security-related behavior in using information systems in the workplace. *Computers and Security, 32*, 242–245. https://doi.org/11.0016/j.cose.2012.10.003

Habibi, A., Sarafrazi, A., & Izadyar, S. (2014). Delphi technique theoretical framework in qualitative research. *International Journal of Engineering and Science, 3*(4), 8–13. http://theijes.com/papers/v3-i4/Version-4/B03404008013.pdf

Habibi, A., Sarafrazi, A., & Izadyar, S. (2015). Fuzzy Delphi technique for forecasting and screening items. *Asian Journal of Research in Business Economics and Management, 5*(2), 130–143. http://doi:10.5958/2249-7307.2015.00036.5

Habibi, A., Sarafrazi, A., & Izadyar, S. (2014). Delphi Technique Theoretical Framework in Qualitative Research, *International Journal of Engineering and Science, 3*(4), 8–13. http://theijes.com/papers/v3-i4/Version-4/B03404008013.pdf

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis.* Prentice Hall.

Halpern, E., & Leite, L. C. (2015). The role of the researcher when using the socio-anthropological method to understand the phenomenon of alcoholism. *Open Journal of Social Sciences, 3*(5), 76–81. http://dx.doi.org/10.4236/jss.2015.35011

Hampton, J. (2009). *Fundamentals of enterprise risk management: How top companies assess risk, manage exposure, and seize opportunity.* AMACOM.

Hampton, K., Rainie, L., Lu, W., Dwyer, M., Shin, I., & Purcell, K. (2014). *Social media and the 'spiral of silence,'* Pew Research Center Project Survey. https://www.pewresearch.org/internet/2014/08/26/social-media-and-the-spiral-of-silence/

Hancock, D. R., & Algozzine, B. (2015). *Doing case study research: A practical guide for beginning researchers* (2nd ed). Teachers College Press.

Hancock, M. E., Amankwaa, L., Revell, M. A., & Mueller, D. (2016). Focus group data saturation: A new approach to data analysis. *Qualitative Report, 21*(11), 2124–2130. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2330&context=tqr

Harris, S. (2010). *The moral landscape: How science can determine human values.* Free Press.

Harvard University. (2020). Conflict Resolution. https://www.pon.harvard.edu/daily

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, G. A., & Khan, S. U. (2015). The rise of "big data" on cloud computing review and open research issues. *Information Systems, 47,* 98–115. https://doi.org/11.0016/j.was.2014.07.006

Hasib, M. (2013). Impact of security culture on security compliance in healthcare in the United States of America: Capitol College. Adapted from "A Model for Information Assurance: An Integrated Approach," by W. V. Maconachy, C. D. Schou, D. Ragsdale, and D. Welch, 2001, June. Paper presented at the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, New York: New York and "Cybersecurity Leadership: Powering the Modern Organization," by M. Hasib, 2014

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing, 32*(4), 1008–1015. https://doi.org/11.0046/j.1365-2648.2000.t01-1-01567.x

Haynes, C., & Shelton, K. (2018). Delphi method in a digital age: Practical considerations for online Delphi studies. In V. X. Wang & T. G. Reio Jr. (Eds.), *Handbook of research on innovative techniques, trends, and analysis for optimized research methods* (pp. 132–151). IGI Global.

Health Insurance Portability and Accountability Act (HIPAA). (1996). Pub. L. No. 104-191, § 264, 110 Stat. 1936.

Heilbrun, M. R., & Brown, I. (2011). Cybersecurity policy and legislation in the 112th Congress. *Intellectual Property & Technology Law Journal*, *23*(12), 14–20. http://www.aspenpublishers.com/product.asp?catalog_name=Aspen&product_id=SS10413952

Herold, R. (2010). *Managing an information security and privacy awareness and training program*. CRC Press.

Hilbert, M., & Davis, C. A. (2015). *How technology evolves: Combinatorics.* Vol. UC-wide online course. http://c2.ucdavis.edu

Hodson, G., Hogg, S. M., & MacInnis, C. C. (2009). The role of "dark personalities" (narcissism, Machiavellianism, psychopathy), big five personality factors, and ideology in explaining prejudice. *Journal of Research in Personality, 43,* 686–690. https://doi.org/11.0016/j.jrp.2009.02.005

Hoffmann, L., Burley, D., & Toregas, C. (2012). Holistically building the cybersecurity workforce. *IEEE Security & Privacy, 10*(2), 33–39. https://doi.org/11.0109/MSP.2011.181

Hohmann, E. M., Brand, J. C., Rossi, M. J., & Lubowitz, J. H. (2018). Expert opinion was necessary: Delphi panel methodology facilitates a scientific approach to consensus *Arthroscopy, 34*(2), 349–351. https://doi.org/11.0016/j.arthro.2017.11.022

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case study research. *Nurse Researcher, 20*(4), 12–17. https://doi.org/10.7748/nr2013.03.20.4.12.e326

Hsu, C. C., & Sandford, B. A. (2007). The Delphi technique: making sense of consensus. *Practical Assessment Research & Evaluation, 12*(10), Article 10. https://doi.org/10.7275/pdz9-th90

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615–659. https://doi.org/11.0111/j.1540-5915.2012

Hunton, J. E., & Norman, C. (2010). The impact of alternative tele work arrangements on organizational commitment: Insights from a longitudinal field experiment. *Journal of Information Systems, 24*(1), 67–90. https://doi.org/12.0308/jis.2012.04.1.67

International Organization for Standardization (ISO). (2013), ISO 27001.

International Electro-Technical Commission (IEC). (2009). I EC 15408-1.

Irving, P. G., & Montes, S. D. (2010). Met expectations: The effects of expected and delivered inducements on employee satisfaction. *Journal of Occupational and Organizational Psychology, 82*(2), 431–451. https://doi.org/11.0348/096317908X312650

Jacob, S. A., & Ferguson, S. P. (2012). Writing interview protocols and conducting interviews: Tips for students new to the field of qualitative research. *The Qualitative Report, 17*(42), 1–10. https://nsuworks.nova.edu/tqr/vol17/iss42/3/

Jakobwitz, S., & Egan, V. (2006). The dark triad and normal personality traits. *Personality and Individual Differences, 40*(2), 331–339. https://doi.org/11.0016/j.paid.2005.07.006

Janesick, V. J. (2011). *Stretching exercises for qualitative researchers* (3rd Ed.). SAGE.

Jonason, P. K., Abboud, R., Dummett, M., & Hazer, A. (2014). Occupational niches and the dark triad traits. *Personality and Individual Differences, 69,* 119–123. https://doi.org/11.0016/j.paid.2014.05.024

Jonason, P. K., Abboud, R., Dummett, M., & Hazer, A. (2017). The dark triad traits and individual differences in self-reported and other-rated creativity. *Personality and Individual Differences, 117,* 150–154. https://doi.org/11.0016/j.paid.2017.06.005

Jordan, P. J., Ramsay, S., & Westerlaken, K. M. (2016). A review of entitlement: Implications for workplace research. *Organizational Psychology Review, 7*(2), 122–142. https://doi.org/11.0177/2041386616647121

Joyner, H., & Smith, D. (2015). Using Delphi surveying techniques to gather input from non-academics for development of a modern dairy manufacturing curriculum. *Journal of Food Science Education, 14*(3), 88–117. https://doi.org/11.0111/1541-4329.12062

Kalaian, S., & Rafa, M. K. (2012). Terminating sequential Delphi survey data collection. *Practical Assessment, Research & Evaluation, 17,* Article 5. https://doi.org/10.7275/g48q-je05

Kaplan, E., & Hecker, C. (2014, April 17). *Understanding the many facets of insider threats.* Forbes. https://www.forbes.com/sites/riskmap/2014/04/17/understanding-the-many-facets-of-insider-threats/?sh=264e048d7ef7

Kaspersky. (2013). *Spam statistics report Q2-2013.* Retrieved October 24, 2017, from https://usa.kaspersky.com/resource-center/threats/spam-statistics-report-q2-2013

Kirkwood, A., & Price, L. (2013). Examining some assumptions and limitations of research on the effects of emerging technologies for teaching and learning in higher education. *British Journal of Educational Technology, 44*(4), 536–540. https://doi.org/11.0111/bjet.12049

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014, February). *Learning from "Shadow security": Why understanding non-compliance provides the basis for effective security* [Paper presentation]. Workshop on Usable Security.

