2019

Managing Security Objectives for Effective Organizational Performance Information Security Management

Ramamohan Gutta
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Ramamohan Rao Gutta

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. David Gould, Committee Chairperson, Management Faculty
Dr. Nikunja Swain, Committee Member, Management Faculty
Dr. Karla Phlypo, University Reviewer, Management Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2019

Abstract

Managing Security Objectives for Effective Organizational Performance Information Security Management

by

Ramamohan Rao Gutta

MBA, Northern Illinois University, 2012

MS, Jawaharlal Nehru Technological University, 1992

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

June 2019

Abstract

Information is a significant asset to organizations, and a data breach from a cyberattack harms reputations and may result in a massive financial loss. Many senior managers lack the competencies to implement an enterprise risk management system and align organizational resources such as people, processes, and technology to prevent cyberattacks on enterprise assets. The purpose of this Delphi study was to explore how the managerial competencies for information security and risk management senior managers help in managing security objectives and practices to mitigate security risks. The National Institute of Standards and Technology framework served as the foundation for this study. The sample was made up of 12 information security practitioners, information security experts, and managers responsible for the enterprise information security management. Participants were from Fortune 500 companies in the United States. Selection was based on their level of experience and knowledge of the topic being studied. Data were collected using a 3 round Delphi study of 12 experts in information security and risk management. Statistical analysis was performed on the collected data during a 3 round Delphi study. The mean, standard deviation, majority agreement, and ranges were used to determine the final concensus for this research study. Findings of this study included the need for managerial support, risk management strategies, and developling the managerial and technical talent to mitigate and respond to cyberattacks. Findings may result in a positive social change by providing information that helps managers to reduce the number of data breaches from cyberattacks, which benefits companies, employees, and customers.

Managing Security Objectives for Effective Organizational Performance Information Security Management

by

Ramamohan Rao Gutta

MBA, Northern Illinois University, 2012

MS, Jawaharlal Nehru Technological University, 1992

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

June 2019

Dedication

This study is dedicated to Mr. Narayana Gutta, my father and Mr. Seshagiri Rao, my high school teacher, who guided and supported me to set my goals and a strong foundation to achieve my personal and academic goals. You told me to never stop and to continue my educational endeavors. You have given me support, love, education, and taught me how to live and help, respect, love those around me. You gave me the inspiration to be the individual and not worry about what everyone else thought.

To my best friend Mr. Venkat Mattela thanks for being a friend with encouragement, support, and unconditional love throughout my educational years. I also dedicate this dissertation to my fabulous wife Sree Gutta, daughter Sreaya Gutta, and son Srikar Gutta, thanks for your unconditional love, support and encouraging words and always believing in me, endured long periods of my absence, and whose love and support were instrumental in my achieving this academic milestone. Thank you.

Acknowledgments

First, I want to acknowledge the guidance, determination, and scholarship of my committee chairperson, Dr. David Gould. Dr. Gould has been accessible, decisive, yet open to new ideas on this journey with me. He has been the catalyst through which completion of this dissertation has been realized. My gratitude to Dr. Gould for being my teacher will remain ever-present in my heart. Thank you.

I would also like to recognize Dr. Steve Jang, my initial dissertation committee member, for his insights and feedback in this challenging process and my current committee member, Dr. Nikunja Swain my gratitude goes also to my URR, Dr. Karla Phlypo. I want to applaud Walden University for giving this opportunity to achieve my important academic goal. I would like to give a special thanks to my 25 reading and literacy experts. Thanks for your patience and taking the time to participate in my Delphi study. I was grateful to have worked with a group of extraordinary people.

I thank my loving and understanding wife Sree, my daughter Sreaya, my son Srikar, for their love and the understanding I could not be at every function or school activities during my dissertation process. I thank my best friend Mr. Venkat Mattela for motivating me to take up this doctoral journey and his unconditional support throughout my doctoral study. I am forever grateful to all those at whatever organization and to everyone else I did not mention but contributed in some fashion to the successful completion of this dissertation. God, I thank you for all your blessings.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Globalization has fueled the growth of the world economy during the last few decades due to advancements in computing, communications, and the Internet (Dhillon, Syed, & Pedron, 2016). The Internet of Things (IoT) is a set of emerging technologies that has improved efficiency in the supply chain for retail industry and safety in high-risk industrial environments (Hosseinian-Far, Ramachandran, & Slack, 2018; Lee & Lee, 2015; Manogaran, Thota, Lopez, & Sundarasekar, 2017). Smartphones and other devices in the IoT are used to connect and share information and to enable transactions such as banking, travel, healthcare, and online commerce. Information technology systems using IoT devices also store and manage sensitive information that, if handled inappropriately, can have devastating consequences for organizations (Ifinedo, 2012; Lebek, Uffen, Neumann, Hohler, & Breitner, 2014; Mbowe, Zlotnikova, Msanjila, & Oreku, 2014). A data breach from a cyberattack harms the reputation of a company and its business operations and could result in a massive financial loss (Edwards, Hofmeyr, & Forrest, 2016). Having a data breach due to cyberattack on company's digital assets makes company senior management look irresponsible in mitigating information security risk (Andreea, 2014; Bauer, & Bernroider, 2017; Dionne, 2013; D'Urso, 2015; Harrison, 2016; Kushwaha, 2016; Marx, 2017; Nicho, 2018). Chapter 1 includes the background of the study, problem and purpose statements, the research questions and hypotheses, conceptual framework, nature of the study, assumptions, limitations, scope and delimitations, definitions, the significance of the study, and its implications for practice, theory and social change.

Background of the Study

The managerial competencies needed for managers who are responsible for managing and mitigating information security risk are the most important success factor in enterprise risk management. There is more collaboration and information exchanged with people and businesses around the world due to advancement in computing and communication technologies (Dhillon et al., 2016). The number of electronic devices connected to the Internet is expected to increase and be in the range of 23 billion by 2020 (Gartner, 2014). However, the increased number of unsecured devices leads to an increased risk of cyberattacks on corporate systems. Home Depot had a major cyberattack that resulted in a data breach that led to 50 million credit card numbers being released. The major credit bureau in the United States also had a cyberattack and lost $145.5 million consumer records contacting sensitive personal information (Moore, 2017). Corporate boards and senior management have recognized the importance of building a core competency in information security and risk management across the organization (Valentine, 2016). The topic of the governance of information technology (IT) and information security is one of the agenda items in corporate board meetings. Information security is an essential part of a company as it ensures information will be safe, which gives confidence to potential investors. Organizations must also comply with government standards to avoid fines and punishment (Lee, Lee, & Kim, 2016).

The managerial competencies developed for information security managers help in implementing an effective enterprise risk management and lead to the security measures being more integrated into the company risk management framework (Barton,

Tejay, Lane, & Terrell, 2016). However, in many organizations, senior management is not practicing the mandated security practices and delegating them to their subordinates (Banks, 2016). The involvement and support of the company board and senior management can help in establishing a strong security framework for information security and improving the quality of security controls across the organization to mitigate risk (Matta, Cavusoglu, & Benbasat, 2016). But security measures tend to be lax in companies where managers are not included in security measures (Soomro, Shah, & Ahmed, 2015). There should be a holistic approach to include business managers in security strategy development and implementation. The most challenging aspect of information security and risk management is addressing the issue at a higher level and aligning resources to take control of data security in the company (Andreea, 2014; Bauer, & Bernroider, 2017; Dionne, 2013; D'Urso, 2015; Harrison, 2016; Kushwaha, 2016; Marx, 2017; Nicho, 2018).

Problem Statement

IoT enables the integration of devices such as smart phones, industrial sensors, and wearables to connect and exchange information (Lee & Lee, 2015; Mukherjee, 2015). Along with new benefits, IoT brings new challenges of security and privacy risks, which may outweigh the benefits regarding exposing sensitive data to unauthorized entities (Weinberg, Milne, Andonova, & Hajjat, 2015). A review of over 100 peer-reviewed articles published within the last 5 years indicated that the risk from data breaches is increasing and the annual cost of data breaches will be over $2.1 trillion

globally by 2019 (Cheng et al., 2017; Cohen, 2017; Gartner, 2014; Juniper, 2017; Meisner, 2018).

The average cost of data breaches from cyberattacks in the United States ranges from $6.53 million to $7.01 million for recovery (Cheng, Liu, & Yao, 2017; Cohen, 2017; Hackett, 2016; Meisner, 2018). The average cost of a data breach in 2020 will exceed $150 million as more Internet infrastructure is connected for business transactions (Juniper, 2017). Every data breach from a cyberattack harms the reputation of the company and its business operations and may result in a massive financial loss (Edwards et al., 2016). A major retailer, Target, had a major cyberattack on November 2013 that resulted in a data breach and over 40 million credit card numbers and 70 million records of personal records were stolen (Cheng et al., 2017; Cohen, 2017; Meisner, 2018). A major health insurer, Anthem, in the United States had a cyberattack on January 2015 and lost 78 million patient records containing sensitive personal and health information (Cheng et al., 2017; Cohen, 2017; Hackett, 2016; Meisner, 2018). The total number of publicized data breaches in the United States as reported in 2015 was 4,571, and the direct and indirect cumulative cost of these data breaches was estimated at $179 billion (Cheng et al., 2017; Cohen, 2017; Edwards et al., 2016).

Senior management should be more proactive in identifying and building competencies for managers who are responsible for integrating and aligning organizational resources such as people, process, and technology to protect critical assets of the organization from cyberattacks. Information security having a major data breach makes company senior management look irresponsible (Aasi, Rusu, & Leidner, 2017;

Andreea, 2014; Bauer, & Bernroider, 2017; Benson, McAlaney, & Frumkin, 2018; Carden, Boyd, & Valenti, 2015; Chaudhry, Chaudhry, & Reese, 2012; Dionne, 2013; D'Urso, 2015; Edwards et al., 2016; Fenz, Heurix, Neubauer, & Pechstein, 2014; Harrison, 2016; Kushwaha, 2016; Marx, 2017; Matta et al., 2016; Nicho, 2018; Pattabiraman, Srinivasan, Swaminathan, & Gupta, 2018). The general problem was that the risk from cyberattacks is increasing even with senior management involvement and increased capital expenditure on information security infrastructure and resources. The specific problem was that many senior managers lack the competencies to align and integrate organizational resources such as people, processes, and technology to prevent cyberattacks on enterprise assets.

Purpose of the Study

The purpose of this qualitative Delphi study was to explore what competencies senior managers need to align and integrate organizational resources for information security and risk management in managing organization security objectives and practices to mitigate information security risks. The findings from this study could help organizations in the development of their information security practices and managerial competencies for aligning and integrating organizational resources. The knowledge may also provide insights that a company can use in developing their budget and organizational strategies (Garg, Curtis, & Halper, 2003).

Research Question

The research question is the main driver of the research approach and methodology in carrying out a research study (Creswell, 2009). This study built

knowledge on several qualitative questions about the current state of managerial competencies and gaps in competencies needed to face the challenges from cyber threats and vulnerabilities. The overall research question was: what competencies should senior managers develop to align and integrate organizational resources such as people, processes, and technology to detect and mitigate the risks of cyberattacks on enterprise critical assets?

Conceptual Framework

After analyzing the significant contributions that the National Institute of Standards and Standards (NIST) framework has made in the field of information security and risk management, I selected the NIST framework as the conceptual framework for my study. The framework core, framework implementation tiers, and framework profiles work together to assess cybersecurity risk. Each component is essential for business operations to continue despite persistent cybersecurity threats.

1. The framework core is made up of five functions: identify, protect, detect, respond, and mitigate. These functions are the cybersecurity activities used to analyze the threat situation and compile potential solutions to reduce damage. The solutions follow the standard practices of the industry such that the framework can exist alongside existing security protocols.
2. The framework implementation tiers are in place for risk assessment. The risks that an organization faces are placed in tiers to denote the level of importance. Organizations use the categorized data to determine the appropriate security plans to accommodate the threat landscape.

3. The framework profile is comprised of the potential solutions that have been determined from the data of various framework categories. The profile includes a comparison of previous security landscapes and new solutions that directly address the needs of the organization.

The NIST framework showcases the ability of an organization to handle the threats from a databreach or cyber threat (Dedeke, 2017; Hiller, & Russell, 2017; NIST, 2018; Pendley, 2018; Stewart, & Jürjens, 2017). Organizations that are at the lowest level of the NIST framework have insufficient security controls and will suffer from cyber threats and attacks. I chose the NIST framework for my research based on the significant contributions that the NIST framework has made in the field of risk management. The NIST framework and managerial competencies were the main components of the conceptual framework. The conceptualizations of data breaches and the effect on business based on managerial competencies are discussed further in Chapter 2.

Nature of the Study

This research involved a qualitative Delphi design to gain consensus on the competencies senior managers need to align and integrate organizational resources for mitigating information security risk from cyber attacks. I chose to use a qualitative method of research because it is a method for seeking a better understanding of the problem under study (Cooper & Schindler, 2011; Matta et al., 2016). The Delphi research methodology was developed by the RAND company after the World War II to determine the influence that technology may have on future wars (Borden, Shaw, & Coles, 2017; Ohtera, Kanazawa, Ozasa, Ueshima, & Nakayama, 2017; Strang & Strang, 2017). This

approach involves a qualitative method with participants who are required to have a certain level of expertise in the topic to provide input and come to a consensus (Linstone & Turoff, 2011; von der Gracht, 2012). The experts are divided up while responding to questions such that their responses would not be influenced by the responses of their peers (Nowack, Endrikat, & Guenther, 2011). The questions are asked by a facilitator and each question builds on the previous answers collected (Linstone & Turoff, 2011). The Delphi technique has been used in many different industries such as politics, psychology, and business where experts in their respective fields have been used to analyze a topic. The Delphi technique has evolved to include different types of research studies as well as improve its structure of data analysis.

Research topics that do not have a robust set of existing data benefit from the Delphi technique, as all data gathered comes from informed experts (Skulmoski, Hartman, & Krahn, 2007). The Delphi technique is popular with security software research because the field is growing and changing with information that the public might not understand. The sample of my study was made up of information security senior managers who were responsible for the enterprise information security management for reducing risk from cyberattacks. The participants were 12 United States residents who work for Fortune 500 companies in the United States and are senior managers with of certified information systems security professional credentials. They were anonymous in the study as well as to each other. Participants were asked a set of questions regarding what managerial competencies are needed for managers who are responsible for the organizations information security and risk management.

The Delphi consensus illustrates the various points of view of the participants and connects them to the experience that is being researched (Creswell, 2009). The data were collected using a 3-round Delphi study, which was important in gaining a holistic understanding of the information collected as well as the topic that is researched (Cooper & Schindler, 2011). The analysis of data collected from these three rounds was important in finding common themes and patterns (Skulmoski et al., 2007). The main purpose of the technique was to reach consensus among a panel of experts, which makes the conclusion of the research more grounded as well as more helpful for future research. The study participants were selected through LinkedIn, a social media site that displays employment and education details. Participants' personal identification information was not collected or used during the process of the data collection or in any part of the study. This approach reduced the chance of violating participant's privacy rights and confidentiality. Direct involvement was also limited as the selection criteria emphasized anonymous contributions (American Psychological Association, 2010; Bernard & Bernard, 2013; Sieber, 2011). Further, participants were free to leave the study if they felt discomfort or pressure.

If consensus was not reached with 12 participants, I planned to interview more participants to reach consensus on managerial competencies required for aligning organizational resources to mitigate risks from cyberattack. The consensus may not occur in every study as participants may continue to have diverging opinions and it may be difficult to achieve. The findings from a study lacking consensus can also contribute to valid conclusions (Gupta & Clarke, 1996; Hsu & Sandford, 2007; James & Warren-

Forward, 2015). The interquartile range is commonly used by researchers to declare a consensus (Haynes & Shelton, 2017; Skinner, Nelson, Chin, & Land, 2015; Strasser, 2017). Statistical measures such as central tendency and distribution were be used to determine the level of consensus between the participants (Cleary, Horsfall, & Hayter, 2014; Lee-Jen Wu, Hui-Man, & Hao-Hsien, 2014; Morgan, 2008).