Kornbluh, M. (2015). Combatting challenges to establishing trustworthiness in qualitative research. *Qualitative Research in Psychology, 12*(4), 397–400. https://doi.org/11.0080/14780887.2015.1021941

Kramer, F. D., Starr, S. H., & Wentz, L. K. (2011). *Cyberpower and national security.* Potomac Books.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, *27*(5–6), 224–231. https://doi.org/11.0016/j.cose.2008.05.006

Kuean, W. L., Kaur, S. S., & Wong, E. K. (2010). The relationship between organizational commitment and intention to quit: The Malaysian companies' perspectives. *Journal of Applied Sciences, 10*(19), 2251–2260. https://doi.org/10.3923/jas.2012.0251.2260

Kui, R., Cong, W., & Qian, W. (2012). Security challenges for the public Cloud. *IEEE Internet Computing, 16*(1), 69–73. https://doi.org/11.0109/MIC.2012.14

Kuman, D., & Morarjee, K. (2014). Insider data theft detection using decoy and user behavior profile. *International Journal of Research in Computer Applications and Robotics, 2*(2), 51–55

Kurtessis, J. N., Eisenberger, R., Ford, M. T., Buffardi, L. C., Stewart, K. A., & Adis, C. S. (2015). Perceived organizational support: A meta-analytic evaluation of organizational support theory. *Journal of Management,* 43(6), 1854–1884. https://doi.org/11.0177/0149206315575554

Latest Technologies. (2011). (ISC) 2®- *Global information security workforce study*. http://www.prnewswire.com/news-releases/latest-technologies training-cyber-security-staffs-study-warns-116412284.html

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

Legg, P. A., Moffatt, N. J. R., Nurse, J. R. C., Happa, J., Agrafiotis, M. G., & Creese, S. (2017). Towards a conceptual model and reasoning structure for insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4*(4), 20–37. https://doi.org/12.02667/JOWUA.2013.12.31.020

Lincoln, Y. S., & Guba, E. G. (2000). Paradigmatic controversies, contradictions, and emerging confluences. In N. K. Denzin & Y. S. Lincoln (Eds.), *The handbook of qualitative research* (2nd ed.; pp. 163–188). SAGE.

Loeser, F. (2013). *Green IT and Green IS: Definition of constructs and overview of current practices* [Paper presentation]. The 19th Americas Conference on Information Systems.

Londoño, E. (2014, April 23). Convicted leaker Bradley Manning changes legal name to Chelsea Elizabeth Manning. *The Washington Post.* https://www.washingtonpost.com/world/national-security/convicted-leaker-bradley-manning-changes-legal-name-to-chelsea-elizabeth-manning/2014/04/23/e2a96546-cb1c-11e3-a75e-463587891b57_story.html https://www.washingtonpost.com/world/nationalsecurity/convicted-leaker-bradley

Ludwig, B. (1997). Predicting the future: Have you considered using the Delphi methodology? *Journal of Extension, 35*(5), Article 5. http://158.132.155.107/posh97/private/research/methods-delphi/future.pdf

Maasberg, M., Warren, M. J., & Beebe, N. L. (2016). *The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits* [Paper presentation]. 2015 48th Hawaii International Conference on System Sciences.

Maddox, L., & Mehta, D. (2011). Focus groups: "Traditional vs. Online." Survey Magazine, March. https://researchdesignreview.com

Mahoney, M. (2011). Randomized algorithms for matrices and data. *Foundations and Trends in Machine Learning, 3*(2), 123–224. https://doi.org/11.0561/2200000035

Majchrzak, A., & Markus, M. L. (2013). Technology affordances and constraints theory (of MIS). In E. Kessler (Ed.), *Encyclopedia of management theory* (pp. 832–836). SAGE.

Mallery, J. (2009). Building a secure organization. In J. R. Vacca (Ed.), *Computer and information security handbook* (pp. 3–21). Morgan Kaufmann.

Marshak, R. J. (2005). Contemporary challenges to the philosophy and practice of organization development. In D. L. Bradford & W. W. Burke (Eds.), Reinventing organization development: New approaches to change in organizations (pp. 19–42).

Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research* (6th ed.). SAGE.

Maslow, A. H. (2012). *A theory of human motivation.* Maslow's Hierarchy of Needs (1954)

Maxwell, J. (2013). Qualitative research design: An interactive approach. SAGE.

Mayer, B. (2012). *The dynamics of conflict: A guide to engagement and intervention.* Jossey-Bass

McAfee, A., & Brynjolfsson, E. (2012). Decision-making. Big data: The management revolution. *Harvard Business Review, 90*(10), 60–66, 68, 128. https://hbr.org/2012/10/big-data-the-management-revolution

Meyers, M. (2018). *CompTIA network+ certification all-in-one exam guide, seventh edition (exam N10-007)* (7th ed.). McGraw-Hill Education.

Miles, M. B., Huberman, M. A., & Saldaña, J. (2014). *Qualitative data analysis - A methods sourcebook.* SAGE.

Moore, A., Cappelli, D., & Trzeciak, R. (2008). The big picture of inside IT sabotage across the U.S. critical infrastructures. In S. J. Stolfo, S. M. Bellovin, S. Hershkop, A. D. Keromytis, S. Sinclair, & S. Smith (Eds.), *Insider attack and cyber security* (pp. 17–52). Springer.

Moustakas, C. (2015). Heuristic research: Design and methodology. In K. J. Schneider, J. F. Pierson, J. F. T. Bugental (Eds.), *The handbook of humanistic psychology: Theory, research, and practice* (2nd ed.; pp. 309–320). SAGE.

Muelder, C., Ma, K. L., & Bartoletti, T. (2005). Interactive visualization for network and port scan detection. In A. Valdes & D. Zamboni (Eds.), *Recent advances in intrusion detection* (pp. 265–283). Springer.

National Initiative for Cybersecurity Education (NICE). (2018). National Institute of Standards and Technology (NIST). http://csrc.nist.gov/nice

National Institute of Standards and Technology. (2018). *FISMA implementation project.* Retrieved July 1, 2015, from http://csrc.nist.gov/groups/SMA/fisma/framework.html

National Institute of Standards and Technology. (2014). Roadmap for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014,

National Institute of Standards and Technology (NIST). (2016). *Risk management framework (RMF) overview.* http://csrc.nist.gov/groups/SMA/fisma/framework.html

National Institute of Standards and Technology. (2018). *Risk Management Framework* (2014). http://csrc.nist.gov/groups/SMA/fisma/framework.html

Nevin, A. D. (2015). *Cyber-psychopathy: Examining the relationship between Dark e-personality and online misconduct* [Master's thesis, The University of Western, Ontario]. Western Graduate & Postdoctoral Studies Electronic Thesis and Dissertation Repository. https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=4531&context=etd

Nguyen, T. H., Yang, R., Azaria, A., Kraus, S., & Tambe, M. (2013). "Analyzing the effectiveness of adversary modeling in security games. In *AAAI '13: Proceedings of the twenty-seventh AAAI conference on artificial intelligence* (pp. 718–724). AAAI Press.