Definitions

Cyberattack: Attack, via Internet or computer connectivity, that targets an organization's use of cyberspace for disrupting, destroying, or maliciously controlling a computer and communications infrastructure; destroying the integrity of the digital assets; or stealing organization's information (NIST, 2013).

Data breach. A data breach or a security breach is theft of sensitive information such as social security number, credit card number, name, date of birth, and personal health records. Breach usually results in unauthorized access to critical data and IT infrastructure (Romanosky, Telang, & Acquisti, 2011).

Governance: Governance is using regulations, internal policies, and procedures (Govindji, Peko, & Sundaram, 2017).

Internet of Things (IoT): IoT is the collection of resource constrained tiny intelligent devices interconnected via the Internet (Piggin, 2016).

Assumptions and Limitations

The study limitations were due to the defined criteria of the research participants being from a specific field for a narrow topic (Nowack et al., 2011). Industry experts in different parts of the United States may have come to a different consensus on the topic.

Another limitation could have been participants feeling pressured in their responses; however, the experts were divided up while responding to questions so their responses would not be influenced (Nowack et al., 2011).

One of the assumptions of this study was that the participants should have a greater understanding of the topic than members of the general population. Another assumption was that the data would be more useful, as it would be backed by research and understanding rather than broad opinions of random participants. This approach was a good choice for a research study as it provided a more concise and educated conclusions compared to other types of studies (Linstone & Turoff, 2011).

Scope and Delimitations

One of the delimitations of this study was its focus on Fortune 500 companies that are based in the United States. This is because the United States has more mature security practices due to the stringent federal regulatory compliance requirements. The companies that were included in the study came from a variety of different private sector industries such as financial, healthcare, insurance, and technology. The participants for this study were selected from a population of senior managers with certified information systems security professional credentials and are responsible for implementing senior management mandates and managing organizational risks in the Fortune 500.

Significance of the Study

The research findings may contribute to the understanding of how information security can be pursued and how senior management may improve organizing organizational resources to mitigate information security risk and its effect on

organizational financial performance. The applicability of traditional enterprise information security controls are not sufficient, and neither are management practices sufficient to provide the required security controls for Internet infrastructure supporting systems and business applications. This study may be used as a basis for additional research to identify new threats and countermeasures. Management can use the findings from this research study to enhance business practices that address information security risks. Organizational management can also use the findings to create new strategies to balance the business and security aspects of a new system. The more data that are cultivated means that leaders will have a better understanding on the most effective security system. This study can also help in preventing data breaches. The information can help in improving information security and lowering the costs involved in responding to threats. The employees that work with IT could use this information to better understand the variances that come with security threats.

Significance to Practice

This study may reduce the gap in existing literature on enterprise risk due to rapid globalization, technology advancements, and dynamically changing regulatory environments. Today's organizations are spanned across countries and are exposed to greater threats from cyberattacks. The collaboration between federal regulators, business leaders, standards organizations, and academic institutions is one of the key success factors in enhancing existing or developing new frameworks, standards, and policies for an effective information security risk management based on integrated system theory's system policy theory, risk management theory, and management system theory. The

system is developed based on individual business needs to minimize organizational risk and improving financial performance. This study may help the organization leadership in aligning, people, process, and technology for achieving information security goals of the organization.

Significance to Theory

This study may be used for further research to identify new threats and countermeasures. The following may be the significant contributions:

1. The gaps identified in management practices that are adopted in organizations using IoT infrastructure to support business applications may help in enhancing the overall information security framework in traditional enterprise security management and security controls implementation.
2. The enterprise security and risk management can reuse the processes, technology, and applications developed for an IoT platform to mitigate risk.
3. The findings may help senior management to oversee systems that protect data (Knapp & Ferrante, 2012). This study may also aid in identifying and exposing potential risks that can result in data breaches. Fewer breaches will lead to a smaller financial burden on companies that otherwise may have had to spend millions of dollars to correct the problem. The appropriate funding can be put aside for the implementation and integration of the new information system.

Significance to Social Change

Investors are looking at breach notifications on various companies while making investment decisions. Information security breaches influence company's financial

performance and overall risk. A data breach that results in the leak of confidential data has a greater negative effect than any other type of breach (Das, Mukhopadhyay, & Anand, 2012). Employee awareness of security threats help improve the overall understanding of security threats and the best practices to use to protect the data. Some of the most malicious breaches occur through simple mistakes of employees. These can be avoided with a better sense of understanding. Employee training can be a valuable investment in protecting the assets of the company. Findings may result in a positive social change by reducing the number of data breaches from cyberattacks in the business world thus protecting organizations, employees, and the public from financial loss.

Summary and Transition

Every data breach from a cyberattack harms the reputation of the company and its business operations and result in financial loss (Edwards et al., 2016). Having a large data leak makes company senior management look unprepared when it comes to protecting themselves (Andreea, 2014; Bauer, & Bernroider, 2017; Dionne, 2013; D'Urso, 2015; Harrison, 2016; Kushwaha, 2016; Marx, 2017; Nicho, 2018). Risk management is the responsibility of senior management in making strategic decisions related to organization's information security controls and risk. Measuring the overall effectiveness of organization's information security management controls is done using return on investment with metrics such as finance, governance, information security incidents, and technology. Top management can effectively integrate the entire organization, people, process, and technology for an information security management to minimize financial loss from cyberattacks and increase organization value to all stakeholders.

This study addressed strategies that managers use to mitigate data risks. The NIST framework served to inform the study, and I used a qualitative Delphi approach. Findings of this study may result in a positive social change by reducing the number of data breaches from cyberattacks in the business world thus protecting organizations, employees, and the public from financial loss.

Chapter 2, the literature review, contains the result from the review and research of published literature which underpinned this study. The associated literature search was based on the research problem involving data breaches and the lack of sufficient leadership and managerial competencies to minimize the risk of data braches resulted from cyber attacks on organizational digital assets.

Chapter 2: Literature Review

The purpose of this qualitative Delphi study was to explore how the managerial competencies for information security and risk management senior managers can help in managing security objectives and practices to mitigate information security risks. Previous research has indicated how managerial competencies impact organizations' information security and risk management. The average cost of data breaches from cyber attacks in the United States ranges from $6.53 million to $7.01 million for recovery (Cheng et al., 2017; Cohen, 2017; Hackett, 2016; Meisner, 2018). The direct and indirect cumulative cost of these data breaches in 2015 was estimated at $179 billion (Edwards et al., 2016; Kushwaha, 2016). The average cost of a data breach in 2020 will exceed $150 million as more Internet infrastructure gets connected for business transactions (Juniper, 2017).

The purpose of this chapter, the literature review, was to analyze, interpret, and synthesize the literature on the phenomenon of managerial competencies and to discuss a conceptual framework for my research. The identification of the gap in literature helped focus this study and justify the selection of research questions. The qualitative research on managerial competencies with data breaches lacked depth and breadth. This chapter starts with the conceptual framework, on which this research project was organized and through which the problem was described. The literature review follows and covers the following topics: The data breaches and impact, managerial competencies, information security and risk management, governance, and alignment of organizational resources.

Literature Search Strategy

The literature researched and reviewed for this dissertation spanned from 1960 to 2018. Sources included text books, peer-reviewed journal articles, publically available government agency standards, and regulatory compliance documents. Additionally, electronic based media sources were researched such as online publications, databases, and websites for government, nongovernmental organizations, and corporations. The following databases were used to identify peer-reviewed articles: EBSCO host, ERIC, ProQuest, ProQuest dissertation, ScienceDirect, Google Scholar, Business Source Complete/Premier, ABI/Inform Complete, and Emerald Management Journals.

By searching these databases using selective keyword search strategy, I determined that I had found all the relevant articles and research question, I could review before the searches became redundant. The following keywords were used for identifying peer reviewed articles and text books: *Assurance, assessing the effectiveness of information security controls "AND" cyber attacks, assessing the impact of management support and involvement in organization risk management, business continuity, change management critical success factors, disaster recovery, data security, effective information security controls development, and implementation, financial performance impacts of security breaches and data theft, information security, information security management, information security standards, information security strategy and alignment, information security governance, information security awareness, internal and external threats, incident management, impact of information security on firm performance, management support, management involvement in risk management, risk*

management strategies, regulatory compliance, risk assessment, security breaches, security controls, security policies and procedures, stake holders, security breaches, and *information theft.* Narrowing the results to the last 5 years yielded 120 relevant articles.

Conceptual Framework

Threats to data security expose existing vulnerabilities of an organization's infrastructure. New developments in communication such as online communication increase the amount of information that is transported via unsafe channels. Information on financial issues, health records, and security protocols can be breached by threats. The financial influence from these threats can be dangerous for and can make recovery very difficult. The reputation of an organization is also placed at risk when there is the appearance of insufficient security protection.

The Cybersecurity Enhancement Act of 2014 was introduced to address the risks of cyber threats. This act enhanced the reach of the NIST, which makes identifying and mitigating threats against frameworks easier. The NIST framework is comprised of the framework core, the implementation tiers, and the framework profiles. The framework core is used to analyze the activity that occurs across an organization. The implementation tiers allocate data for the use of building individual profiles to fit into the organizational framework. The framework profiles help the system divide activity to the areas of the framework that require the most help. These factors work together in the NIST framework to create an effective system that will uphold the requirements of cyber security protection (see Figure 1). I chose the NIST framework for this study because it addresses security risks.

Figure 1. NIST framework core structure. (Source: https://nvlpubs.nist.gov)

Framework Core

The framework core functions of identify, protect, detect, respond, and recover work to access cybersecurity risks. The various functions are broken down into categories to determine the needs of the organizational programming. The subcategories are an additional subdivision below categories that help narrow down the specific technical and managerial resources that are needed to combat threats. The purpose of the identify function is to obtain an understanding of the organization's ability to detect threats and protect against their negative effects. The protection aspect involves introducing new security protocols that will handle the needs of the organization. The detection element requires the security protocols to find threats and adapt the system to protect against similar attacks. The purpose of the response function is to develop security systems that will carry out solutions that fight against threats. The system must also be able to recover lost information and capabilities that were affected by cyber security breaches.

Framework Implementation Tiers

The framework implementation tiers are used to divide the risks of an organization by their urgency and potential effect. Each tier builds on the rigor of the previous tier. The highest tier level will include the most serious risks with the potential of the most damage. Most resources and managerial attention will be allotted to higher level risks. Organizations that include framework implementation tiers in their cost-benefit analysis will be able to assess the situation and understand how to address security concerns.

Tier 1: Partial risk. Tier 1 includes risk management process and integrated risk management program. The risk management process includes gathering data and developing ideas on security protocols that can address the issues being faced by the organization. Responses to current cyber security risks are also addressed. The integrated risk management program may have a lack of understanding of the overall risks being faced by the organization, which means that there will need to be extensive research to develop appropriate programs.

Tier 2: Risk informed. Tier 2 involves known risks and the strategies that can be used to mitigate potential effects. The risk management process at Tier 2 includes established security protocols designed to address current risks facing the organization. The protocols may only be limited to certain sections and not widespread through each division. Priority of risks will depend on current and former risks that have impacted the security landscape. Secure data may not have established secure channels to transfer information between employees.

Tier 3: Repeatable. The risk management process of Tier 3 has extensive security protocols that are implemented throughout the organization. The protocols are adapted to fit the changing security needs faced by the system. The integrated risk management program involves company-wide security practices to combat cyber security risks. These practices are studied to illustrate effectiveness in protecting data while fending off future issues. The employees of the organization have a rigorous understanding of security protocols and supervisors ensure the protocols are being followed. Senior level management also make data security a priority and ensure the appropriate number of financial and managerial resources are devoted to upkeep the organizational information security risk management system.

Tier 4: Adaptive. The risk management process of Tier 4 involves the organization evolving its security practices based on acquired knowledge of the risk landscape. Technology and threats are always changing, such that organizations need to stay on trend to protect the long-term security of the organization. Organizations that are unable to evolve with the times become obsolete.

The integrated risk management program of Tier 4 involves the highest level of security integration into the overall business structure. The people, processes, and procedures of the organization are aligned with the organizational structure to ensure that the capabilities of the organization are appropriately protected. The employees have a full understanding of the link between success and data security and conduct their behavior accordingly. Senior management champion new security ventures to protect sensitive

data and communication. The security budget reflected the importance of rigorous data security protocols.

Framework Profile

The framework profile is the alignment of organizational regulations, risk assessment, and resources for mitigating cybersecurity risk. There may be more than one profile needed to analyze the security landscape of the organization depending on size and scope. The profiles address the current state and the target state of the security elements in the organization. The current framework profile addresses the current state of security while the target framework profile represents the potential outcomes of new security implementations. Effective communication between individuals in the organizations as well as between multiple organizations need to be analyzed to test for secure channels and risk. Vulnerabilities are found through analysis of current and target profiles. Future security plans need to address these vulnerabilities while keeping the strengths intact. The number of resources and employees needed to fight back against risk are also calculated by the numbers of the framework profiles.

The NIST framework can be used by any type of organization. Variances in magnitude of risk, size, and resources make little difference in the effectiveness of the framework. The universal nature of the NIST framework is due to its practical approach and solutions. Despite its practical usage, the framework will not manage cybersecurity risks of different origins the same way. There are differences in each system depending on how the infrastructure is set up in a framework. The ultimate purpose is to reduce and mitigate risks in the system. The employees who oversee the framework need to be

experienced in threats and how to work with the system to handle solutions. NIST is constantly evolving based on new information obtained by threats and gets more intuitive after every incident. The framework follows a set of guidelines to address the security needs of an organization. The guidelines cover the cybersecurity landscape of the organization, specific vulnerable areas, potential improvement areas, progress in handling threats, and communication between employees about maintaining a safe system.

Coordination of Framework Implementation

Figure 2 includes a common flow of information and decisions at the following levels within an organization. Framework implementation occurs between the executive level, business level, and the implementation level. The executive level involves the overview of operational goals, current resources, and risk management. The business level involves the alignment between operational goals and business goals in the creation of the framework profile. The operations level completes the framework profile and then share the data with the business level. The business level uses the data acquired by the profile to conduce a risk assessment, which is communicated to the executive level to create a plan to address the risks in their overview report. The NIST framework works alongside existing security controls without replacing existing infrastructure. The framework core, framework implementation tiers, and framework profiles work together to assess cybersecurity risk.

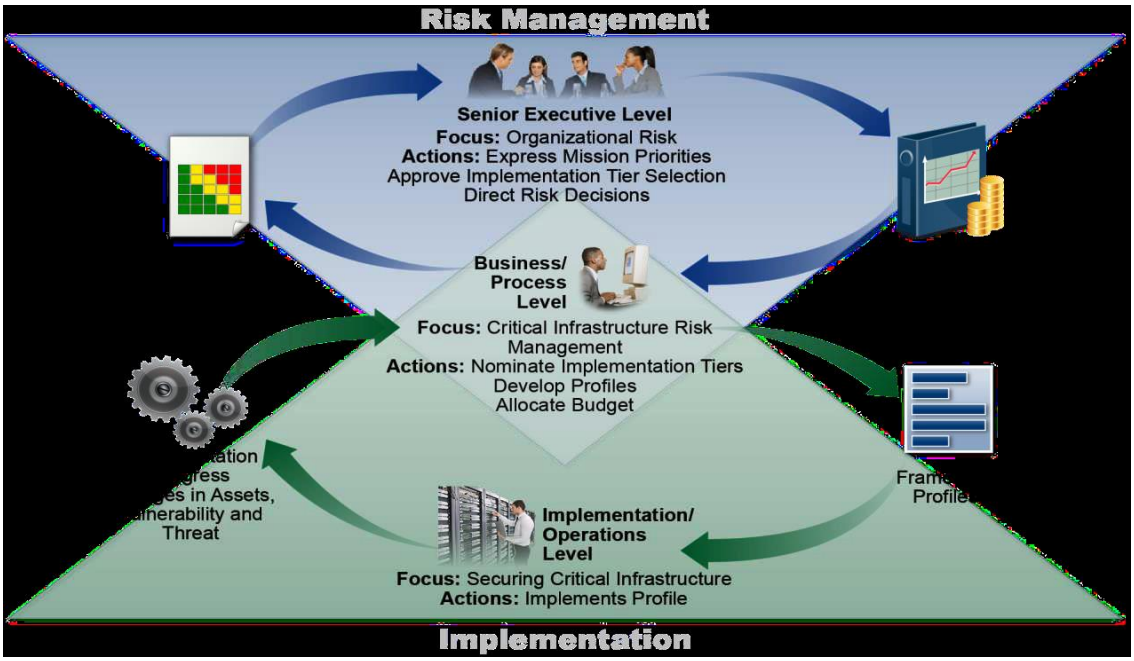

Figure 2. NIST framework implementation for risk management. (Source: https://nvlpubs.nist.gov)

NIST Framework Cybersecurity Practices

Proper cybersecurity practices are essential to the growth of an organization. Organizations that are not able to adequate protect their data will be given a poor reputation and little to no chance for improvement. There are seven steps that are involved in the implementation of new cybersecurity practices. The first step is to determine the operational objectives and priorities of the organization. The second step is aligning resources with the goals of the organization. The third step is to create a current profile that describes the existing security landscape, categories, and subcategories of the organization. The fourth step is to conduct a risk assessment to understand the current threats being faced by the company as well the effectiveness of current security protocols. The fifth step is to create a target profile that predicts the outcome of potential security

protocols. The sixth step is to determine vulnerabilities and gaps in the system. The seventh step is to create a plan that addresses the risks facing the organization while utilizing the set resources available in the organization.

Information Security Risk Management

Even a small vulnerability can lead to a large breach and financial loss. Breaches are most often caused by internal and external vulnerabilities in an organization (Fenz et al., 2014). People, process, and technology are integrated elements in any organization and should be aligned to achieve information security goals. If proper security controls are not put into place to protect the data, data breaches rise exponentially (Soomro et al., 2015). Security risk analysis is the area of enterprise risk management that determines the level of risk and the method in handling the risk. As security become a part of a company's focus, so does the role of senior management (Feng, Wang, & Li, 2014).

Risk management is a program that incorporates multiple systems to deal with the information security risks that affect operations (Safa et al., 2015). The process includes creating a framework to recognize risky activities, analyzing the risk, creating a solution to combat the risk, and to keep up with dealing with risk over an extended period. The system also includes features that address risk to the organization (Bodin, Gordon, & Loeb, 2008).

Information Security Controls

In a business context, control can help in maintaining behaviors that can assist in improving the performance of a company (Cram, Brohman, Chan, & Gallupe, 2016). It is a challenge for management to implement a change and controls in any organization

(Jensen, 2017). Management must exercise control over people, process, and technology through a risk awareness program to positively affect the company. There are several drivers such as internal and external threats, business and regulatory requirements that are necessary to analyze to create a proper control system for an effective information management system (McFadzean, Ezingeard, & Birchall, 2011). McFadzean et al. stated that senior management at board level and their support for organizational level information security initiatives will help to bring security awareness across the company with a minimal resistance from employees for a change to adopt new processes and procedures to implement new security controls. The information security controls suggested by NIST (2013) are included in Table 1.

Table 1

Information Security Controls Family

Sr.No	Security control family ID	Security control family name
1	AC	Access control
2	MP	Media protection
3	AT	Awareness and training
4	PE	Physical and environmental protection
5	AU	Audit and accountability
6	PL	Planning
7	CA	Security assessment and authorization
8	PS	Personal security
9	CM	Configuration management
10	RA	Risk assessment
11	CP	Contingency planning
12	SA	System and services acquisition
13	IA	Identification and authentication
14	SC	System and communications protection
15	IR	Incident response
16	SI	System and information integrity
17	MA	Maintenance
18	PM	Program management

Note. Source: NIST SP 800-53r4, Joint Task Force Transformation Initiative (NIST, 2013).

Literature Review

The alignment of people, process, and technology at every level of the organization towards risk management helps in reducing internal and external threats from cyberattacks (Chen, Ramamurthy, & Wen, 2015; Kohnke, Shoemaker, & Sigler, 2017). Organizations that integrate and align people, process, and technology into the overall business process lower the costs of data breaches (McFadzean et al., 2011; Pooley, 2017; Scarfò, 2018). Companies that have an alignment gap between organizational resources are found to have an increased amount of security risks. This literature review includes the effect of managerial capabilities for creating organizational readiness for handling information security risks. The leadership competencies of a manager play a large part in how the organization prevents and responds to threats. Certain managerial competencies are essential for information security managers for aligning organizational resources to prevent data breaches from internal external threats.

The literature research and review was organized into data breaches and impact, competency domains such as information security risk management, leadership and managerial competencies, communication competencies, project management competencies, on the organizational performance. The leadership and managerial competency attributes are identified from literature review and classified in to the following three categories: people, process, and technology as shown in Table 2. People management competency includes all internal and external stake holders, goal setting, performance management, performance metrics, training, conflict resolution, delegation, rewards and recognition. Process domain includes communication at all levels of the

organization, organizational strategy and organizational alignment, regulatory compliance and governance, finance and budgeting, Industry networking, vendor and supplier management, ethics and social responsibility, quality management, and change management. Technology competency includes IT and systems, communications and networking infrastructure, information security, risk management, and industry specific domain competencies.

Table 2

Competencies for Aligning Organizational Resources

Sr.No	People Skills And Competency Attributes
1	People and stake holder management
2	Goal setting and monitoring
3	Performance measurement and corrective actions for improvement
4	Rewards, recognition and corrective actions
5	Education training and Training and awareness programs
6	Conflict resolution
7	Ethics and compliance
8	Social responsibilities
9	Ownership and responsibilities
10	Understanding organizational goals and vision
11	Developing strategic skills
12	Mentoring and building teams
Sr.No	Organizational Process Skills And Competency Attributes
1	Communication at all levels of the organization
2	Organizational strategy development
3	Governance and regulatory compliance requirements
4	Finance and budget development
5	Industry peer networking to new and emerging process improvements, lesons learned at other
6	Vendor management
7	Project management
8	Quality management
9	Customer support
10	Resource planning and optimization
11	Organizational risk management and regulatory compliance applicable to the organization
12	Organizational vision and strategy development and implementation to achive operational strategic goals
Sr.No	Technology Skills And Competency Attributes
1	Information technology and systems used by the organization to achieve organizational goals
2	Organizational business applications
3	Communication and computing technology
4	Information Security tools and technology
5	New and emerging technologies such as internet of things (IoT), artificial intelligence, big data, and cloud technologies
6	Industry specific domain
7	Technology alignment with organizational
8	Industry specific regulations and their impact on the organization

Note. The competencies are compiled from literature review

Data Breaches and Their Effects

This section includes a review of the different data breach literature with focus on the financial effects of data breach incidents. The review of data breach incidents and their effect on financial performance of the organizations, review of the entire organization including organizational performance, alignment, capabilities, culture, and strategies. The review of the senior management's role in aligning the entire organization, people, process, and technology to manage the risk effect from cyber attacks and data breaches to an acceptable level. The review of information security risk management, governance, framework, regulatory compliance, financial impact, security investments, the stock market price and market value implications due to a data breach. A summary of the overall data breach effect on organization financial performance and the cost of a data breach incident and critical success factors.

Data breaches are some of the most intense security threats that a company faces. Breaches are concerned with exposed data to forces outside the company. As data are the most important asset of a company, a leak can create severe damage to the finances and reputation of a company (Cheng et al., 2017). Data breaches are becoming more common as more data is being placed online. The breaches are constantly evolving so it can be difficult for security programs to find and destroy threats. There is significant research being done about threats but there is no best method of protection (Cavusoglu, Cavusoglu, Son, & Benbasat, 2015).

Scholars have recently begun to investigate multiple aspects of data breaches that are determined by the source of the data breach and the industry it affects (Das et al.,

2012). Data breaches can occur due to the loss of physical objects, loss of documents or devices with sensitive data can lead to massive data breaches. About half of the companies that had a data breach incidents between 2006 to 2008, resulted from a lost portable device (Grahn, Westerlund, & Pulkkis, 2017; Schafer, 2016).

A data breach that results in the leak of confidential data has a greater negative effect than any other type of breach (Das et al., 2012). Research conducted from 2003 to 2012 has found that information security breaches have a considerable effect on the financial performance of a company (Ayyagari, 2012). The economic cost of publicly announced information security breaches has some financial repercussion and the repercussions can come in the form of stock drops or loss of cash flow (Campbell, Gordon, Loeb, & Zhou, 2003). The data reviewed from 1997 to 2003 showed that the characteristics and intensity of the security breach have an impact on stock market response to the breach (Andoh-Baidoo & Osei-Bryson, 2007). Research on the market price effect from data security breaches was also conducted from 2000 to 2010 (Morse, Raval, & Wingender, 2011). The results of the study proved that a data breach could hurt stock market performance. This negative effect can last for a long time after the initial breach (Morse et al., 2011).

Ultimately, denying a data breach has occurred has a greater negative effect on the stock market than addressing the issue properly (Veltsos, 2012). The effects of security breaches on the market value of companies were researched between 1996 and 2001 (Cavusoglu et al., 2015). Cavusolu analyzed the company within 2 days after a data breach was reported. The results were that companies lost an average of 2.1% of their

market value, which is an average loss of $1.65 billion dollars per incident (Cavusoglu et al., 2015). The factors that were tested were company size, type, type of breach, and time. While the breached company was negatively affected, security developers had a positive market value in response to a breach. Security developers had a 1.36% gain in market value which led to a gain in $1.06 billion dollars in the span of 2 days (Cavusoglu et al., 2015). The conclusion of this study was that investors largely penalize poor security practices, which lead a negative market value of a company. The size of the firm seemed to have no significant effect on the market response to a breach.

Healthcare organizations also have large risks associated with data breaches. Hospitals and medical insurance companies handle patient health records containing personal health and personal information while providing care and processing payments (Holtfreter, & Harrington, 2015; Houser, 2015; Kierkegaard, 2012). The Health Insurance Portability and Accountability Act were put into place in 2013 to ensure privacy, provide protection against fraud, and to continue coverage for health plans (Holtfreter & Harrington, 2015; Houser, 2015). The Health Information Technology for Economic and Clinical Health Act was enacted in 2009 for the purpose of covering security mandates in the wake of a healthcare information breach (Caldwell, 2012; Kierkegaard, 2012).The notification allows individuals to seek out measures to protect against further attacks and to attempt to maintain privacy (Bisogni, 2016; Schuessler, Nagy, Fulk, & Dearing, 2017). Some states have less restrictive laws on this matter than others, which brings in the need for a federal law (Caldwell, 2012; Romanosky et al., 2011). The benefits of notification laws include companies having an incentive to

improve their data security, individuals are better able to protect themselves against identity theft, and priority is placed on the privacy rights of a person whose personal data has been breached (Bisogni, 2016; Schuessler et al., 2017).

Federal Notification Laws: The Data Security and Breach Notification Act was enacted in 2011, which stated that when a breach occurs, all affected individuals would have to be notified (Caldwell, 2012). A federal law that affects healthcare information is the Health Information Technology for Economic and Clinical Health Act which requires the Department of Health and Human Services as well as the Federal Trade Commission to address breach issues that apply to the Health Insurance Portability and Accountability Act (Kierkegaard, 2012). The federal laws have led to better protection against data breaches due to the potential financial and reputation damage (Kierkegaard, 2012). Most research done on data breach effects have focused on the stock market price or the market value days after the breach announcement. The studies that have researched the effects of data breaches have varied in the years they cover.

In a research study done by Garg et al. (2003), only 22 breaches were reported during the period before the mid 90's. Loss of data from the retail industry alarms many people as it can lead to credit card information being leaked. The retailer then had to face numerous lawsuits from angry customers, regulatory oversight audits and fines (Archer, 2012; Ayyagari, 2012; Cheng et al., 2017). The incident at the Michael stores and TJX Corporation is another example as the company reported what is now the largest case of credit card fraud. Data breaches have a large effect on retail companies as the trust that the public had with the company is greatly affected.

Information Security Risk Management

Even a small vulnerability can lead to a large breach and large financial loss. Breaches are most often caused by internal and external vulnerabilities in the organization (Fenz et al., 2014). The pillars of modern organization such as people, process, and technology are tightly integrated elements in any organization and should be aligned to achieve information security goals. If proper security controls are not put into place to protect the data, data breaches rise exponentially (Soomro et al., 2015). Security risk analysis is the area of enterprise risk management that determines the level of risk and the method in handling the risk and as security becomes a large part of a company's focus, the role of senior management changes (Feng et al., 2014).

Risk management is a program that incorporates multiple systems to manage information security risks that affect operations (Safa et al., 2015). The process includes creating a framework to recognize risky activities, analyzing the risk, creating a solution to combat the risk, and to keep up with dealing with risk over an extended period of time. The system also must include features that address risk to the organization (Bodin et al., 2008).

Information Security Policies

Security policy includes a set of standards that incorporate all the aspects that the security service works with. There are several internal and external factors that are included in a security policy (Hu, Dinev, Hart, & Cooke, 2012; Soomro et al., 2015). The regulations and practices must be set into place such that all the members of a company can follow the rules. This ensures that the company has the sufficient amount of

protection for their data. Senior management is responsible for the implementation and assurance of policies, procedures, and security controls across the organization (Hagen, Albrechtsen, & Hovden, 2008).

Information Security Controls

In a business context, control can help in maintaining behaviors that can assist in improving the performance of a company (Cram et al., 2016). It is a challenge for management to implement changes and controls in any organization (Jensen, 2017). Management must exercise control over people, process, and technology through a risk awareness program to positively affect the company. There are several drivers such as internal and external threats and business and regulatory requirements, that are necessary to analyze to create a proper control system for an effective information management system (McFadzean et al., 2011). McFadzean et al. (2011) stated that senior management at board level and their support for organizational level information security initiatives will help to bring security awareness across the company with a minimal resistance from employees for a change to adopt new processes and procedures to implement new security controls.

Organizational Alignment

The entire organization's buy-in for adopting a stringent information security control using employee awareness training and workshops is an important step towards the organizational alignment with people (Hagen et al., 2008). The information security awareness should be a top-down approach, and senior management intervention will help to achieve the resources alignment at organization level.

The human resource challenge of information security management has been neglected and has focused more on technology. People, processes, and technology are the critical components of the organizational resources which are vital for an effective information security management (Ashenden, 2008). The organizational culture, communication between information security team, end users, and management should be aligned to achieve the overall information security risk and corporate risk management (Makhlouf, 2017). Risk management is everyone's responsibility.

Well established business operations with highly integrated and aligned organizational resources are vital for any organization to achieve its strategic goals. Business operations with people, process, and technology alignment will reduce the cost of information security breaches from cyberattacks (Gordon, Loeb, & Lei, 2011; Pathari & Sonar, 2013). Chang and Lin (2007) and McFadzean et al. (2011) noted that it is the responsibility of the management to align resources within in the organization to achieve organizational performance and mitigate the internal and external threats.