Niederman, F., Ferratt, T. W., & Trauth, E. M. (2016). On the co-evolution of information technology and information systems personnel. *ACM SIGMIS*

Nurse, J. R. C., Legg, P. A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Upton, D., Goldsmith, M. & Creese, S. (2014a). Understanding insider threat: A framework for characterizing attacks. In *2014 IEEE security and privacy workshop* (pp. 214–228). IEEE Press.

Nurse, J. R. C., Legg, P. A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Upton, D., Goldsmith, M., & Creese, S. (2014b). A critical reflection on the threat from human insiders – Its nature, industry perceptions, and detection approaches. In T. Tryfonas & I. Askoxylakis (Eds.), *Human aspects of information security, privacy, and trust* (pp. 270–281). Springer.

O'Boyle, E. H., Forsyth, D. R., Banks, G. C., & McDaniel, M. A. (2012). A meta-analysis of the dark triad and work behavior: A social exchange perspective. *Journal of Applied Psychology, 97*(3), 557–570. https://doi.org/11.0037/a0025679

Onwuegbuzie, A. J., Leech, N. L., & Collins, K. M. (2012). Qualitative analysis techniques for the review of the literature. *The Qualitative Report, 17*(28), 1–28. https://nsuworks.nova.edu/tqr/vol17/iss28/2

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: An insider threat perspective. *Decision Support Systems, 92*, 47–56. https://doi.org/11.0016/j.dss.2016.09.012

Padilla, A., Hogan, R., & Kaiser, R. B. (2007). The toxic triangle: destructive leaders, susceptible followers, and conducive environments. *The Leadership Quarterly, 18*(3), 176–194. https://doi.org/11.0016/j.dss.2016.09.012

Page, J. (2015). 4 different types of attacks - Understanding the “insider threat”. Cloud Tweaks. Retrieved February 26, 2021, from https://cloudtweaks.com/2015/01/attacks-understanding-insider-threat/

Palfrey, J., & Gasser, U. (2008). *Born digital: Understanding the first generation of digital natives.* Basic Books.

Panetta, K. (2017, October 3). *Gartner top 10 strategic technology trends for 2018.* Gartner. https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/

Papageorgiou, K. A., Wong, B., & Clough, P. J. (2017). Beyond good and evil: Exploring the mediating role of mental toughness on the dark triad of personality traits. *Personality and Individual Differences 119,* 19–23. https://doi.org/11.0016/j.paid.2017.06.031

Parker, J. F. (2008). *Do the right thing.* Wharton School.

Patton, M. Q. (2015). Qualitative research and evaluation methods (4th ed.). SAGE.

Paulhus, D. L., & Williams, K. M. (2002). The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality, 36*(6), 556–563. https://doi.org/11.0016/S0092-6566(02)00505-6

Pearlson, K. E., Saunders, C. S., & Galletta, D. F. (2016). *Managing and using information systems* (6th ed.). Wiley.

Persson, B. N., Kajonius, P. K., & Garcia, D. (2017). Testing construct independence in the short dark triad using item response theory. *Personality and Individual Differences, 117,* 74–80. https://doi.org/11.0016/j.paid.2017.05.025

Peterson, A. (2014, March 7). Snowden: I raised NSA concerns internally over 10 times before going rogue. *The Washington Post.* https://www.washingtonpost.com/news/the-switch/wp/2014/03/07/snowden-i-raised-nsa-concerns-internally-over-10-times-before-going-rogue/

Pew Research Center Project Survey. (2017).

Pinder, C. C. (2008). *Work motivators in organizational behaviors* (2nd ed.). Psychology Press.

Poe, D. (2011, September 29). *Briefing outlines security measures on JBLM*. U.S. Army. https://www.army.mil/article/66424/briefing_outlines_security_measures

Ponemon Institute. (2015, October). *2015 cost of cybercrime study: United States.* https://www.ponemon.org/local/upload/file/2015%20US%20CCC%20FINAL%204.pdf.

Ponemon Institute. (2016, June). *2016 cost of data breach study: Global analysis.* https://www.cloudmask.com/hubfs/IBMstudy.pdf

Ponemon Institute. (2017). *2017 cost of data breach study: Global analysis benchmark research.* https://www.ncsl.org/documents/taskforces/IBM_Ponemon2017CostofDataBreachStudy.pdf

Ponemon Institute (2020). *Cost of insider threats*: *Global Report*. IBM Security.

Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes *Computers and Security, 30*(6–7) 486–497. https://doi.org/11.0016/j.cose.2011.05.002

PricewaterhouseCoopers (PwC). (2020). CISO's hurdle an extreme test of resilience, plan to emerge stronger. PwC's Digital Trust Insights Pulse Survey Findings, 17.

Privacy Act. (1974). 5 U.S.C. § 552a.

Project Management Institute. (2015). *A guide to the project management body of knowledge.* Project Management Institute.

Rabai, B. A., Jouini, M. L., Aissa, Ben, & Mili, A. (2014). A cybersecurity model in Cloud computing environments. *Journal of King Saud University– Computer and Information Sciences, 25*(1), 63–75. https://doi.org/11.0016/j.jksuci.2012.06.002

Radack, D. V. (1994). Understanding confidentiality agreements. *Journal of Management, 46*(5), 68. https://doi.org/11.0007/BF03220704

Raley, M. E., Ragona, M., Sijtsema, S. J., Fischer, A. R., & Frewer, L. J. (2016). Barriers to using consumer science information in food technology innovations: An exploratory study using Delphi methodology. *International Journal of Food Studies, 5*(1), 39–53. https://doi.org/10.7455/ijfs/5.1.2016.a4

Rhoades, L., & Eisenberger, R. (2002). Perceived organizational support: A review of the literature. *Journal of Applied Psychology, 87*(4), 698–714. https://doi.org/11.0037/0021-9010.87.4.698

Riiskjær, E., Ammentorp, J., & Kofoed, P. E. (2012). The value of open-ended questions in surveys on patient experience: number of comments and perceived usefulness from a hospital perspective. *International Journal for Quality in Health Care, 24*(5), 509–516, https://doi.org/11.0093/intqhc/mzs039

Roeser, K., McGregor, V. E., Stegmaier, S., Mathew, J., Kübler, A., & Meule, A. (2016). The dark triad of personality and unethical behavior at different times of day. *Personality & Individual Differences, 88*, 73–77. https://doi.org/11.0016/j.paid.2015.09.002

Rosenfeld, A., Zuckerman, I., Azaria, A., & Kraus, S. (2012). Combining psychological models with machine learning to better predict people decisions. *Synthese, 189*(1), 81–93. https://doi.org/11.0007/s11229-012-0182-z

Rosenthal, R., Hoffmann, H., Clavien, P. A., Bucher, H. C., & Dell-Kuster, S. (2015). Definition and classification of intraoperative complications (CLASSIC): Delphi study and pilot evaluation. *World Journal of Surgery, 39*(7), 1663–1671. https://doi.org/11.0007/s00268-015-3003-y

Rossi, P. H., Wright, J. D., & Anderson, A. (1983). *Handbook of research.* Academia Press.

Salya, A., & Ravi, M. (2013). Survey on defense against insider misuse attacks in the Cloud. International Journal of Advanced Computing, 5(1). https://dl.acm.org/doi/abs/10.1145/3172869

Sanbonmatsu, D., & Strayer, D. (2013). Who multi-tasks and why? Multi-tasking ability, impulsivity, and sensation seeking. *PLoS ONE, 8*(1), Article e54402. https://doi.org/11.0371/journal.pone.0054402

Sastry, A. (2011). *Honeypots for network security: How to track attackers' activity.* TechTarget. Retrieved February 26, 2021, from https://searchsecurity.techtarget.com/tip/Honeypots-for-network-security-How-to-track-attackers-activity

Schein, E. H. (2017). *The organizational culture and leadership* (5th ed.). Wiley.