Accountability

Security threats are rapidly evolving and having a highly integrated and coordinated risk management strategy will help in mitigating organizational risks from cyberattacks. The economic factors, internal and external threats, and regulatory requirements are the main drivers for implementing information security controls by management (Chaudhry et al., 2012). Strategic alignment and integration of organizational resources is an important aspect for organizations and it will help to

streamline company operations to improve the efficiency and productivity of a company (Hagen et al., 2008).

Management is accountable for leading the organization and managing information security risks to achieve organizational strategic goals, efficiency, and value to stakeholders (Chander, Jain, & Shankar, 2013). Management has control of resources and decides how those resources are assigned to projects based on organizational goals. Management involvement is also essential in information security and risk management to protect the organization assets (Chen et al., 2015).

Managerial Competencies for Information Security Management

Technology draws the most focus from management and is treated with higher priority than human resources and processes (Ashenden, 2008; Bauer, & Bernroider, 2017; Stewart, & Jürjens, 2017). Human resources go through numerous challenges of discovering and handling risks to the company as technology alone cannot manage organizational risk (Burns, Posey, Roberts, & Lowry, 2017). Management tends to focus more on the technology aspect information security controls, as they is the most visible part of security infrastructure (Pattabiraman et al., 2018; Stewart, & Jürjens, 2017).

Managerial competencies are the behaviors that a manager has that align with the skills and knowledge of their field. Leaders with managerial competencies are identified by the stakeholders (Anderson & Sun, 2017; Anthony, 2017). Companies that select leaders with poor managerial competencies will suffer from financial losses and wasted resources (Eberly, Bluhm, Guarana, Avolio, & Hannah, 2017; Ulrich & Smallwood, 2012). The selected leaders have little room for mistakes as even the smallest error can

have a large negative influence on the company (Pavlou & El Sawy, 2006; Wei, Samiee, & Lee, 2014). Understanding the qualities that make a good leader will help in leadership selection. A better understanding of which leadership competencies are required in highly effective managers for managing the information security risk is a pressing research concern.

Leaders need to have a diverse set of skills that can handle a shifting business environment. The main leadership styles are intellectual, managerial, and emotional leadership. The three styles of leaderships are vastly different and require differing skill sets (Laureani & Antony, 2017; Maamari & Majdalani, 2017; Pierce & Newstorm, 2015). According to Sanchez, & Terlizzi (2017) the competencies are different factors of human characteristics that can be useful in identifying high performing employees and leaders. Candidates with high level competencies will be able to use their skill sets in a variety of business environments (Drucker, 2016; Northouse, 2018). Competencies are different from the concept of competence as they relate to the behaviors and characteristics of an individual, and not the overall quality of those characteristics (Croft & Seemiller, 2017).

Harrison (2016) reviewed empirical literature on the effect of competencies in job performance and stated that tests measuring intellectual capacity were not enough to determine quality of employees. According Lo, Macky, and Pio (2015), it would also be important to analyze employee's behavioral characteristics. The management competencies, behavioral competencies, and organizational competencies are foundational competencies for an effective manager (Harrison, 2016; Lo et al., 2015). Behavioral competencies are preferred behaviors that would be useful in any work

setting. Organizational competencies are business focused behaviors with the aim of improved performance. Competencies measure emotional, social, and cognitive intellect based on behavioral patterns (Maamari & Majdalani, 2017). The authority of the leader enables managers to control follower's decision as opposed to a more democratic approach in which the leader gives up some control (Hogan, 2017; Mendenhall, Weber, Arna Arnardottir, & Oddou, 2017; Sturm, Vera, & Crossan, 2017).

Communication Competencies

Effective communication between individuals and groups in an organization will help improve the performance of the company. Having employees that can inform and understand each other helps to better use time and resources to fulfill the goals of the organization (Bachmann, 2017; Gochhayat, Giri, & Suar, 2017; Raina, 2010). It has been found that the poor communication abilities of managers have a negative effect on the performance of the employees (Henry, 2017; Schuttler, 2010). Highly effective leaders and managers will communicate very well with team to achieve organizational goals (Harrison, 2016; Lo et al., 2015; Northouse, 2018).

The workplace has become more global and diverse. Employees must now be able to handle different interpersonal dynamics with people of different cultures and background (Anzengruber, Goetz, Nold, & Woelfle, 2017). Mayfield, Mayfield, and Sharbrough (2015) stated that challenge for managers is to effectively engage employees in information processing and sharing, problem-solving, and decision-making. The diversified social, cultural, educational, and generational differences among workforce is a new challenge for managers at workplace in today's business environment

(Anzengruber et al., 2017; Morreale, Valenzano, & Bauer, 2017). Despite the need for improved communication, there has been little practical research done on the topic of improving managerial communication. Researchers working on managerial competencies would agree that there are cognitive, interpersonal, personal, and motivational competencies (Mikkelson, York, & Arritola, 2015). Ulmer, Sellnow, & Seeger, 2017). Despite this agreement, studies have failed to identify the complete range of competencies required for effective performance of managers who are critical for organization information security and risk management (Mohamad, Nguyen, Melewar, & Gambetti, 2018; Solomon & Steyn, 2017). Communication between employees can be hindered due to multiple reasons such as social and cultural changes, intergenerational gaps, and the changing workplace environment in the global economy. New managerial methods must be established to overcome the new obstacles.

Project Management Competencies

As the expansion of the Internet in the business landscape, companies have depended on IT to conduct day-to-day business practices. However, IT projects have a high failure rate despite their importance in business (Hughes, Rana, & Simintiras, 2017). The primary goal of any organization is to create new products, systems or solutions that will create a strategic value and edge with the competition. Optimal deployment and alignment of organizational resources are required to achieve the end goal (Pavlou & El Sawy, 2006; Wei et al., 2014). The Project Management Institute (PMI) found that only 25% of IT projects were meeting their established goals, 50% of IT projects were having troubles continuing, and the remaining 25% of IT projects were failing. IT projects are

unique due to their aggressive delivery schedules, shortage of resources, and frequent scope changes demanded by the business atmosphere and changing technology standards (Stevenson & Starkweather, 2010). The competitive business conditions and changing technology landscape has mandated the need of optimal utilization of organizational resources to reduce cost and increase productivity to stay in business (Kerzner & Kerzner, 2017; Müller & Turner, 2010; Müller, Geraldi, & Turner, 2012; Stevenson & Starkweather, 2010). Papke-Shields and Boyer-Wright (2017) identified seven highly visible causes for IT project failures. The causes were: misunderstood requirement, optimistic schedules and budgets, inadequate risk assessment and management, inconsistent standards and training, management of resources, the unclear charter for the project, and lack of communication. Project managers may be trained to use emotional intelligence in their leadership style to reduce the risk of project failure (Maamari & Majdalani, 2017).

An effective and competent manager will be able to oversee a successful project (Stevenson & Starkweather, 2010). The core competency theory includes six competency areas: results orientation, interpersonal skills, personal accountability, flexibility, problem-solving, and planning and organization (Bass & Bass, 2009; Dulewicz & Higgs, 2005; Geoghegan & Dulewicz, 2008; Marx, 2017; Meng & Boyd, 2017) stated that leadership competencies and emotional awareness of project manager are a key factor in the success of project. The ability to understand and communicate with employees is just as important as the technical expertise for a project manager. The five key functions that are a part of project management are scope, organization, time, cost, and quality

Ibrahim, Boerhannoeddin, and Bakare (2017) suggested that the competencies associated with soft skills such as emotional intelligence and communication abilities were more important than the hard skill knowledge. Leaders that have soft skill abilities will be able to transition their leadership abilities into different situations. A project manager in the IT field must have technical competencies as well as leadership competencies (Meng & Boyd, 2017; Müller & Turner, 2010; Ulrich & Smallwood, 2012). Project managers that lack technical and leadership competencies will struggle in prioritizing and aligning resources, which leads to project cost and schedule overrun and impact returns on investment (Ulrich & Smallwood, 2005). Stevenson and Starkweather (2010) stated that the aggressive project delivery schedules, shortage of budgets and resources increased the risk of costly project failures.

Technical skills enhance the ability of the project manager to lead and manage through an understanding of the complex issues that develop during a project life cycle (Bauer, Richardson, & Marion, 2014). Organizations are undertaking and executing large and complex projects and it is no longer possible for a project manager to remain a technical expert in all aspects of a project. Project managers were spending most of their time scheduling, performing cost control, and monitoring progress rather than providing technical direction (Bauer et al., 2014; Frame, 2003). Müller & Turner (2010) stated that the leadership competencies should be considered when assigning project managers to projects. Project management training and development should focus not only on technical and management skills but also on the development of leadership competencies.

According to Fan, Thomas, and Anantatmula (2014), there is no formula for finding the right project manager in today's dynamic business environment and organizational context. Brill, Bishop, and Walker (2006) questioned the validity of the PMBOK in terms of breadth. He noted that there are inadequacies in the areas of project strategy, project definition, value management, and technology management in current project management standards. These inadequacies are significant as they affect the outcome of the project. Skulmoski and Hartman (2010) stated that the new research appears to have changed focus from the technical skills of a manager to more behavioral skills. The landscape of an organization is constantly changing. Managing organizational change is an essential skill for managers to have to succeed in the changing business landscape (Ahmed, & Anantatmula, 2017; Hornstein, 2015). The main factors analyzed for project success were time and costs (Ibrahim et al., 2017; Stevenson & Starkweather, 2010). The factors of product success, business benefit, and stakeholder satisfaction are analyzed when determining the success of a project in today's business environment (Dulewicz & Higgs, 2005).

Soft skills include social skills and effective personality factors that can be used for positive social interactions inside and outside a business environment (Ibrahim et al., 2017; Skulmoski & Hartman, 2010). Hard skills include technical abilities and knowledge of business procedures. Hard skills are learned through education while soft skills are developed through life experiences (Ibrahim et al., 2017). Companies are still in the process of understanding the importance of soft skills in job performance. Ibrahim et al. (2017) stated that the managers with good technical, communication and people skills

can handle the requirements of the team members and stakeholders. The six competencies involved with strategy are leadership, communication, verbal skills, writing skills, attitude, and ability to clear ambiguity (Ibrahim et al., 2017; Stevenson & Starkweather, 2010). A better understanding of which leadership competencies are required in a highly effective manager for managing and delivering the IT and information security projects on schedule and on a budget is a pressing research concern. While leadership competencies of a project manager are important factors in a project's outcome, there is a limited amount of research on the people competencies of project managers (Ahmed & Anantatmula, 2017).

Competencies for Building Secure Software

Business and government have both been victims of high-level data breaches (Chang, 2015; Houser, 2015; Huckvale, Jose, Tilney, Benghozi, & Car, 2015). The complexity and importance of software security will continue to increase along with the growth of digital systems and networks (Kushwaha, 2016). Business uses software to handle many tasks such that security protecting their information must be strong to accommodate the volume of data (Capretz, 2014; Gisladottir, Ganin, Keisler, Kepner, & Linkov, 2016; Mesquida & Mas, 2015; Touhill, & Touhill, 2014). The IoT is a rapidly emerging field that allows many electronic devices to be connected to the Internet (Ghani, Khelil, Suri, Csertán, Gönczy, Urbanics, & Clarke, 2014; Piggin, 2016). Software security also have to evolve to handle the security demands of a widely-connected system that involves the different types of electronics (Cavelty, 2014; Gisladottir et al., 2016; Jing, Vasilakos, Wan, Lu, & Qiu, 2014; Kahtan, Bakar, & Nordin, 2014; Touhill, &

Touhill, 2014). Existing systems can be built on to improve security and new systems can include high-level security software (Astuti, Muqtadiroh, Darmaningrat, & Putri, 2017; Chen et al., 2015). There are high costs involved in implementing high-level security software. Having security safeguards in software development will increase the overall development costs. The costs are needed as the security software protects the data and the system from unauthorized access. Security protocols in every phase of the development are essential as they prevent against the biggest risks of system vulnerability (Astuti et al., 2017; Houser, 2015; Kushwaha, 2016; Piggin, 2016). The industry has acknowledged that security should be included into every aspect of software design, development, and implementation (Aasi et al., 2017; Cavelty, 2014; Islam, Mouratidis, & Weippl, 2014). Despite industry encouragement, the need for enhanced security protocols in the SDLC is still being overlooked (Ghani et al., 2014; Jones & Rastogi, 2004). The problem is with the time and resources that have been allocated to implement security requirements in software changes. Another industry concern is how to best implement new security protocols and systems into the phases of software development (Ghani et al., 2014; Gisladottir et al., 2016; Jones & Rastogi, 2004; Khan, 2014; Touhill & Touhill, 2014).

The existing approach to include security controls in software design is to implement it after the development and it is very expensive. Companies that keep security design in mind while starting their software application phases will have a better chance of keeping their systems and data safe at lower cost (Gisladottir et al., 2016; Khan, 2014; Piggin, 2016; Touhill & Touhill, 2014). Including security during the initial testing of new software allows a company to find weaknesses early in the process.

Finding and correcting errors in security controls is an easier process during the early stages of the software development life cycle, than at the deployment stage. The current standard of waiting until a stage is completed before including security makes correcting errors to correct, expensive and difficult (Astuti et al., 2017; Houser, 2015; Kushwaha, 2016; Mesquida & Mas, 2015; Piggin, 2016).

Different levels of employee groups must be involved in the software design process so that the system will be able to meet the needs of everyone in the organization (Dabbagh & Lee, 2014; Gisladottir et al., 2016; Khan, 2014; Piggin, 2016; Touhill & Touhill, 2014). Software systems become more complex as time in the development cycle passes due to scope creep and lack of resource to meet new scope (Khaim, Naz, Abbas, Iqbal, & Hamayun, 2016). Integrating security processes early allows the best resources to be used for security development and prevent against weaknesses caused by oversight and limited investment (Dabbagh & Lee, 2014; Gisladottir et al., 2016; Kahtan et al., 2014; Khan, 2014; Mesquida & Mas, 2015). Many companies are reluctant to assign resources for security controls early in the software development life cycle due to the increased cost of the project (Kahtan et al., 2014). Companies that choose to include security into the initial testing have better end results with resource allocation and security strength (Aasi et al., 2017; Houser, 2015). Flaws in the initial stages of software development could be caught and fixed in a way that avoids a large time and resource commitment at a later stage of the product life cycle. The leaders and stakeholders of the organization must include early security implementation in their plans to improve their projects and data safety (Posey, Roberts, Lowry, & Hightower, 2014).

There are several reasons for organizations for not including security controls in their initial plans for software development such as budget, schedule and resource constraints. Organizational leadership should act proactively to identify the best methods for encouraging early security implementation in software development to build and implement secure software systems to address risk from data breaches (August, August, & Shin, 2014; Frydman, Ruiz, Heymann, César, & Miller, 2014; Ghani et al., 2014; Gisladottir et al., 2016).

Technology Competency for Managers

Cloud computing systems have been a hosting platform of recent technology for social networks and artificial intelligence projects (Hosseinian-Far et al., 2018; Raguseo, 2018). Artificial intelligence was a conceptual model until the faster computing processors, better algorithms, and data organized for cloud computing made it possible to build a real version for practical applications. Many organizations are hosting their information systems on cloud platforms, because of cost and flexibility of scaling as needed. One issue with the use of cloud computing system is information security (Bertino & Ferrari, 2018; Choi & Lambert, 2017; Cook et al., 2018). The main drawbacks of cloud computing are security vulnerabilities for data that are hosted on cloud infrastructure (Dave et al., 2018). Organizations must assess and evaluate the potential risks that cloud computing could bring with its flexibility and scalability. Organizations with high-value data must understand the risks and implement security protocols to use cloud computing (Khari, 2018; Mishra, Sharma, Sharma, & Vimal, 2018).

Big data and security analytics. Big data are comprised of large data structures and complex data sets that come from several independent data sources (Reddy & Sunil, 2017). The size and nature of the data make it additionally vulnerable to threats that conventional security measures are not able to combat (Olson & Wu, 2017; Raguseo, 2018; Tian, 2017). The term big data is becoming a standard part of organizational vernacular. Big data and data analytics have become a necessity for organizations making business decisions to improve organizational value and to stay competitive (Raguseo, 2018; Vassakis, Petrakis, & Kopanakis, 2018). The value of big data is in its data analytics as organizations can use the information to gain additional knowledge to develop strategies to stay ahead of the competition. Strategies developed using intelligence from big data analytics can bring in a strategic value to the organization (Hosseinian-Far et al., 2018; Reddy, & Sunil, 2017; Sagiroglu & Sinanc, 2013; Vassakis et al., 2018).

Current security measures are created for smaller sets of data and would not be able to handle the nature of big data. Organizations need to address the vulnerabilities of big data to be able to use it for their business operations (Olson & Wu, 2017; Tian, 2017). All types of business and organizations are building big data capabilities to remain a viable part of the current technological landscape (Raguseo, 2018; Vassakis et al., 2018).

Data security and confidentiality are the main concerns with big data deployment (Olson, & Wu, 2017). Many new software systems using big data are unable to handle advanced security threats (Bertino & Ferrari, 2018; Choi & Lambert, 2017; Undavia, Patel, & Patel, 2018). Many financial institutions have had wide scale public scandals due

to mass leaks of confidential data (Singh, Halgamuge, Ekici, & Jayasekara, 2018; Undavia et al., 2018). New innovations that follow cloud computing will involve big data and IoT technology (Hosseinian-Far et al., 2018). Data are needed to build on ideas and to expand on existing concepts. Data must be kept secure to maintain its value (Bertino, & Ferrari, 2018; Choi, & Lambert, 2017).

Artificial intelligence and machine learning. Machine learning is the evolution of computer technology in which the machines themselves can find solutions independently for complex problems (Andrade, Torres, & Flores, 2018; Hosseinian-Far et al., 2018). Some examples include facial recognition, virus software, and self-driving cars. Two categories of machine learning are pattern recognition and anomaly detection (Chio & Freeman, 2018). A decision support system can handle majority of security threats a company will face while implementing organizational plans to reduce threats (Andrade et al., 2018; Chio & Freeman, 2018; Hirsch, 2018; Verma, Calo, & Cirincione, 2018).

Implementation of an artificial intelligence (AI) and machine learning systems requires a specialized competency to integrate it with the existing organizational IT infrastructure and systems for organizational alignment (Hirsch, 2018; Liu, Liu, Liu, Wang, Jin, & Wen, 2018). Using automated tools for analysis could increase the effectiveness of the decision support system in data protection while reducing the total time spent on security operations (Liu et al., 2018).

Security in an organizational structure requires alignment of people, technology, and processes to identify organizational threats, develop and implement sufficient

security controls to mitigate risk from cyberattacks (Verma et al., 2018). Non-alignment of organizational resources may lead to gaps in security controls which expose organizational digital assets to cyberattacks and increased organizational risk. The additional knowledge gained by the analysis of big data will help in implementing specific strategies to handle relevant threats (Liu et al., 2018; Vassakis et al., 2018). The organizational resource alignment will increase organizational readiness with established policies, processes, trained resources, and security technology infrastructure in meeting threats from cyberattacks.

There are several opportunities for security advancement with new innovations in artificial intelligence, machine learning, and blockchain technology (Chio, & Freeman, 2018; Hirsch, 2018; Rabah, 2018) such as enabling things in IoT and continuous adaptive threat identification of risk. The zero-trust security feature of blockchain ensures identity verification of the users and keeps data safe from misuse and data attacks. The opportunity comes from the intersection of artificial intelligence and machine learning for information security risk management (Rosenberg, 2017). Artificial intelligence and machine learning can be used to determine trends in security threats and implement solutions to detect, and to identify the required security controls to prevent cyber attacks (Andrade et al., 2018; Liu et al., 2018).

There are multiple considerations that must be made when addressing the human-machine relationship of artificial intelligence (Brynjolfsson & McAfee, 2017; Morris, 2017). The increased number of data breaches has shown potential risk factors of targeted data such as the manipulation of social media regarding social issues and outcomes

(Benson et al., 2018; Demek, Raschke, Janvrin, & Dilla, 2018; Luna & Pennock, 2018). Artificial intelligence is needed to combat the high risk nature of new cyber threats (Hess & Ludwig, 2018; Kumar, Pattnaik, & Pandey, 2017; Lawless, Mittu, Sofge, & Russell, 2017; Rosenberg, 2017).

Bring your own devices. Bring your own device is when employees bring their own technology into the office to use for business purposes (Gaff, 2015; Thompson, 2017). Some devices that employees bring to office are tablets and smartphones. This is a new concept used by some companies that have been proven to increase productivity in the workplace. An issue that arises from bring your own device is that new vulnerabilities are added to the company system that places company data at risk. It is difficult to implement the same security protocols that can be implemented on a company owned device. Companies that choose to have a bring your own device policy should require strict security standards and have liability policies for their users to avoid legal issues (Gaff, 2015; Thompson, 2017). Having an approval process that requires digital certificates also helps in reducing risks.

Risks for an organization rise when managing social networks, IoT technology, and bring your own device (Kumar & Singh, 2015; Thompson, 2017). The security risks of IoT are still being determined as the implementation is still new (Kumar & Singh, 2015; Thompson, 2017). IoT technology innovations are becoming more advanced as they can learn to adapt to their environment by taking new information in and adapting to the new circumstances.

Drones and surveillance. Drone regulations must take security threats of civilian drones into consideration when developing new rules. An increased number of civilian drones need better security to handle potential safety risks such as intrusion and privacy (Lin, He, Kumar, Choo, Vinel, & Huang, 2018; Martin, Tomkinson, & Scott, 2017). Morris (2017) stated that the use of drones needs to be monitored and regulated with strict policies and operational guidelines. Today, systems of drones do not prioritize security and thus exposed to cyber attacks and data breaches. Future drone design must integrate data protection to handle vital tasks. The security of the drones that use IoT is still evolving (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015).

Internet of Things (IoT). The role of IoT technology has expanded to key business applications such as healthcare, retail, power, and industrial (Lee & Lee, 2015; Weinberg et al., 2015; Hosseinian-Far et al., 2018). IoT devices are growing in deployment as there will be 50 billion IoT devices by 2020 (Jayakumar, Raha, Kim, Sutar, Lee, & Raghunathan, 2016).

Personal and financial data used by the industry such as healthcare, finance; insurance, military, and other disciplines must be kept safe from data breaches due to its sensitive nature. Threats and vulnerability areas must be addressed by healthcare organizations when implementing IoT technology to reduce risk from data breaches (Cirani, Ferrari, & Veltri, 2013; Ning, Liu & Yang, 2015; Sicari et al., 2015).

IoT devices have limited computing power to support embedded security protocols and are vulnerable for security threats (Zhang, Cho, & Shieh, 2015). The alignment of organizational resources such as people, process, and technology is essential

while adopting IoT technology for business applications (Amaral, Tiburski, de Matos, & Hessel, 2015; Mashal, Alsaryrah, Chung, Yang, Kuo, & Agrawal, 2015).

IoT technology helps to increase productivity with its volume and scale (Weinberg et al., 2015). The data used in business transactions will be handled by IoT devices. The current security should be examined for weaknesses and those weaknesses should be corrected when the devices are implemented (Ara, Al-Rodhaan, Tian, & Al-Dhelaan, 2015; Granjal, Monteiro, & Sa Silva, 2015). Modern technology has integrated the Internet capabilities of computers and communication abilities of phones into personal devices such as tablets and smartphones. These devices face threats on multiple levels from predatory breaches of personal data to privacy breaches in social media (Bertino & Ferrari, 2018; Choi & Lambert, 2017).

Social media platforms. The rise of social media platforms such as Twitter, Facebook, Instagram, YouTube, and LinkedIn has increased the amount of data sharing and consumption on a global level (Benson et al., 2018; Demek et al., 2018; Luna & Pennock, 2018). The modern era is synonymous with the digital era. Personal information in the form of data is shared in every aspect of life from financial transactions to social interactions (Hosseinian-Far et al., 2018). Digital data exchange has altered the perception of privacy and ownership as our personal information is difficult to control once placed on a public platform (Sicari et al., 2015).

Enterprise Risk Management Competency

Risk management provides an organizational framework to identify critical assets, vulnerabilities, threats, potential risks and mitigation strategies using organizational

resources (Brustbauer, 2016; Lundqvist, 2015). Enterprise risk management is comprised of several internal and external factors. The external factors include competition from other firms, corporate governance, industry regulations, and changes in technology (Yilmaz & Flouris, 2017). The internal factors include business operations and relationship with shareholders. A good risk management strategy is holistic and balances both the external and internal factors (Farrell & Gallagher, 2015; Grace, Leverty, Phillips, & Shimpi, 2015). Employees across the organization must provide information on issues that influence different sections of the company (Babu, Babu, & Sekhar, 2013; Shad & Lai, 2015). The strategy must be able to protect the organization while complying with federal regulations.

Determining asset value and its estimated risk is the first part of risks analysis (Grace et al., 2015; Hoyt & Liebenberg, 2015; Ramakrishna, 2015). Risk management has helped the business to meet regulations such as Sarbanes-Oxley Act (Ahmed & Manab, 2016; Dionne, 2013; Lam, 2014; Lundqvist, 2015; McNeil, Frey, & Embrechts, 2015; Ramakrishna, 2015; Walker, 2013). The data from risk analysis process of risk management helps management to make better executive decisions on organizational risk (Andreea, 2014; Brustbauer, 2016; Carden et al., 2015; Shad & Lai, 2015; Steinhoff, Price, Comello, & Cocozza, 2016). The amount of total loss should be less than the expected amount of loss of an organization.

The threats that an organization faces are constantly evolving due to changes in technology and the business landscape (Nehari-Talet, 2014). The specific resources that a company needs to have continuous operations require specialized security controls (Shad

& Lai, 2015; Soomro et al., 2015). Critical assets are more vulnerable and may be under an increased amount of threats by those who want to cripple the organization from its business operations (Mbowe et al., 2014; Nehari-Talet, 2014; O'Neill, 2014; Zhang et al., 2015).

Enterprise governance. The long-term success of an organization is dependent on the ability to keep data safe. The organizational data from operations and income statements are used to make executive decisions (Carden et al., 2015; Cavusoglu et al., 2015; Chen et al., 2015; McFadzean et al., 2011). The data is very critical to business operations and vulnerable to cyber threats. Data breaches may have an effect on business continuity and organizational performance (Safa et al., 2015; Shad & Lai, 2015; Skorodumov, Skorodummova, & Matronina, 2015; Steinhoff et al., 2016).

Senior management owns the responsibility of protecting the organization from risk from cyberattacks (Shad & Lai, 2015; Soomro et al., 2015). But in any organization, the information security department is responsible for understanding company strategy and implementing suitable information security management system aligning organizational resources soliciting management support mitigate the risk to an acceptable level of the organization (Steinbart, Raschke, Gal, & Dilla, 2016). The security strategy must address requirements from business, industry-specific compliance regulations and fit into the financial budget of the company (Shad & Lai, 2015; Soomro et al., 2015).

Employees are more likely to follow the necessary protocols if they see management making security a priority. Corporate governance is helped by risk management as it provides stability in decision making (Shad & Lai, 2015; Soomro et al.,

2015). The organizational risk analysis provides a holistic view on the strengths and weaknesses of a company that can be used when developing strategies (Carden et al., 2015; Lundqvist, 2015). The board of directors is responsible for selecting employees that can fit organizational strategies into industry regulations (Lundqvist, 2015). Risk analysis also helps in aiding employee transparency that ensures quality governance.

Haislip, Masli, Richardson, and Watson (2015) also stated that an ineffective information security controls can negatively impact the financial resources of a company and bring legal consequences to senior leadership and the organization. The financial reports are governed by SOX 404 IT regulations and require ethical behavior and consistency from CEO and CFO of the organization on material weaknesses of financial reports (Cardinaels, 2015; Haislip et al., 2015). Any irregularities in reports can damage the integrity of the company (Cardinaels, 2015; Haislip et al., 2015; Otero, 2015). Additional help can come from external auditors that are not affiliated with the company (Kaya, 2018; Rubino, Vitolla, & Garzoni, 2017). Auditors have a critical role in identifying security control gaps and help information security and risk management experts in designing and implementing required controls and help management to bolster the reputation of the company by showing the company's willingness to fix the problem in a transparent manner (Cardinaels, 2015; Haislip et al., 2015; Otero, 2015; Safa et al., 2015; Skorodumov et al., 2015; Soomro et al., 2015).

Information Security Standards and Frameworks

The information security and risk management are a part of the overall organizational strategy and should be led by executive leaders that are familiar with the

organizational landscape of the company (Murphy & Murphy, 2013; Safa et al., 2015; Soomro et al., 2015). The Information Security framework is made up of multiple organizational business requirements, policies and procedures (Steinhoff et al., 2016; Shad & Lai, 2015; Soomro et al., 2015; Zhang et al., 2015). The framework should reduce the vulnerabilities of the system to prevent security threats (Ahmad & Mohammad, 2012; Murphy & Murphy, 2013; Zhang et al., 2015;). The information security and industry-specific standards are:

1. The international organization for Standardization (ISO) 27000 series

   The International Standards Organization oversees security standards with the ISO 27000 series (Mataracioglu & Ozkan, 2011). The ISO 27000 series such as ISO 27001 and ISO 27005 are mature security standards and adopted in numerous organizations from small businesses to large corporations globally for mitigating risk from cyberattacks (Ahmad & Mohammad , 2012; Bahtit & Regragui, 2013; Everett, 2011; Faris, Hasnaoui, Medromi, Iguer, & Sayouti, 2014; Watkins & Calder, 2015).

2. The National Institute of Standards and Technology (NIST) 800 series

   NIST is a federal governmental agency for responsible for standards that oversee the governmental use of technology. The organizations have used the NIST framework for over 2 decades (NIST, 2018; Pendley, 2018). The framework holds a myriad of security standards and strategies (Dedeke, 2017; Hiller, & Russell, 2017; NIST, 2018; Pendley, 2018). The NIST framework is useful as it helps in developing secure systems for complex systems. Large organizations benefit as

the numerous security threats they face require nuanced solutions (Ross, Katzke, Johnson, Swanson, & Stoneburner, 2008; Tenable, 2018). NIST works closely with ISO to develop and manage security guidelines such as NIST 800-53 and NIST 800-30 to guide organizations in the U.S for risk mitigation from internal and external cyber threats (Das et al., 2012). Smaller organizations can also benefit due to the ease of integrating NIST framework into the organizational framework.

3. The Committee of Sponsoring Organizations

   The Committee of Sponsoring Organizations works to create and implement strategies to reach the compliance goals of risk management (Kaya, 2018; Pierce & Goldstein, 2018; Rubino et al., 2017).

4. The control objectives for information and related technologies

   The control objectives for information technology develops objectives for proper IT that comply industry standards and regulatory compliances (Heninger, Johnson, & Kuhn, 2017; Pereira, Ferreira, & Amaral, 2017; Rubino et al., 2017). The control objectives for information and related technologies framework reduces risks through identification and mitigation (Ahmad & Mohammad, 2012; ISF, 2014; Mataracioglu & Ozkan, 2011; Tofan, 2011).

5. Industry-specific standards

   There are certain framework standards that target the needs of a specific industry that control objectives for information and related technologies and NIST are not able to meet. Standards such as Sarbanes-Oxley (SOX) for financial reporting

with integrity and transparency (Gao & Zhang, 2018; Govindji et al., 2017; Rubino et al., 2017; Cardinaels, 2015). The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for credit card processing (Haber & Hibbert, 2018; Nicho, 2018; Sabillon, 2018).