Schleifer, T., & Scott, E. (2016, July 25). *What was in the DNC email leak?* CNN. https://www.cnn.com/2016/07/24/politics/dnc-email-leak-wikileaks/index.html

Schubert, P., & Leimstoll, U. (2007). Importance and use of information technology in small and medium-sized companies. *Electronic Markets*, *17*(1), 38–55. https://doi.org/11.0080/10196780601136799

Sedighi, M., Piroozfar, S., & Shojaie, A. (2011). *Proposing a rigorous framework of primary components and evolution of extended enterprise resource planning (ERPII)* [Paper presentation]. The 41st International Conference on Computers & Industrial Engineering, Los Angeles, CA, United States.

Sennewald, C. A., & Baillie, C. (2016). *Effective security management* (6th ed.). Elsevier.

Shaw, E., Ruby, K., & Post, J. (1998). The insider threat to information systems: The psychology of the dangerous insider." *Security Awareness Bulletin,2* (98) 1-10.

Singh, A. S. (2014). Conducting case study research in non-profit organisations. *Qualitative Market Research, 17*(1), 77–84. https://doi.org/11.0108/QMR-04-2013-0024

Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems, 7*(7), Article 19. https://doi.org/11.07705/1jais.00095

Skillings, J. (2020, May 27). *In '95, these people defined tech: Gates, Bezos, Mitnick and more.* CNET. https://www.cnet.com/news/in-95-these-people-defined-tech-gates-gosling-bezos-mitnick-and-more/

Skulmoski, G., Hartman, F., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education, 6,* 1–21. https://doi.org/12.08945/199

Society for Human Resource Management. 2020. https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/new-employee-onboarding-guide.aspx

Software Engineering Institute (SEI). (2013). *Unintentional insider threats: A foundational study* (Report No. CMU/SEI-2013-TN-022). https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf

Sokolowski, J. A., Banks, C. M., & Dover, T. J. (2016). An agent-based approach to modeling insider threat. *Computational & Mathematical Organization Theory, 22*, 273–287. https://doi.org/11.0007/s10588-016-9220-6

Sonnenberg, C. (2020). E-Government and social media: The impact on accessibility. *Journal of Disability Policy Studies, 31*(3), 181–191. https://doi.org/11.0177/1044207320906521

Spain, S. M., Harms, P. D., & LeBreton, J. (2014). The dark side of personality at work. *Journal of Organizational Behavior, 35*(S1), S41–S60. https://doi.org/11.0002/job.1894

Spear, B., Beyer, B. A., Cittadini, L., & Saltonstall, M. (2018). Changing mechanisms of enterprise security (comparing beyond corp with prevalent network security mechanisms). International Journal of Engineering & Technology 7(3.12):81. https://doi.org/11.04419/ijet.v7i3.12.15867

Spector, J. M., Ohrazda, C., Van Schaack, A., & Wiley, D. A. (Eds.) (2005). *Innovations in instructional technology. Essays in honor of M. David Merrill.* Lawrence Erlbaum Associates

Spitzner, L. (2013a). *The top seven human risks - Initial findings.* SANS Institute. https://www.sans.org/security-awareness-training/blog/top-seven-human-risks-initial-findings

Spitzner, L. (2013b). Honeypots: Catching the insider threat. In *ACSAC '03: Proceedings of the 19th annual computer security applications conference* (pp. 170–181). IEEE Press.

Stalla-Bourdillon, S., Phillips, J., & Ryan, M. D. (2014). *Privacy vs. security (Springer briefs in cybersecurity).* Springer.

Stolfo, S. J., Bellovin, S. M., Hershkop, S., Keromytis, A. D., Sinclair, S., & Smith, S. (Eds.). (2013). *Insider attack and cybersecurity: Beyond the hacker.* Columbia University.

Sundararajan, S., Narayanan, H., Pavithran, V., Vorungati, K., & Achuthan, K. (2011). Preventing insider attacks in the Cloud. In A. Abraham, J. Lloret, M. J. Buford, J. Suzuki, & S. Thampi (Eds.), *Advances in computing and communications* (488–500). Springer.

Talanquer, V. (2014). *Strategies for analyzing qualitative data with qualitative analysis software*. Invited Presentation 247th ACS National Meeting Dallas, TX. European Conference on Research in Chemistry Education.

Talke, K., & Snelders, D. (2013). Information in launch messages: Stimulating the adoption of new high-tech consumer products. *Product Innovative Management, 30*(4), 732–749. https://doi.org/11.0111/jpim.12017

Tang, J., Wang, D., Ming, L., & Li, X. (2012). A scalable architecture for classifying network security threats. Science and Technology on Information System Security Laboratory

Taylor, G. A. (2012). Readability of OHS documents - A comparison of surface characteristics of OHS text between some languages. *Safety Science, 50*(7), 1627–1635. https://doi.org/11.0016/j.ssci.2012.01.016

The Site Security Handbook, published as RFC 2196. http://www.ietf.org/rfc/rfc2196.txt

Thoroughgood, C., & Padilla, A. (2013). Destructive leadership and the Penn State scandal: A toxic triangle perspective. *Industrial and Organizational Psychology, 6*(2), 144–149. https://doi.org/11.0111/iops.12025

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review, 4*(3), 356–367. https://doi.org/11.0177/1534484305278283

Tourangeau, R. (2018). Choosing a mode of survey data collection. In D. Vanette & J. Krosnick (Eds.), *The Palgrave handbook of survey research* (43–50). Palgrave Macmillan.

Trochim, W., Urban, J. B., Hargraves, M., Hebbard, C., Buckley, J., Archibald, T., Johnson, M., & Burgermaster, M. (2015). *The guide to the systems evaluation protocol.* Cornell University Cooperative Extension. https://core.human.cornell.edu/documents/SEPGuide2_small.pdf

Tucker, N. (2002, October 17). Spy for Cuba sentenced to 25 years. *The Washington Post.* https://www.washingtonpost.com/archive/local/2002/10/17/spy-for-cuba-sentenced-to-25-years/0ad8e190-e5cb-4198-a9d7-9cf683aa0a70/

U.S. Customs and Border Protection. (n.d.). *What does a background investigation involve?.* Retrieved February 27, 2021, https://www.cbp.gov/faqs/what-does-background-investigation-involve.

U.S. General Services Administration. (n.d.). *FedRAMP*. Retrieved August, 31, 2020, from https://www.gsa.gov/technology

U.S. Office of Personnel Management. (2020). *Data policy & guidance*. https://www.opm.gov/policy-data-oversight/data

Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'theory' back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal, 20*(4), 357–381. https://doi.org/11.0111/j.1365-2575.2007.00292.x

Value Neutrality in Sociological Research. (2021, February 20). Retrieved June 28, 2021, from https://socialsci.libretexts.org/@go/page/7927

Vernon, W. (2009). A Delphi technique: A review. *International Journal of Therapy and Rehabilitation, 16*(2), 69–76. https://doi.org/11.02968/ijtr.2009.16.2.38892

Yang, X., Zeng, L., & Zhang, R. (2012). Cloud Delphi method. *International Journal of Uncertainty, Fuzziness & Knowledge-Based Systems, 20*(1), 77-97. https://www.worldscientific.com/doi/abs/10.1142/S0218488512500055

Wakefield, R., & Watson, T. (2014). A reappraisal of Delphi 2.0 for public relations research. *Public Relations Review, 40*(3), 577–584. https://doi.org/11.0016/j.pubrev.2013.12.004

Walden University. (n.d.). *How do I write a literature review?* Retrieved June 20, 2016, from http://academicanswers.waldenu.edu/faq/72693

Walker, S. J. (2014). Big data: A revolution that will transform how we live, work, and think. *International Journal of Advertising, 33*(1), 181–183. http://dx.doi.org/12.0501/IJA-33-1-181-183

Wallensteen, P. (2018). *Understanding conflict resolution.* SAGE.