The Health Insurance Portability and Accountability Act of 1996 is the United States legislation that provides data privacy and security provisions for safeguarding medical information (Chen & Benusa, 2017; Farhadi, Haddad, & Shahriar, 2018). The health industry has the Health Insurance Portability and Accountability Act that sets security and confidentiality standards for health records and medical information (Chen & Benusa, 2017; Farhadi et al., 2018; Haber & Hibbert, 2018). The need for additional legal standards comes from the increased amount of harm that could result from leaked medical records (Farhadi et al., 2018; Haber & Hibbert, 2018).

The Committee of Sponsoring Organizations and NIST frameworks are widely used in the business landscape as part of the organizational security framework (Wieczorek-Kosmala, 2014). Companies choose one or the other depending on the needs of their organization. NIST framework is used in federal governments and places a high priority on mitigating risks from breached data systems. NIST is easy to adapt to existing organizational framework (Paape & Speklé, 2012).

Committee of Sponsoring Organizations frameworks are commonly chosen for the security needs of corporate organizations. Businesses place a higher level of trust in Committee of Sponsoring Organizations frameworks (Kaya, 2018; Pierce & Goldstein,

2018; Rubino et al., 2017). The Committee of Sponsoring Organizations was developed by private auditing employees while NIST was created by the government (NIST, 2018; Pendley, 2018). The framework of Committee of Sponsoring Organizations is also applicable to a wide range of organizations (Das et al., 2012). The use of components differs between Committee of Sponsoring Organizations and NIST while the components themselves are similar.

Developing a security framework is integral to the success and protection of a company. Employees of all levels and fields should be included in the decision making so that all types of data in the company are protected (Barafort, Mesquida, & Mas, 2017; Leszczyna, 2018; Von Solms & von Solms, 2018). Executive leaders should be involved in the planning process and should direct other employees to share their security requirements (Dedeke, 2017; NIST, 2018; Von Solms & von Solms, 2018; Watkins & Calder, 2015).

According to Tenable (2018) and Von Solms and von Solms (2018) there are several factors involved in implementing a security framework into an existing organizational structure. Many organizations use multiple frameworks to target different issues and threats (Dedeke, 2017; NIST, 2018; Pendley, 2018). Existing frameworks have strengths that can be used for some parts of the organizations that may not be of useful in other parts. Organizations should use current frameworks as a reference for creating a specific framework that can handle their unique requirements (Yeo, Rolland, Ulmer, & Patterson, 2014).

The resources and time that are needed to implement a new framework would be analyzed against the needs of the organization (Heninger et al., 2017; Pereira et al., 2017; Rubino et al., 2017). There are situations where the existing frameworks are sufficient for an organization. Ahmad and Mohammad (2012) also stated every organization has different risks and priorities when conducting the risk analysis and risk management based on organization size, geographical location, and its industry segment (Tenable, 2018).

Summary and Conclusions

This literature review includes various leadership theories and competencies that are essential in containing risk from ever-increasing cyber threats. This literature review took broad-based categories and narrowed in on specific areas that inform the topic of this study. A review of various aspects of competencies, cybersecurity, data breaches, and risk was conducted to provide the foundation for this research study. A description of what is known and unknown is provided with this literature review.

Through this review of the literature, various data breaches and skills were identified as they relate to cybersecurity. This literature review examined the theoretical basis for leadership, competencies information security managers. Leadership has been a prominent topic in scholarly research for decades. The study of information security management shares many of the same attributes of general management literature but at the same time, there are unique characteristics, such as technical, people skills, communication skills, and finance expertise that makes information security management a unique role within the organization. The literature suggests technical competencies and

minimal on general management skills for information security managers, but nontechnical skills and technical skills are critical to align organizational resources such as people, process, and technology to contain the organizational risk.

I identified significant competencies for an information security manager for managing organizational information security risk. The project management skills for delivering information security projects on schedule, information security and risk management domain knowledge, regulatory and compliance expertise, and emerging technologies and their risks are critical for managing risks from cyberattacks on organizational business-critical digital assets. (Skulmoski & Hartman, 2010). This study findings provided an additional support for many of the key competencies that have been identified for implementing an organizational information security management system for mitigating risk.

The objective of this study was to investigate and provide qualitative data showing how the need of managerial competencies can play a major role in aligning organizational resources to mitigate the risk from cyberattacks and data breaches. This study enhances the literature by investigating the managerial competencies impact of information security breaches. Most the prior studies on the effects of security breaches on competencies were limited to technical competencies to mitigate cyber threats.

Several researchers have studied the effect of security regulations and controls on data breaches in many organizations and leadership involvement and support, but not explored the competencies of people who are leading the effort. This study may provide a

valuable contribution to the research literature on managerial competencies that are effective in managing organizational risk from cyber threats.

Based on the literature review, there is an information security and risk management skills shortage among non-information security professionals and non-technical skills such as leadership, communication, and project management skills shortage among information security professionals. As the intent is to solicit expert opinions, the study would be a qualitative approach using a Delphi technique with an expert panel chosen for their experience and expertise in the field of SDLC. Chapter 3 includes the methodology, population, sampling procedure and hypotheses formulated to study this topic. Chapter 3 also includes the research method, sample and population, instrumentation, validity, reliability, data collection, data analysis, and report.

Chapter 3: Research Method

The purpose of this qualitative Delphi study was to explore the managerial competencies that senior managers need to align and integrate organizational resources such as people, process, and technology to manage information security and risk to prevent cyberattacks. This study may be useful in determining the competencies that can increase the effectiveness of information security procedures such that organizational data can be protected. Chapter 3 contains details on the research methodologies and procedures. The Methodology section includes details of the Delphi technique and the reasons for its selection. The benefits and liabilities are detailed for a holistic view of the Delphi technique. The section on procedures includes the population selection, the process involved in population selection, the data selection process, and the analysis process. The data used for analysis were collected from an expert panel of information security and risk management experts. The required approval of institutional research methods and ethical guidelines regarding participant safety are also included in this chapter.

Research Design and Rationale

The role of senior management is to build critical competencies for IT managers, who are responsible for implementing information security controls by aligning and integrating organizational resources to mitigate security risks. Specific competencies were analyzed through data from questionnaire responses provided by an expert panel to test the research question: What competencies should senior managers develop to align and integrate organizational resources such as people, process, and technology to detect

and mitigate the risks of cyberattacks on enterprise critical assets? The research question is the main driver of the research approach and methodology during a research study (Cooper & Schindler, 2011; Marshall & Rossman, 2011; Morgan, 2008; Salkind, 2012; Sekaran & Bougie, 2013). This research was built on knowledge about several qualitative questions regarding the current state of managerial competencies and gaps in competencies needed to face the challenges of cyber threats and vulnerabilities. I selected a qualitative inquiry to conduct an in-depth data analysis from a practicing information security and risk management expert sample of participants. The questions were set up to identify the needed managerial competencies that can address the challenges of cyberattacks on critical assets of the organization.

The Rationale for Using the Delphi Technique

My research benefited from the Delphi technique because of the limited amount of empirical data and research on the security effect of managerial competencies. There were also limitations in the data available on the connection between information security management and the reduction of cyberattacks. These gaps in knowledge increased the difficulty of using traditional methods of research for research studies (Eycott, Marzano, & Watts, 2011; Powell, 2003). Quantitative, qualitative, and mixed methods research studies are difficult to conduct when there is a lack of substantial data (Eycott et al., 2011; McCusker & Gunaydin, 2015).

Despite being a traditional research method, the Delphi technique allows research to be conducted without existing literature, making it an effective research tool in the field of managerial competencies and data security (Brady, 2015; Clayton, 1997; Haynes

& Shelton, 2017; Linstone & Turoff, 1975). The Delphi technique has been found to be a useful tool for investigating issues where analytical precision may be impossible but the subjective opinions of a group of experts could lead investigators closer to a solution of the problem (Brady, 2015; Cole, Donohoe, & Stellefson, 2013; de Loë, Melnychuk, Murray, & Plummer, 2016; Haynes & Shelton, 2017). The Delphi technique has also been found to be an effective research tool in studies with a limited time frame and in areas of study with limited existing information.

Along with the Delphi technique, I used an expert panel because it provides independent backgrounds on the topic and allows a consensus to be formed based on the collective expertise of the participants (Clayton, 1997; Eycott et al., 2011; Meijering, Kampen, & Tobi, 2013). An analytic research method would have been difficult to implement due to the subjective nature of the topic (Sekaran & Bougie, 2013; Strasser, 2017). The reliance on expert opinions also increases the value of the study (Clayton, 1997; Dalkey & Helmer, 1963; Posey et al., 2014). The expert panel in this study worked to come to a consensus on critical managerial competencies, and data were collected from the subjective ideas of group members. Though each expert has a varied stance on which managerial competencies contribute to efficiency, the guided questions in this study narrowed the topic such that a consensus was more likely to be found (see Heiko, 2012; Hsu & Sandford, 2007; James, & Warren-Forward, 2015). As the area of study had limited information, the expert panel responses to my questionnaires were used to obtain answers to my research question (see Eycott et al., 2011; Heiko, 2012; Singh, 2015).

The Delphi technique is flexible and can be used in a variety of research methods (McCusker & Gunaydin, 2015; Salkind, 2012; Strasser, 2017). The most common use for the Delphi technique is in cases with limited amounts of information (Clayton, 1997; Dalkey & Helmer, 1963; Strasser, 2017). As the area of data security is still new, there are large gaps in knowledge. Thus, the Delphi technique was able to provide nuanced data for analysis (Brady, 2015; de Loë et al., 2016; Gupta & Clarke, 1996; Haynes & Shelton, 2017; Hsu & Sandford, 2007).

Benefits of the Delphi Technique

A benefit of the Delphi technique was that it is easy to understand (Thomas & Magilvy, 2011; Trevelyan & Robinson, 2015; von der Gracht, 2012). There was no need for advanced knowledge of research methodologies, whereas quantitative and mixed research methods require specialized training in statistical analysis. The skills needed to use the Delphi technique are easy to learn and could benefit studies with short timelines (Brady, 2015; Clayton, 19975; Cooper & Schindler, 2011; Donohoe, Stellefson, & Tennant, 2012). The anonymous nature of Delphi studies was another benefit because it allowed participants the comfort to share their honest opinions.

Research studies that benefit the most from the Delphi technique are areas of study with a limited amount of existing data. A lack of comprehensive data prevents the use of traditional research methods (Brady, 2015; Donohoe et al., 2012; Hsu & Sandford, 2007; Skinner et al., 2015). Using the Delphi technique allows an in-depth analysis of managerial competencies using expert opinions. The lack of existing literature does not

hinder the progress of the study as the background information comes from an expert panel.

Along with the benefits, the Delphi technique also contains liabilities. One of the liabilities is the amount of influence the researcher has throughout the data collection process (Clibbens, Walters, & Baird, 2012; Donohoe et al., 2012; Eycott et al., 2011; Rowe & Wright, 2011). The researcher is involved in collecting data, creating survey questionnaires, and analyzing data. These interactions increase the possibility of interference. Even unintentional influences from the researcher can undermine the validity of the study and invalidate the conclusions (Okoli & Pawlowski, 2004; Rowe, & Wright, 2011). Time constraints are also a liability with the Delphi technique (Donohoe et al., 2012; Haynes & Shelton, 2017). The short time span between data collection and the feedback process places pressure on participants and researchers (Hsu & Sandford, 2007). The researcher needs to keep up with the schedule of providing feedback and developing new surveys. Some participants may not turn in certain surveys and that contribute to low response rates (de Loë et al., 2016; Gupta & Clarke, 1996; Haynes & Shelton, 2017; Hsu & Sandford, 2007). This decreases the amount and quality of the data that is required for analysis. Sizable panels with 12-20 participants should be selected to ensure a stable influx of data (Cleary et al., 2014; Hsu & Sandford, 2007; Trevelyan & Robinson, 2015).

The researcher must maintain a level of consistency throughout the study to reduce the effects of any liabilities that the Delphi technique provides (Hasson & Keeney, 2011; Rowe & Wright, 2011; Strasser, 2017). The flexible nature of the Delphi technique

can be helpful or a hindrance depending on how the researcher handles the technique during the study. However, I chose the Delphi method as the best suited for my study.

Role of the Researcher

As the researcher, I had several responsibilities throughout the study. I identified several industry experts for the panel with information security and risk management experience at Fortune 500 companies in the United States. Recruitment of the participants included research procedures to protect the rigor of the study and ensure continued participation throughout the study. The privacy protections of the expert participants were an integral aspect of the study (Donohoe et al., 2012; Nowack et al., 2011). The participants were given details of privacy procedures that were enforced throughout the study to maintain confidentiality. Personal information from recruitment documents and e-mail communication were obscured for protection.

The biggest threat to this study was researcher bias. Any biases could result in the obscuring of collected data, which would negatively affect analysis. It was important to reflect on every step of the data collection process to ensure validity and rigor of the collected data (Marshall & Rossman, 2011; Mendoza, 2014). Several experts in the fields of business administration and business policy were recruited to assist with the feedback process. This helped to decrease the amount of time spent on creating analysis and developing the next rounds of data collection. The ability of participants to view data also decreased the possibility of bias (Rowe & Wright, 1999; Thomas & Magilvy, 2011; von der Gracht, 2012). With the Delphi technique, the participants can also change their views on competencies after feedback and the answers of other panel members are

provided (Heiko, 2012; McCusker & Gunaydin, 2015; Salkind, 2012; Strasser, 2017). This allowed an exchange of ideas with the hopes of a final consensus.

Methodology

I used the Delphi technique to identify the competencies that best aligned the resources of people, processes, and technology in organizations. The Delphi technique is an iterative process that uses expert opinions (Clayton, 1997; Dalkey & Helmer, 1963; Eycott et al., 2011; Heiko, 2012; Hsu & Sandford, 2007; James & Warren-Forward, 2015). The Delphi technique has been used by researchers since the 1950s (Loo, 2002; Linstone & Turoff, 2002; Rowe & Wright, 1999) and is used for a variety of research methods, especially in cases with large gaps of knowledge. The research steps of problem identification, solution development, solution validation, and forecasting can benefit from the Delphi technique (Eycott et al., 2011; Salkind, 2012). The emphasis on communication between researcher and participants allows for a more nuanced understanding of the research topic. The goal of the Delphi technique is to find a consensus that is minimally contested by experts in the field (Hsu & Sandford, 2007; James & Warren-Forward, 2015).

Essential factors used for the Delphi technique are sample selection, expertise criteria, set number of research participants, initial questions, stable mode of interaction, multiple rounds of data collection, level of consensus, and the validity of data (Gupta & Clarke, 1996; Keeney, Hasson, & McKenna, 2006; Landeta, 2006). The interactions are comprised of anonymous participation of experts in the field of research (James & Warren-Forward, 2015; Strasser, 2017). In this study, the data were collected

anonymously through three sets of data collection. Feedback was provided between the sets of data analysis (Brady, 2015; Cole et al., 2013; de Loë et al., 2016; Gupta & Clarke, 1996; Haynes & Shelton, 2017; Hsu & Sandford, 2007). The feedback that is provided between questioning helped to clarify responses and reduced the variation of individual answers.

The feedback that is provided between rounds of questioning is based on the analysis of the responses (Sekaran & Bougie, 2013; Okoli & Pawlowski, 2004; Strasser, 2017). Despite the importance of consensus, researchers should avoid having participants interact with each other, and participants should not be questioned as a group. Discussions among participants can allow pressure from other participants to change answers (Brady, 2015; Cole et al., 2013; de Loë et al., 2016). Pressure from other participants can also decrease the understanding of the research topic as people can feel uncomfortable providing converging or controversial opinions (Clayton, 1997; Dalkey & Helmer, 1963). The answers from each participant are analyzed between rounds of questioning as well as against other participants (Gupta & Clarke, 1996; Haynes & Shelton, 2017; Hsu & Sandford, 2007). This allows for intensive discussions with multiple perspectives (Okoli & Pawlowski, 2004; Posey et al., 2014; Strasser, 2017).