Whitworth, B., & Ahnad, A. (2014). *The social design of technical systems: Building technologies for communities.* Interaction Design Foundation.

Willison, R. (2009). *Motivations for employee computer crime: Understanding and addressing workplace disgruntlement through the application of organizational justice* (Working Paper No. 1). Copenhagen Business School. https://research-api.cbs.dk/ws/portalfiles/portal/59197583/WP_2009_001.pdf.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1–20. https://dl.acm.org/doi/12.05300/MISQ/2013/37.1.01

Wise, R. I. (2015). *Managing with measures: How to choose the right performance measures for your organization.*

Yaseen, Q., & Panda, B. (2011). Enhanced insider threat detection model that increases data availability. In R. Natarajan & A. Ojo (Eds.), *Distributed computing and internet technology* (pp. 267–277). Springer.

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report*, *20*(2), 134–150. https://nsuworks.nova.edu/tqr/vol20/iss2/12/.

Yin, R. K. (2010). Analytic generalization. In A. J. Mills, & G. Durepos, & E. Wiebe (Eds.), *Encyclopedia of case study research* (pp. 21–23). SAGE.

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). SAGE.

Yoshimura, S. (2007). Goals and emotional outcomes of revenge activities in interpersonal relationships. *Journal of Social and Personal Relationships, 24*(1), 87–98. https://doi.org/11.0177/0265407507072592

Zhao, H., Zhang, H., & Xu, Y. (2016). Does the dark triad of personality predict corrupt intention? The mediating role of belief in good luck. *Frontiers in Psychology, 7,* Article 608. http://doi.org/10.3389/fpsyg.2016.00608

Ziegeldorf, J. H., Garcia, M. O., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks, 7*(12), 2728–2742. https://doi.org/11.0002/sec.795

Zulkefli, M. Y., & Jemal, A. J. (2014). Analysis of insider attack mitigation strategies. *Procedia Social and Behavioral Sciences, 129,* 581–591. https://doi.org/11.0016/j.sbspro.2014.03.716

Appendix A: Glossary

The following definitions for data threat classification are applicable to this study:

Access Type	Privilege to perform an action on an object to read, write, execute, append, modify, delete, and create in a system (http://opensecuritytraining).
Accountability	The principle that an individual was entrusted to safeguard and control equipment, keying material, and information (http://opensecuritytraining.info/CISSPMain_files/CISSP).
Accreditation	Formal declaration by a Designated Accrediting Authority (DAA) that an information system was approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards (http://opensecuritytraining.info/).
Accredit adequate security	Identifies the information resources Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification of information. This includes assuring that information systems operate effectively

	and provide appropriate confidentiality, integrity, and availability (OMB Circular A-130) http://opensecuritytraining.info/CISSP-Main_files/CISSP).
Access	Opportunity to make use of an information system (http://opensecuritytraining.info/CISSP-Main_files/CISSP0.
Authentication	Protection of data from unauthorized (accidental, or intentional) modification, destruction, or disclosure (http://opensecuritytraining.info/CISSP-
Best Practices	Processes, practices, or systems used by public and private organizations that perform exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas. Successfully identifying and applying best practices can reduce business expenses and improve an organization's efficiency
Clearance	Formal security determination by an authorized adjudicative office that an individual was authorized to access, on a need-to-know basis, to a specific level of collateral classified information (TOP SECRET,

	SECRET, CONFIDENTIAL). (http://opensecuritytraining.info/CISSP-
Community Risk	The probability that a vulnerability will be exploited within an interacting population and adversely impact some members of that population (http://opensecuritytraining.info/CISSP-Main_files/CISSP).
Critical System Events	Interim milestones in the acquisition process that review a system's capability, either operational, technical,or other, that must be questioned before a system's overall suitability can be known and that are of primary importance to the Milestone Decision Authority in reaching a conclusion on allowing the system to advance to the next phase.
Data Integrity	Condition existing when data are unchanged from its source and has not been accidentally, or maliciously modified, altered, or destroyed (http://opensecuritytraining.info/CISSP-Main_files/CISSP).
Data Origin	Corroborating the source of data areas claimed

Encryption	The process of translating a message from the native form of the sender to a standard transmittable form--encoding the message--for security reasons. Also called ciphering.
Decertification	Revocation of the certification of an IS item,or equipment for cause http://opensecuritytraining.info/CISSP-Main_files/CISSP).
Decipher	Convert enciphered text to plain text by means of a cryptographic system (http://opensecuritytraining.info/CISSP-Main_files/CISSP).
Data Transfer Device (DTD)	Intentional release of sensitive data to an unauthorized entity (http://opensecuritytraining.info/CISSP-Main_files/CISSP).
Disruption	Any action,or series of actions that prevent any part of an IS from functioning (http://opensecuritytraining.info/CISSP)
Deliberate Exposure	Incident that allows for unauthorized access to data resulting from hardware, or software failure,

	(http://opensecuritytraining.info/CISSPMain_files/CISSP).
Denial of Service (DoS)	The methodology used to detect imminent hardware, or software failure and provide fail/safe, or fail/soft recovery (http://opensecuritytraining.info/CISSPMain_files/CISSP).
Failure Control	The aggregate of processes and procedures designed to inhibit unauthorized access, contamination, elimination, modification, or destruction of a file, or any of its contents (http://opensecuritytraining.info/CISSPMain_files/CISSP).
File Protection	Means that access to computer files is limited only to authorized users (http://opensecuritytraining.info/CISSP-Main_files/CISSP).
File Security	Hardware and/or software that limits the exposure of a computer, or group of computers to an attack from outside. The most common use of a firewall is on a local area network (LAN) connected to the Internet.

	Without a security system, anyone on the Internet could theoretically jump onto the corporate LAN and pick up any information on, or transfer anything to any of the computers on the LAN. All access should be logged to ensure adequate information for a detailed security audit
Firewall	Process for authorizing access to classified, or sensitive information with specified access requirements, such as Sensitive Compartmented Information (SCI),or Privacy Data a determination of the individual's security eligibility and need-to-know
Hacker	An unauthorized user who attempts to,or gains access to an IS (http://opensecuritytraining.info/CISSP-Main_files/CISSP).
Inadvertent Disclosure	Type of incident involving accidental exposure of information to an individual not authorized access (http://opensecuritytraining.info/CISSPMain_files/CISSP)
Incident	Assessed occurrence, or event having an actual impact
Information Assurance	Measures that protect and defend information and information systems by ensuring their availability,

	integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (http://opensecuritytraining.info/CISSP-Main_files/CISSP).
Insider Threat	An insider threat was a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data and computer systems (http://opensecuritytraining.info/CISSP-Main_files/CISSP)
Internal Threat	Any internal failure of the infrastructure, communications, logistics, IT resources, or planning (http://opensecuritytraining.info/CISSPMain_files/CISSP).
Local area network (LAN)	A short distance data communications network. LANs allow users to be given access to databases and

	programs running on client servers and allow users to work jointly and send messages.
Metropolitan area network	A data network covering an area larger than a LAN, but less than a wide area network (WAN).
Multi-Factor Identification (MFA)	An electronic authentication requiring a user to provide two, or more pieces of evidence (,or factors) to authenticate: knowledge (something only the user knows), possession (something the user has), and inherence (something only the user is). MFA protects a user's data from being accessed by an unfamiliar individual, such as personal ID information, or financial assets.
Network management	A set of procedures and practices to keep a network operating near maximum efficiency. The International Standards Organization defines network management as configuration management, fault management, security management, performance management, and accounting management.
Private network	A network (MAN, WAN, or set of interconnected MANs, WANs, or LANs) used by an organization, or other end-user such as a department, agency, bureau,