Similar to other research methods, the Delphi technique has certain advantages and disadvantages. The advantages of the Delphi technique are that it is inexpensive and allows efficient data collection (Donohoe et al., 2012; Gupta & Clarke, 1996; Haynes & Shelton, 2017). The anonymous data collection also prevents outside influences from affecting the end results. Expert involvement allows a higher-level conclusion to be

formed. The disadvantages of the Delphi technique are that the small sample sizes can be unreliable when conducting analysis (Clibbens et al., 2012; Donohoe et al., 2012; McCusker & Gunaydin, 2015). However, issues with the sample size can be avoided with careful selection of participants that will provide the best possible data (Cleary et al., 2014; McFadzean et al., 2011). Additional disadvantages include the pressure that participants may feel to accommodate other views of participants. As questioning continues until a consensus is reached, researchers will need to ensure that participants feel comfortable in their answers to ensure reliable results (Donohoe et al., 2012; Giorgi, 2002; Haynes & Shelton, 2017). Feedback between question sets narrow answers from open-ended questions (Skinner et al., 2015; Strasser, 2017). The Delphi technique ensures reliability as it exposes the study to a panel of differing, and often contradictory, opinions while seeking convergence through subject matter experts' feedback (McFadzean et al., 2011).

I used anonymous online questionnaires. The data collected from the questionnaire were analyzed for feedback before additional rounds of questioning. The e-mail to recruit participants contained the questionnaire. Qualitative research methods were used in the questionnaire for collecting expert opinions in the field of information security and risk management (Haynes & Shelton, 2017; Posey et al., 2014; Skinner et al., 2015; Strasser, 2017).

Population

The target population for this research study was the senior managers in the fields of information security and risk management. The expert participants had a minimum of

15 years of experience in their respective fields and worked at notable organizations in the United States. The expert participants provided valuable data used to answer research questions (see Posey et al., 2014; Strasser, 2017; von der Gracht, 2012).

Research Study Participants Sample Selection

The participants were selected through purposeful sampling. Purposeful sampling is when the researcher selects participants based on their ability to provide relevant data for the study (Cleary et al., 2014; Haynes & Shelton, 2017; Hasson, Keeney, & McKenna, 2000; Skinner et al., 2015; Strasser, 2017). The Delphi technique is most helpful when researching topics in specialized fields that the general population would have limited knowledge (Linstone & Turoff, 2011; Posey et al., 2014; Strasser, 2017). Experts in the information security and risk management domain have an advanced understanding of their domain that would greatly benefit this research study.

Data Collection and Analysis

The data collection process began after getting approval from the Walden University Institutional Review Board (IRB; approval no. 01-29-19-0491679). This study contained three rounds that were completed by a panel of experts in the information security and risk management domain. The surveys were in a questionnaire format. The intent of the questionnaires was to develop a greater understanding of the managerial competencies required to best protect and manage company data.

Data Collection

Participants completed a consent form before beginning the research survey. The participants were given a score after each task was completed in the survey. The score

was recorded on a password protected spreadsheet. Data screening was done before analysis to ensure accuracy and consistency (Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). Potential data errors and quality issues were identified and resolved to maintain the integrity of the research study. Examination of data was also done before the final round of analysis to check for missing data to ensure data consistency (Cleary et al., 2014; James & Warren-Forward, 2015; Lee-Jen Wu et al., 2014; Strasser, 2017). Missing data can potentially damage the accuracy of research conclusions (Donohoe et al., 2012; Haynes & Shelton, 2017).

During the research, the expert panel was asked to rank managerial competencies in order of importance and to provide additional competencies they felt would be helpful in managing information security (Clayton, 1997; Eycott et al., 2011; James & Warren-Forward, 2015). Data were collected from 12 information and risk security experts from a variety of industries. Having a collection of experts from multiple fields helped to cultivate a holistic conclusion that can be applied across industries (Posey et al., 2014; Strasser, 2017; von der Gracht, 2012). The study contained a review of existing research done on the topics of information security, data breaches, and managerial competencies. The themes identified during the literature review as shown in Appedix F were used in the development of the first round of data collection. The first round of expert input via the Delphi technique was analyzed and used for the following two rounds of data collection (Brady, 2015; Haynes & Shelton, 2017; James & Warren-Forward, 2015). Feedback from the Rounds 1, 2, and 3 were sent to the participants through email. The expectation is that a consensus will be achieved after the third and final round of data

collection (Heiko, 2012; Hsu & Sandford, 2007; James & Warren-Forward, 2015). The end goal was to find universal managerial competencies that could be beneficial in the fields of information security and risk management to mitigate the organizational risk of cyberattacks and data breaches.

Participant Selection Logic

Expertise is an integral part of the Delphi technique as expert participants provide the most nuanced conclusions (Clayton, 1997; Posey et al., 2014; Strasser, 2017; von der Gracht, 2012). Participants needed to have 15 to 20 years of information security and risk management experience to be considered experts. The experience must also come from working at credible organizations (Hsu & Sandford, 2007; James & Warren-Forward, 2015; Powell, 2003). The accumulated knowledge and years of experience help in answering the research questions (Posey et al., 2014; Strasser, 2017). The end goal of the Delphi technique is to come to a consensus from the research questions and data from the expert panel.

The definitive size of Delphi studies varies depending on the topic and scope of the research topic. Sizes vary depending on the complexity of the subject, the number of experts available in the field of study, and resources of the researcher (Cleary et al., 2014; Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). The generally accepted size is 12-30 participants (Clayton, 1997; Dalkey & Helmer, 1963; Eycott et al., 2011; Heiko, 2012; Hsu & Sandford, 2007; James & Warren-Forward, 2015). Despite the small sample size, the expert participants provide valuable data that to be used in research analysis.

Expert participants in the Delphi study are selected from multiple fields including technology, finance, retail, manufacturing, insurance, telecommunications, and healthcare. The experts of information and risk management in various fields bring a diverse range of perspectives when answering the research questions (Posey et al., 2014; Strasser, 2017; von der Gracht, 2012). The participants were asked to join the study via email. They were required to sign a consent form to officially join the research study.

The expert participants were not intended to be representatives of the information security field. The industry is too vast for every sector to have representation. The participants were selected for their unique perspectives and expertise (Posey et al., 2014; Powell, 2003; Strasser, 2017). In the Delphi technique, expertise is based on the level of credibility that an individual has in their respective field (Clibbens et al., 2012; de Loë et al., 2016; Hasson & Keeney, 2011; Mendoza, 2014). The amount of relevant information an employee has bolsters the value they provide to a research study. The perception of credibility enhances the end conclusions (de Loë et al., 2016; Hasson & Keeney, 2011).

The participants of the study have years of experience in a variety of fields. The types of fields include public organizations, private organizations, non-profit organizations, startup companies, Fortune 500 companies, and federal organizations within the United States. The expert panel had information security and risk management expertise in industry sectors such as finance, healthcare, retail, technology, and insurance. The profile of the participants was vast and multifaceted. The various managerial competencies that were considered useful benefit organizations in mitigating information security risk across the industry.

Expert participants were questioned on the relevancy of each survey question to analyze the value of managerial competencies (Hasson et al., 2000; Haynes & Shelton, 2017). Using expert feedback in developing new questions takes the participants into consideration while making the study more reliable and trustworthy (Clibbens et al., 2012; de Loë et al., 2016; Hasson & Keeney, 2011; Strasser, 2017).

Sampling

Participant selection of studies using the Delphi technique requires experts in the specific field of study (Cleary et al., 2014; Haynes & Shelton, 2017; Skinner et al., 2015). Experts in the field of information security and risk management provided a range of nuanced perspectives of the research topic (Posey et al., 2014; Strasser, 2017; von der Gracht, 2012). A sample size of 12 participants allowed for multiple perspectives of the large topic of study (Cleary et al., 2014; Haynes & Shelton, 2017; McFadzean et al., 2011; Skinner et al., 2015).

Email requests were sent to potential research study participants. The emails contained detailed explanations of the goals and nature of the study. The data collection process was explained as part of the nature of the study. The iteration process had three rounds of online questionnaires with feedback provided between rounds (Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). Consent forms were also be included in the email. The consent forms required the consent of participation and understanding of the study (Cleary et al., 2014; James & Warren-Forward, 2015; Lee-Jen Wu et al., 2014; Morgan, 2008). After receiving the emails, participants who decided to join the study had to sign the consent agreements. I then sent confirmation emails along with

links to the online questionnaires. Each participant was assigned an identification number to maintain anonymity (James & Warren-Forward, 2015; Strasser, 2017). The password for the first round was included in the email for the first round of data collection.

Instrumentation

The first round of questionnaires was developed using the information found in the literature review as shown in Appendix D. The questions helped guide the interviews with the expert participants (Eycott et al., 2011; Heiko, 2012; Hsu & Sandford, 2007; James & Warren-Forward, 2015). The study included open-ended questions in later rounds of questioning such that extensive analysis can be done (Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). The topics of the first found of questioning were data breaches and effects, information security, risk management, leadership competency, project management competency, communication competency, and technical competency.

Pilot Study

I conducted a pilot study before the first round of questioning. Pilot studies help to maintain the rigor of collected data (Clibbens et al., 2012). Pilot tests prevent inconsistencies as they provide feedback from the research participants, such that changes can be made to the data collection process and questions.

The pilot study was made up of three experts in the field of information security and risk management. Established questions were used to drive the study. The research participants were asked nine questions on the topic for the first round of data collection.

The feedback allowed fine-tuning questions and methods of questioning and thus biases and inconsistencies could be reduced.

My role in the pilot study was to select the expert participants, restructure research questions based on feedback, and to maintain consistent communication with the pilot study participants. Researchers have often used pilot studies to determine the transferability of the Delphi method (Clibbens et al., 2012). Even though the Delphi method is used in a myriad of research studies, the researcher should be able to adapt the method to fit the needs of the study (Skulmoski et al., 2007). My research study used broad and focused questions such that the panel of information security experts could provide their varying perspectives on the organization information security and risk management to reduce risks from cyberattacks.

The qualitative questions of a research study drive the focus of the study such that relevant data can be collected. Studies that start off with weak questions have a difficult time realigning the focus of the study. Researchers need to formulate questions that receive relevant data without interference from researcher biases. I addressed potential issues with my research questions by working with the committee on my initial round of questioning and using a pilot study to address issues during data collection. Pilot studies require testing of research questions before the first round of questioning (Linstone & Turoff, 1975). The pilot tests can be conducted on the participants of the study so that immediate changes can be made to the study. Pre-testing has been found to be important in maintaining the reliability of results (Okoli & Pawlowski, 2004).

Procedures for Recruitment, Participation, and Data Collection

An email was the primary mode of interaction during this research study. The expert participants were sent questionnaires for responses and analysis. There were three rounds of questionnaires until consensus was found. The data collected was kept anonymous to protect the confidentiality of the participants (Clibbens et al., 2012; de Loë et al., 2016; Mendoza, 2014). The Delphi technique is heavily focused on privacy as it allows participants to respond without external pressures (Brady, 2015; Haynes & Shelton, 2017; James & Warren-Forward, 2015). The exchange of data was monitored by me such that irrelevant data could be removed before analysis begins.

Iterations of data collection are a major part of the Delphi technique. Iterations helped participants fine tune their perceptions or change their opinions from round to round, and allowed me to provide feedback to the participants (Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). Delphi studies have one to three rounds of questioning (Skinner et al., 2015; Strasser, 2017). The preferred outcome is to gain a consensus about the topic and to obtain a deeper level of understanding of managerial competencies. There were three Rounds of data collection with the goal of a consensus between participants after Round 3 (Brady, 2015; de Loë et al., 2016; Haynes & Shelton, 2017; Hsu & Sandford, 2007).

Data Analysis Plan

Data analysis was performed based on collected data (Alias, 2015; Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). The analysis helped find the most efficient managerial competencies to guide me in information security and risk

management. The Delphi technique helped in providing reliable results that could be used to form an exhaustive conclusion (Brady, 2015; Haynes & Shelton, 2017; James & Warren-Forward, 2015). There were five potential limitations in this research study that should be considered such that data integrity is not compromised (Donohoe et al., 2012; Giorgi, 2002; Haynes & Shelton, 2017). The limitations are the small population sample of expert participants, the exhaustion of participants from multiple rounds of questioning, the few perceptions from multiple rounds of questioning, the possibility of bias from the researcher, and the possibility of selection bias due to nonrandom selection (Haynes & Shelton, 2017; James & Warren-Forward, 2015).

Delphi round 1. The first round of the Delphi technique started with the participants receiving their first online questionnaire with details on the research study, methodologies, and return dates. The questionnaire included the overarching research question on the competencies that will best guide information security and risk management (Posey et al., 2014; Strasser, 2017). Participants ranked the competencies in order of importance using the 5-point Likert scale. Open-ended questions allow the participants to include additional competencies that would help management. There were 20 questions and two additional open questions. The questionnaire was sent via email and was due after a week such that feedback can be compiled.

Analysis of responses from round 1. Statistical analysis was performed on the collected data during Round 1 and presented for Round 2 (Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). The data was stored in Excel spreadsheets. The data

was analyzed for all participants before feedback was created and returned. The first round included the ranked competencies and answers from the open-ended questions.

Delphi round 2. The second round of questioning included a new questionnaire based on analysis done on Round 1 to rank the managerial competencies. The Round 2 questionnaires were sent through email to participating experts with a due date. Follow up reminders were sent as required to obtain participants attention. Participant responses were kept anonymous to protect confidentiality (Brady, 2015; Haynes & Shelton, 2017; James & Warren-Forward, 2015). New questions were added based on the feedback created from the first round of questioning. The Likert scale was also used to rank managerial competencies.

The competencies that had the greatest level of consensus were grouped together and the competencies with the least level of consensus were grouped together (Clayton, 1997; Eycott et al., 2011; James & Warren-Forward, 2015). Any new competencies that were suggested in the open questions were included. Participants were sent feedback from the first round of questioning and other participant's opinion such that participating experts had an opportunity to review and change their ranking of managerial competencies if needed (Cleary et al., 2014; McFadzean et al., 2011). This gave the participants an opportunity to alter their answers or to solidify their original views (Landeta, 2006; Mendoza, 2014; Strasser, 2017). The answers of other participants were summarized in a short statistical analysis of the entire group (Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017)

Analysis of responses from round 2. There was a statistical analysis performed on the second round of data collection (Cleary et al., 2014; Lee-Jen Wu et al., 2014; Morgan, 2008). The questionnaire answers were collected in an Excel spreadsheet. The 5-point Likert scale was used to rank competencies. A mean score was calculated based on the total rankings of each competency. The consensus level for this study was set at 80% of agreement on each themed statement between participating information security experts. The competencies that score in the top five were used for creating a questionnaire for Round 3.

Delphi round 3. The data from the second round of questioning were analyzed and condensed in a statistical summary. The summary included the most important competencies that the participants could come to a consensus on. A slideshow was created with the survey results as well as a new survey based on earlier results. The survey was emailed to participants for Round 3 data collection. Participant identities were still kept anonymous to avoid unreliable data (Mendoza, 2014; Strasser, 2017). The Likert scale was used to rank competencies that had the lowest level of consensus. The bottom five competencies on each round of questioning were included in the ranking. The new survey was also include new items suggested in the previous answers. Feedback was provided based on earlier analysis and the new summary helped guide new answers from participants.

Analysis of responses from round 3. A statistical analysis was conducted on data collected from Round 3 responses from participating experts. The responses with the highest level of consensus was chosen for a final summary. The summary included a

spreadsheet and a graphical representation of the findings. The physical view of findings was in developing a conclusion of the research questions of best managerial competencies for data security.