	division, etc. A private network might use dedicated circuits and private lines leased from public carriers
Ransomware	bypassing the switches, or they may use microwave technology. Malicious software used by cybercriminals to prevent data owners from accessing their data. The data are withheld until ransom, or payment is received.
Risk Analysis	A technique to identify and assess factors that may jeopardize the success of a project, or achievement of a goal. This technique helps define preventive measures to reduce the probability of these factors from occurring and identify countermeasures to successfully deal constraints when they develop.
Security Management	One of the categories of network management defined by the International Standards Organization. Security management was a set of procedures and practices that may use various tools to restrict access to various resources in the network.
Software	The detailed instructions to operate a computer, or other type of equipment, or hardware. The term was

	created to differentiate instructions (i.e., the program) from the hardware.
Stakeholder	An individual, or group with interest in the success of an organization in delivering intended results and maintaining the viability of the organization's products and services. Stakeholders influence programs, products, and services.
Telecommunications	Telecommunications arere the full range of voice, data and video services and equipment, including the Internet, intranet, and extranet services and equipment as well as wireless services and equipment (e.g., cellular and pager), 800 services and credit card services, excluding radio services and equipment.
Telecommunications architecture	The governing plan showing the capabilities of functional elements of an organization's telecommunications resources and their interaction, including configuration, integration, standardization, life-cycle management, and definition of protocol specifications, among these elements. Equipment includes Routers, switches, Private Branch Exchanges, cell phones, etc., used for various modes of

	transmission, such as digital data, audio signals, image, and video signals.
Virtual Private Network (VPN)	VPNs are a means of augmenting a shared network on a secure basis through encryption or tunneling. Such a shared network could be an Internet Protocol Network,
Zero Trust.	or the Internet, or an Intranet, or frame relay network. A process for granting permissions and access to networks based on the ‘least privileged’ access required to perform the duties of a job.

Appendix B: Round 1 Survey Open-Ended Questions

The overarching research question for this study is: What is the level of consensus among a panel of SMEs regarding the reasons for insider threats in organizations?

Please answer the following questions:

1. What are the motivators for insider threats in organizations?

2. What are the security strategies, and early interventions used in your organization to prevent data breaches and insider threats?

3. What policies and procedures can be developed to manage insider threats' access to systems in organizations?

Appendix C: Round 2 Closed-Ended Questions

SURVEY 2 CLOSED-ENDED QUESTIONS	SURVEY 2 CLOSED-ENDED QUESTIONS	SURVEY 2 CLOSED-ENDED QUESTIONS	SURVEY 2 CLOSED-ENDED QUESTIONS
RQ1. Based on the responses to the first round of interviews questions, the following categories were identified by SMEs about insider threat? Please rate to what extent you Strongly Agree/Strongly Disagree that the following are reasons for insider threats	SQ1-Based on the responses to the first round of interviews questions, the following categories were identified by SMEs about insider threat MOTIVATORS in the workplace. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are motivators for insider threats	SQ2- Based on the responses to the first round of interviews questions, the following categories were identified by SMEs about SECURITY STRATEGIES & EARLY INTERVENTIONS used in organizations to prevent data breaches and insider threats. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are strategies and early interventions for insider threats	SQ3Based on the responses to the first round of interviews questions, the following categories were identified by SMEs as POLICIES AND PROCEDURES to regulate insider threats access. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are best industry policies and procedures to manage insider threats

ANSWERS	ANSWERS	ANSWERS	ANSWERS
Employees with no regard for the organization	Pushing Boundaries	Limited access controls	Download protection policy
Fraudulent activities on the part of the organization	Money, financial gain	Update software regularly (virus protection)	Limit 3rd party usage policy
Little, or no security on the part of the organization	Hackers wanting to sell your information/ ransomware; Political, or religious affiliation	Using antiviruses such as Bitdefender	Pulseway policy
Lack of Training	Greed	Shielding sensitive information from all employees	Controlled access policy
Hiring of chronic rule violators	Power centric	NDAs	Log analysis SOP
Lack of behavioral screening (negative social patterns)	Money	Cybersecurity training	Background screening at hiring policy

SURVEY 2 CLOSED-	SURVEY 2 CLOSED-ENDED QUESTIONS	SURVEY 2 CLOSED-ENDED QUESTIONS	SURVEY 2 CLOSED-ENDED QUESTIONS

ENDED			
QUESTIONS			
RQ1. Based on the responses to the first round of interviews questions, the following categories were identified by SMEs as reasons for insider threats. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are reasons for insider threats	SQ1-Based on the responses to the first round of interviews questions, the following categories were identified by SMEs about insider threat MOTIVATORS in the workplace. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are motivators for insider threats	SQ2- Based on the responses to the first round of interviews questions, the following categories were identified by SMEs about SECURITY STRATEGIES & EARLY INTERVENTIONS used in organizations to prevent data breaches and insider threats. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are strategies and early interventions for insider threats	SQ3Based on the responses to the first round of interviews questions, the following categories were identified by SMEs as POLICIES AND PROCEDURES to regulate insider threats access. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are best industry policies and procedures to manage insider threats
ANSWERS	**ANSWERS**	**ANSWERS**	**ANSWERS**
Personal recognition	Mental Illness	Change Management Policies	Logs and need to know areas policy

Employees sent by competitors	Immaturity	Limiting administrative rights	Risk Management Plans
Insufficient guidelines and security awareness	Disrupting economies of scale	Audits and network scannings	No access to social networks policy
Intentional, or Unintentional access to systems	Personal gain, revenge and/or ideology.	User activity monitoring, separation of duties, and training.	Separation of duties, enforcement of least privileged access, training, oversight policy
Manager's Treatment of employees	Depression	Buddy system	Polygraphs' policy
Discontent with the culture of the organization	Entry level employees want to do social networking at work	Access controls, one Administrator per site	Conflict resolution plan
Political Affiliation	Disregard for authority	Background checks	Training policy
Foreign influences	Financial need	Firewalls	Non-disclosure agreements

SURVEY 2 CLOSED-ENDED QUESTIONS	**SURVEY 2 CLOSED-ENDED QUESTIONS**	**SURVEY 2 CLOSED-ENDED QUESTIONS**	**SURVEY 2 CLOSED-ENDED QUESTIONS**

RQ1. Based on the responses to the first round of interviews questions, the following categories were identified by SMEs as reasons for insider threats Please rate to what extent you Strongly Agree/Strongly Disagree that the following are reasons for insider threats	SQ1-Based on the responses to the first round of interviews questions, the following categories were identified by SMEs about insider threat MOTIVATORS in the workplace. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are motivators for insider threats	SQ2- Based on the responses to the first round of interviews questions, the following categories were identified by SMEs about SECURITY STRATEGIES & EARLY INTERVENTIONS used in organizations to prevent data breaches and insider threats. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are strategies and early interventions for insider threats	SQ3Based on the responses to the first round of interviews questions, the following categories were identified by SMEs as POLICIES AND PROCEDURES to regulate insider threats access. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are best industry policies and procedures to manage insider threats
ANSWERS	**ANSWERS**	**ANSWERS**	**ANSWERS**
Lack of knowledge about insider threat	Retribution	Polygraphs	References checking procedure
Careless	Dislike of Management	Cybersecurity training	Internal Referrals
Recruiting			

Lack of background investigations and reference checking	Money	NDAs	Training procedures
Sense of entitlement	bad intentions, emotional, financial, or politically based motivators drive the intent.	training, implementing multiple factor authentication to reduce data breaches.	Regularly monitoring, implementation of access controls, technology hardening, and regular interval training for all on how to protect data.
Resentment	Money	ID Cards, dual sign on	Risk Management Plan
Social Media	Revenge	effective oversight, coordinated multi-disciplinary coordination, analysis	Audits/compliance
	Religion	Need to know access.	auditing, personnel vetting, and analysis.
	Politics	Training	Reference Checking practice
	Arrogance	Security indoctrination	Hiring the right people for the right jobs
SURVEY 2 CLOSED-ENDED QUESTIONS	**SURVEY 2 CLOSED-ENDED QUESTIONS**	**SURVEY 2 CLOSED-ENDED QUESTIONS**	**SURVEY 2 CLOSED-ENDED QUESTIONS**

RQ1. Based on the responses to the first round of interviews questions, the following categories were identified by SMEs as reasons for insider threats Please rate to what extent you Strongly Agree/Strongly Disagree that the following are reasons for insider threats	SQ1-Based on the responses to the first round of interviews questions, the following categories were identified by SMEs about insider threat MOTIVATORS in the workplace. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are motivators for insider threats	SQ2- Based on the responses to the first round of interviews questions, the following categories were identified by SMEs about SECURITY STRATEGIES & EARLY INTERVENTIONS used in organizations to prevent data breaches and insider threats. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are strategies and early interventions for insider threats	SQ3Based on the responses to the first round of interviews questions, the following categories were identified by SMEs as POLICIES AND PROCEDURES to regulate insider threats access. Please rate to what extent you Strongly Agree/Strongly Disagree that the following are best industry policies and procedures to manage insider threats
	Religious affiliation	Insider threat impact training	Limited Access SOP
	Revenge	Security logs	Different levels of access
	Showing others what one can do; show off	Need to know access.	Rewards and recognition for following rules practice

Appendix D: Survey Round 3 Consensus and Validation Questions

Insider Threats and Data Security Management Strategies Survey Round 3 – Final

A. SMEs REASONS FOR INSIDER THREATS

1. Please rate to what extent you Strongly Agree/Strongly Disagree that EMPLOYEES WITH NO REGARDS FOR THE ORGANIZATION are a Reason for insider threats in organizations

2. Please rate to what extent you Strongly Agree/Strongly Disagree that INSUFFICIENT GUIDELINES AND SECURITY are a Reason for insider threats in organizations

3. Please rate to what extent you Strongly Agree/Strongly Disagree that A LACK OF CYBER SECURITY TRAINING is a Reason for insider threats in organizations

4. Please rate to what extent you Strongly Agree/Strongly Disagree that PERSONAL RECOGNITION is a Reason for insider threats in organizations

5. Please rate to what extent you Strongly Agree/Strongly Disagree that INTENTIONAL OR UNINTENTIONAL ACCESS are a Reason for insider threats in organizations

6. Please rate to what extent you Strongly Agree/Strongly Disagree that DISCONTENT WITH THE CULTURE OF THE ORGANIZATION is a Reason for insider threats in organizations

7. Please rate to what extent you Strongly Agree/Strongly Disagree that IDEOLOGY, FOREIGN INFLUENCE are Reasons for insider threats in organizations

8. Please rate to what extent you Strongly Agree/Strongly Disagree that LACK OF KNOWLEDGE ABOUT INSIDER THREATS is a Reason for insider threats in organizations

9. Please rate to what extent you Strongly Agree/Strongly Disagree that LACK OF BACKGROUND INVESTIGATIONS AND REFERENCE CHECKING are a Reason for insider threats in organizations

10. Please rate to what extent you Strongly Agree/Strongly Disagree that a SENSE OF ENTITLEMENT is a Reason for insider threats in organizations

11. Please rate to what extent you Strongly Agree/Strongly Disagree that RESENTMENT is a Reason for insider threats in organizations

12. Please rate to what extent you StronglyAgree/Strongly Disagree that SOCIAL MEDIA is a Reason for insider threats in organizations

13. Please rate to what extent you Strongly Agree/Strongly Disagree that DISLIKE OF MANAGEMENT, COMPANY CULTURE and COWORKERS are a Reason for insider threats in organizations

B. SMEs MOTIVATORS FOR INSIDER THREATS

14. Please rate to what extent you Strongly Agree/Strongly Disagree that PUSHING BOUNDARIES is a Motivator for insider threats in organizations

15. Please rate to what extent you Strongly Agree/Strongly Disagree that FINANCIAL GAIN/MONEY is a Motivator for insider threats in organizations

16. Please rate to what extent you Strongly Agree/Strongly Disagree that DISREGARD FOR AUTHORITY is a Motivator for insider threats in organizations

17. Please rate to what extent you Strongly Agree/Strongly Disagree that REVENGE/RETRIBUTION is a Motivator for insider threats in organizations

18. Please rate to what extent you Strongly Agree/Strongly Disagree that HACKERS WANTING TO SELL INFORMATION is a Motivator for insider threats in organizations

19. Please rate to what extent you Strongly Agree/Strongly Disagree that BAD INTENTIONS, EMOTIONAL, FINANCIAL OR POLITICAL reasons are Motivators for insider threats in organizations

20. Please rate to what extent you Strongly Agree/Strongly Disagree that ENTRY LEVEL EMPLOYEES WANTING TO ACCESS SOCIAL NETWORKS are Motivators for insider threats in organizations

C. SMEs MAIN SEURITY STRATEGIES AND EARLY INTERVENTIONS TO PREVENT INSIDER THREATS

21. Please rate to what extent you Strongly Agree/Strongly Disagree that LIMITED ACCESS CONTROLS is a main Security Strategy and Early Intervention to prevent insider threats in organizations

22. Please rate to what extent you Strongly Agree/Strongly Disagree that UPDATING SOFTWARE REGULARLY (VIRUS PROTECTION) is a main Security Strategy and Early Intervention to prevent insider threats in organizations

23. Please rate to what extent you Strongly Agree/Strongly Disagree that SHIELDING SENSITIVE INFORMATION FROM ALL EMPLOYEES and SEPARATION OF DUTIES are main Security Strategy and Early Intervention to prevent insider threats in organizations

24. Please rate to what extent you Strongly Agree/Strongly Disagree that CYBER SECURITY TRAINING isa SecurityStrategy and Early Intervention to prevent insider threats in organizations

25. Please rate to what extent you Strongly Agree/Strongly Disagree that a CHANGE MANAGEMENT POLICY is main Security Strategy and Early Intervention to prevent insider threats in organizations

26. Please rate to what extent you Strongly Agree/Strongly Disagree that AUDITS AND NETWORK SCANNING are main Security Strategy and Early Intervention to prevent insider threats in organizations

27. Please rate to what extent you Strongly Agree/Strongly Disagree that a BUDDY SYSTEM is main Security Strategy and Early Intervention to prevent insider threats in organizations

28. Please rate to what extent you Strongly Agree/Strongly Disagree that SECURITY LOGS are main Security Strategies and Early Interventions to prevent insider threats in organizations

D. SMEs MAIN POLICIES AND PROCEDURES TO MANAGE INSIDER THREATS IN ORGANIZATIONS

29. Please rate to what extent you Strongly Agree/Strongly Disagree that DOWNLOAD PROTECTION POLICY is a main Policy and Procedure to manage insider threats access in organizations

30. Please rate to what extent you Strongly Agree/Strongly Disagree that LIMITING THIRD PARTY USAGE/SOCIAL NETWORKS is a main Policy and Procedure to manage insider threats access in organizations

31. Please rate to what extent you Strongly Agree/Strongly Disagree that CONTROLLED ACCESS/PHYSICAL SECURITY is a main Policy and Procedure to manage insider threats access in organizations

32. Please rate to what extent you Strongly Agree/Strongly Disagree that a STANDARD OPERATING PROCEDURE (S0P) is a main Policy and Procedure to manage insider threats access in organizations

33. Please rate to what extent you Strongly Agree/Strongly Disagree that BACKGROUND SCREENING AT HIRING is a main Policy and Procedure to manage insider threats access in organizations

34. Please rate to what extent you Strongly Agree/Strongly Disagree that having a RISK MANAGEMENT PLAN is a main Policy and Procedure to manage insider threats access in organizations

35. Please rate to what extent you Strongly Agree/Strongly Disagree that having a SEPARATION OF DUTIES, ENFORCEMENT OF LEAST PRIVILEGED

ACCESS AND TRAINING OVERSIGHT are a main Policy and Procedure to manage insider threats access in organizations

36. Please rate to what extent you Strongly Agree/Strongly Disagree that having a CONFLICT RESOLUTION PLAN is a main Policy and Procedure to manage insider threats access in organizations

37. Please rate to what extent you StronglyAgree/Strongly Disagree that having a POLYGRAPH POLICY is a main Policy and Procedure to manage insider threats access in organizations

38. Please rate to what extent you Strongly Agree/Strongly Disagree that having a NONDISCLOSURE AGREEMENT is a main Policy and Procedure to manage insider threats access in organizations

39. Please rate to what extent you Strongly Agree/Strongly Disagree that having a CONFLICT RESOLUTION PLAN is a main Policy and Procedure to manage insider threats access in organizations

40. Please rate to what extent you StronglyAgree/Strongly Disagree that having an INTERNAL REFERRAL POLICY is a main Policy and Procedure to manage insider threats access in organizations

41. Please rate to what extent you StronglyAgree/Strongly Disagree that having a PHYSICALSECURITY PLAN, SYSTEM SECURITY PLAN, and a CHANGE CONTROL PLAN is a main Policy and Procedure to manage insider threats access in organizations

42. Please list any additional information you think would enhance the previously stated categories.

Appendix E: Survey Invitation via LinkedIn

Dear Colleague:

My name is Gladys Cooley, and I am a Ph. D candidate at Walden University. As a part of my dissertation requirements, I am conducting a Delphi study on "*Insider Threats' Behaviors and Data Security Management Strategies*." The goal of this Delphi study was to gather subject matter consensus on identifiable insider threat behaviors and best security and control practices to counter insider threats and safeguard data.

Because you are a Certified Member of either, PMI, ISACA, ISO, SANS, GIAC, ISC, or a similar technology/security organization, and a subject matter expert in your field, I am inviting you to participate in this qualitative Delphi research study, consisting of **three rounds of surveys,** administered by me during approximately 3-week periods. If consensus was not achieved, a fourth survey round may be administered.

Each SME will receive an individual survey link using SurveyMonkey®. Answering the survey questions was estimated to take between 15-20 minutes each round. The first SurveyMonkey request, or Survey Round 1, will provide open-ended questions and will serve to generate a baseline to determine how SMEs view insider threat, risks, behaviors, and describe their experiences in securing the data. Survey Round 2 presents closed-ended questions based on your responses to Survey Round 1 questions. Upon classification and analysis of Round 2 responses, Survey Round 3 closed-ended questions will be prepared to validate answers and determine consensus.

Your participation was confidential, that was, no other participant will be aware of your personal identifiable information. You may refuse to continue at any time, or for

any reason. Your participation in these surveys is unpaid and voluntary. The findings will be password protected and saved for five years in accordance with the Walden University guidelines. After such time, it will be destroyed. A consent form will follow to confirm your voluntary/unpaid participation. Please email me to the addresses below if you have any questions.

Sincerely,

Gladys C. Cooley

Emails: Gladys.cooley@waldenu.edu

Walden University IRB Approval No. 12-11-19-0429821

Appendix F: Answers to Open-Ended Survey Round 1

SURVEY 1 OPEN-ENDED QUESTIONS	**SURVEY 1 OPEN-ENDED QUESTIONS**	**SURVEY 1 OPEN-ENDED QUESTIONS**	**SURVEY 1 OPEN-ENDED QUESTIONS**
RQ1. What are the REASONS for insider threats in the organizations?	SQ1. What are the MOTIVATORS for insider threats in the workplace?	SQ2. What are the SECURITY STRATEGIES & EARLY INTERVENTIONS used in your organization to prevent data breaches and insider threats?	SQ3. What POLICIES AND PROCEDURES can be developed to regulate insider threats' access to systems in organizations?
ANSWERS	**ANSWERS**	**ANSWERS**	**ANSWERS**
Employees with no regard for the organization	Pushing Boundaries	Limited access controls	Download protection
Fraudulent activities on the part of the organization	Money, financial gain	Update software regularly (virus protection)	Limit 3rd party usage
Little, or no security on the part of the organization	Hackers wanting to sell your information/ ransomware; Political, or religious affiliation	Using antiviruses such as Bitdefender	Pulseway
Lack of Training	Greed	Shielding sensitive information from all employees	Controlled access
Hiring of chronic rule violators	Power centric	NDAs	Log analysis

Lack of behavioral screening (negative social patterns)	Money	Cybersecurity training	Background screening at hiring
Personal recognition	Mental Illness	Change Management Policies	Logs and need to know areas
Employees sent by competitors	Immaturity	Limiting administrative rights	Risk Management Plans
Insufficient guidelines and security awareness	Disrupting economies of scale	Audits and network scannings	No access to social networks
Intentional, or Unintentional access to systems	Personal gain, revenge and/or ideology.	User activity monitoring, separation of duties, and training.	Separation of duties, enforcement of least privileged access, training, oversight
Manager's Treatment of employees	Depression	Buddy system	Polygraphs

SURVEY 1 OPEN-ENDED QUESTIONS	SURVEY 1 OPEN-ENDED QUESTIONS	SURVEY 1 OPEN-ENDED QUESTIONS	SURVEY 1 OPEN-ENDED QUESTIONS
RQ1. What are the REASONS for insider threats in the organizations?	**SQ1. What are the MOTIVATORS for insider threats in the workplace?**	**SQ2. What are the SECURITY STRATEGIES & EARLY INTERVENTIONS used in your organization to prevent data breaches and insider threats?**	**SQ3. What POLICIES AND PROCEDURES can be developed to regulate insider threats' access to systems in organizations?**
ANSWERS	**ANSWERS**	**ANSWERS**	**ANSWERS**
Discontent with the culture of the organization	Entry level employees want to do social networking at work	Access controls, one Administrator per site	Conflict resolution
Political Affiliation	Disregard for authority	Background checks	Training policy
Foreign influences	Financial need	Firewalls	Non-disclosure agreements
Lack of knowledge about insider threat	Retribution	Polygraphs	References
Careless Recruiting	Dislike of Management	Cybersecurity training	Internal Referrals
Lack of background investigations and reference checking	Money	NDAs	Training.

Sense of entitlement	bad intentions, emotional, financial, or politically based motivators drive the intent.	Our organization ensures that annual training is given to employees. Additionally, they are trying to improve the technological aspects of protecting data by implementing multiple factor authentication to reduce data breaches.	Regularly monitoring, implementation of access controls, technology hardening, and regular interval training for all on how to protect data.
Resentment	Money	ID Cards, dual sign on	Risk Management Plan
Social Media	Revenge	effective oversight, coordinated	Audits, personnel vetting
	Showing others what you can do	multi-disciplinary coordination, analysis	Reference Checking
			Rewards and recognition for following rules
	Religion	Need to know access. Need to know access	Auditing personnel.
	Politics	Training	Reference Checking
	Arrogance	Security indoctrination	Hiring the right people for the right jobs
	Religious affiliation	Insider threat impact training	Limited Access
	Revenge	Security logs	Different levels of access