Level of Consensus

Based on the Delphi technique, the data collection process ended after participant answers reach a final level of consensus after Round 3 (Clayton, 1997; Eycott et al., 2011; Heiko, 2012; Hsu & Sandford, 2007; James & Warren-Forward, 2015). The full consensus was potentially difficult to reach due to the complexity of the topic (Posey et al., 2014; Strasser, 2017). I used statistical methods to analyze the three rounds of data. The participants were asked to reassess their responses to questions that lacked a common consensus during the third round of questioning. Most Delphi studies use statistical analysis when determining the median, range, and standard deviations of data (Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). The standard deviations and mean values are important elements for reaching consensus. The mean, standard deviation, majority agreement, and ranges were used to determine the final outcome for this research study (Cleary et al., 2014; Lee-Jen Wu et al., 2014; Morgan, 2008). Responses with the least amount of disagreement are the most realistic end goal (Eycott et al., 2011; Gupta & Clarke, 1996). Consensus is reached when the responses of participants are finalized and will likely not change (Hsu & Sandford, 2007; James & Warren-Forward, 2015). The three rounds of questioning helped in cultivatating high-level answers for consensus.

Issues of Trustworthiness

Credibility

Rigor is defined in the academic setting as the value of being methodical and accurate (Haynes & Shelton, 2017; James & Warren-Forward, 2015; Thomas & Magilvy, 2011). Rigor is important when conducting research studies as it ensures a level of consistency in research methodologies. Researchers who value rigor will strive to have data that is valid and reliable (Cleary et al., 2014; James & Warren-Forward, 2015; Lee-Jen Wu et al., 2014; Strasser, 2017). The value of verification is also important during research as it provides quality in data and results. Strategies with a strong focus on verification help guide researchers to amend the research process during times of inconsistencies (Donohoe et al., 2012; Giorgi, 2002; Haynes & Shelton, 2017; James & Warren-Forward, 2015). Verification and rigor are correlated with proper verification methods to ensure rigor. Procedures should be altered when the researcher has doubts about the consistency of data collection (Skinner et al., 2015; Strasser, 2017).

The Delphi technique has a special approach to rigor that differs from traditional scientific methods. Delphi seeks to demonstrate the rigour of research studies by using the goodness criteria (de Loë et al., 2016; Mendoza, 2014; Powell, 2003). The goodness criteria value the reasoning behind decisions in the research process as well as the strength of execution. The Delphi technique is beneficial when analyzing the specific managerial competencies that can reduce risk (Posey et al., 2014; Strasser, 2017; von der Gracht, 2012). The three rounds of questions were useful in collecting data from expert

participants while the feedback guided the study to meet specific goals (Eycott et al., 2011; James & Warren-Forward, 2015).

Transferability

The field of information security and risk management involve specific variances that separate them from experts from other fields of study (Posey et al., 2014). Specific criteria such as exclusive participation of senior managers in with 15 to 20 years of experience in information security and risk management help in strengthening the the research study (Eycott et al., 2011; James & Warren-Forward, 2015). The outcome may provide valuable insights into the essential managerial competencies that enhance managerial abilities in organizing and aligning organizational resources to build a robust information security and risk management system to mitigate risks from cyber attacks and data breaches. The questionnaire was reviewed by my committee chair before conducting the pilot study and Round 1 for data collection from the expert panel. The purpose of the first round of questioning was to gain an understanding of the enterprise level security landscape.

The Delphi technique is useful in analyzing managerial competencies as it improves the reliability of the study (Donohoe et al., 2012; Haynes & Shelton, 2017). The competencies are being evaluated for their effectiveness in a specific field. The field of information security requires high-level expertise that only some employees can attain. The expert participation provides a high level of reliability as their responses are backed with expertise (Landeta, 2006; Linstone & Turoff, 2011; Meijering et al., 2013; Skinner et al., 2015; Strasser, 2017). The consensus that the panel reaches is from the collective

knowledge of multiple high-level industry specialists. Group decisions are more valid and rigorous than individual decisions (Englander, 2016; James & Warren-Forward, 2015; McCusker & Gunaydin, 2015; Singh, 2015). Although the results of the Delphi study may not be relevant to all information security and risk management programs implemented at various organizations, I worked to ensure that the results of the study aligned with existing literature on the organizational risk management and managerial competencies. The results of the study may not be transferable; however, the research process may be transferable to other fields of study.

Dependability

The Delphi technique helped guide decision making with the intention of finding a group consensus on managerial competencies (Posey et al., 2014; Strasser, 2017; von der Gracht, 2012). The level of expertise, number of data collection rounds, and level of consensus were selected before the implementation process to reduce obstacles to achieving valid and reliable results. The anonymous nature of the study promotes honesty from participants (Haynes & Shelton, 2017; James & Warren-Forward, 2015). Honest participants provide valid data. The participant feedback improves answers without influencing participants into giving certain answers (Brady, 2015; Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). The responses from the group provided additional perspectives that could provide depth for analysis (Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017).

Ethical Procedures

The IRB at Walden University oversees the ethical standards of the university by making sure research follows federal and local regulations. Approval was needed to be granted by the IRB for my research study to move forward. The anonymous nature of the study protected participant identities during and after the study. Anonymity was especially important as the research participants will be experts in their fields. Identifiable information was not be included in the communication between the researcher and participants. The study followed the code of ethics set by the American Psychological Association (APA, 2010), which exists to protect the safety of the participants.

Summary

The purpose of this qualitative Delphi study was to explore how the managerial competencies for information security and risk management senior managers can help in managing security objectives and practices to mitigate information security risks. The purpose of this chapter, the literature review, is to analyze, interpret, and synthesize a body of published literature on the phenomenon of managerial competencies and to determine a conceptual framework for my research topic.

Chapter 3 contains details on the research question, research methodologies, and research procedures. The research methodology section included aspects of the Delphi technique and the reasoning for being selected for this research study. The benefits and liabilities detailed so that a holistic view of the Delphi technique could be understood. The research procedure section included the population selection, the process involved in population selection, the data selection process, and the analysis process. The data used

for analysis was collected from the expert panel of information security and risk management experts. The required approval of institutional research methods and ethical guidelines regarding participant safety are included in this chapter. The data collection rounds and limitations for the Delphi study were also described. Chapter 4 includes the responses for three rounds of data collection and subsequent data analysis. The best competencies that increase managerial efficiency in protecting data were determined from the data analysis.

Chapter 4: Results

Chapter 4 contains the results collected from the Delphi panel of experts on competencies essential for managing security objectives for organizational performance with information security management. The purpose of this study was to analyze the panel opinions on the best methods to reduce cyberattacks and prevent data breaches. The participants reviewed the questionnaire through e-mail. The rounds of data collection involved a 5-point Likert scale for evaluating the agreements and importance of various competencies. The group median was shared with panel participants to provide feedback and find a consensus with other participants. With the increase of cyberattacks and data breaches that can significantly affect organizational performance, this study's results may provide information that can reduce cyberattacks and risk from data breaches. I used qualitative questioning based on the literature review to create the first round of questions, which guided the overall study:

1. How effective can organizational leaders and information security managers be when following traditional risk management strategies to recover from the effect of cyberattacks?
2. What managerial competencies are needed to mitigate the risks of cyberattacks? How do these competencies compare to the competencies required to handle traditional organizational risk?
3. What are the managerial competencies that can be found by in a company that is prepared for the effect of cyberattacks compared to the companies that are unprepared for cyberattacks?

4. What are common factors of cyberattacks that could have been prevented with the effective alignment of organizational resources such as people, process, and technology with a cyber security framework focus?
5. What are the types of expertise that should be recruited by companies to build a successful recovery program that can respond to cyberattacks?
6. What advantages or disadvantages exist in defining cyber security risk and controls frameworks?

The questions from Round 1 were focused on the managerial and technical competencies for managing enterprise information security risk management. This chapter includes the pilot study, research setting, demographics, data collection and analysis, evidence of trustworthiness, results, and summary.

Pilot Study

A pilot study was performed to verify the rigor and confirmability of the Delphi study. The pilot study involved four participants who fit the selection criteria provided in Chapter 3. The participants were from different industries and roles. The first participant was a cybersecurity advisor for the financial, insurance, and healthcare sectors. The second expert was an executive member responsible for governance, compliance, and audit sectors. The third expert was an architect responsible for delivering a cloud-based secured e-commerce solution for the retail and banking industries. The fourth expert was a data security expert responsible for protecting electronic patient health information, personally identifiable information, and credit card data.

The pilot study was used to collect feedback from the first round of data collection to ensure that the study was on track and focused. Participants were allowed to make improvements to the research process to strengthen the rigor of the main study. One suggestion of the panel was to improve the initial questions by including the definitions of information security management competencies, security strategy enterprise, and overall strategy alignment. An additional suggestion was to modify the communication methods for between the researcher and participants. Pilot study participants also provided feedback on communication protocols to improve the communication and follow-up e-mails for reminding participants to complete the questionnaire and suggested providing additional details on competencies on new standards and emerging technologies such as IoT, Cloud, artificial intelligence, and social media for managing cybersecurity risk.

Research Setting

Data for this Delphi study were collected electronically. This technique was different from traditional data collection technique of observations and interviews. One advantage of this Delphi technique was that data were reported directly by the study participants. A disadvantage of this technique was that the conditions that the participants were under during the questionnaire were unable to be reported.

The only information collected from the participants was the consent form and data. The Delphi instrument did not require information about the conditions and demographics of the participants. Both of these factors could potentially alter responses.

The expertise of each participant was verified on LinkedIn before the start of the study and thus was not included as a question in the research questionnaire.

Demographics

One hundred and thirteen experts in the field of information security and risk management were contacted for participation in the study. They were identified on LinkedIn and contacted for their potential involvement in the study. Eighteen participants confirmed their participation. The participants managerial and information security experience in managing information security risk was recognized by:

- Expertise in the organizational leadership and risk management strategies.
- Demonstrated managerial competencies and cyber-security, cyber threats, and cyber vulnerability management.
- Expertise in aligning organizational resources for mitigating enterprise cyber risk
- Expertise in IT, applications, data, and infrastructure security and risk management
- Expertise cyber security standards, frameworks, governance, policies, and audit

Panel participants in the fields of information security and risk management were chosen for their involvement within large corporations in the United States. Due to the size of the organizations, employees were given various responsibilities to handle the phases of development, architecture, design, deployment, implementation, and management. The participants were also chosen based on their education, experience, and

expertise. The information found in LinkedIn on each participant was checked to ensure eligibility and contributions to the study. The panel contained multiple participants who were interested in finding effective strategies and competencies to add a value to information security management practice. The summary of participant education and experience profile is shown in Table 3.

Table 3

Participant Demographic Summary

Sr.NO	Information security expertise	Education	Years of experience	Gender
1	Information security, risk management, infrastructure security governance, and strategy	MS	16 Plus	Female
2	Information security, risk management, and application security	BS	16	Female
3	Information security, risk management, governance, strategy, policy, compliance and BCP/DR	PhD	20 Plus	Male
4	Information security, risk management, IAM, data security	BS	16 Plus	Male
5	Information security, risk management, and compliance	MS, CPA	18 Plus	Male
6	Information security, risk management, and operations security	MS, MBA	16 Plus	Male
7	Information security, risk management, strategy, governance, cloud security	MS, MBA	16 Plus	Male
8	Information security, risk management, ERP, compliance	BS	20 Plus	Male
9	Information security, risk management, infrastructure security governance, and strategy	MS	18	Male
10	Information security, risk management, and application security, governance	MS	16	Male
11	Information security, risk management, and compliance	MS	22	Male
12	Information security, risk management, infrastructure security governance, and strategy	MS, MBA	24	Male

Eighteen experts participated in the study, and 12 out of 18 participants finished the first two rounds of data collection. Two of the participants exited the study after the first round was completed. Due to this loss, I invited two additional participants who were able to complete the first two rounds with 12 participants. The participants who turned in their submissions late were sent reminders through e-mail and phone messages to encourage study participation. Participants who had conflicts with the study requirements or lacked the time due to work schedules at work were free to exit the study as mentioned in the consent form.

Data Collection

Recruitment

I created a short list of potential participants on LinkedIn while the IRB approval process was occurring. I set aside 1 month to complete the participation selection. One month was enough time for me to verify the participant information and request interviews for participants that had the necessary experience in managing security objectives for effective organizational performance with information security management. Invitations with information regarding the study along with IRB consent forms were sent to 113 potential participants. Out of the 113, 34 responded, and 18 of those participants agreed to join the research study. These participants fit the selection criteria and were deemed credible for study inclusion. I also selected some additional participants for backup in case other participants were unable to complete the study requirements. Information regarding Delphi study schedule is included in Table 4.

Table 4

Pilot and Delphi Study Schedule

Event	Start Date	End Date
Delphi Round 1	3/3/2019	3/20/2019
Round 1 analysis	3/21/2019	3/30/2019
Delphi Round 2	4/2/2019	4/8/2019
Round 2 analysis	4/9/2019	4/12/2019
Delphi Round 3	4/15/2019	4/19/2019
Round 3 analysis	4/19/2019	4/22/2019

Delphi Round 1

Participants were sent the details and expectations of the study after their completion of the consent forms. All the documents were in Microsoft Word files. All 18 of the participants had areas of expertise that made them useful for participation in the study. The panel was sent the qualitative research questionnaire and given 2 weeks to complete the first round of questions. The participants recorded their answers in the form of Microsoft Word documents. All of the responses were categorized in a Microsoft Excel spreadsheet. Each panel member had their answers provided with a number to keep their identity hidden. The participants answered six questions and sent their responses to me. Based on the responses, I found several recurring statements among responses from participants. Recurring statements or themes were removed to maintain quality and rigor. Total of 111 statements was collected in the Round 1 survey and grouped them based on themes to develop a survey questionnaire for Round 2.

Delphi Round 2

The answers to the open-ended questions of the first round of data collection were used to create Round 2 questions. The second round was centered on competencies that

can influence the information security structure of an organization. A 5-point Likert scale was used for Delphi agreements following the first round of submissions with 5 = *strongly agree* and 1 = *strongly disagree* (Hasson & Keeney, 2011; Haynes, & Shelton, 2017; Mendoza, 2014).

The panel participants used the 5-point Likert scale to evaluate each of the statements. For the statements that scored a 2 or below, participants were asked to expand on their answers to understand the reasoning for the low score. The purpose of this was to understand why they felt certain competencies were unhelpful in managing information security. A score of 3 was the natural benchmark and a score of 4 and over is general agreement by the panel. All of the data from the participants were placed into an Excel spreadsheet. The values for the mean, standard deviation, and percent agreement were calculated based on collected data. The statements with a high value and high level of consensus were used in the third round of questioning. The questions from the second round of data collection are found in Appendix E. The calculation of consensus is a standard deviation below 1.5 and 80% participant agreement (Cleary et al., 2014; Lee-Jen Wu et al., 2014; Morgan, 2008).

Delphi Round 3

During Round 3, four out of 68 statements scored below the consensus standard. Sixty-four statements reached consensus and 81 statements were used to understand the managerial competencies that can improve the efficiency of management. The filtered statements were shown to be inefficient in dealing with information security-related issues. Appendix C contains all of the questions from Round 3.

The participant panel was able to rank the competencies that they found to be important in effective management during Round 3. Sixty-four of the 68 statements reached consensus on essential managerial competencies. The questions from the third round of data collection are found in Appendix F. The Likert scale used for ranking importance judgement was formatted as 5 = *very important* and 1 = *not important*.

Data Analysis

The goal of qualitative research is to observe and record data patterns during the research process (Eycott et al., 2011; McCusker & Gunaydin, 2015). The statements collected from the initial round of data collection were analyzed to create the statements for the second round of the Delphi method. The initial round of questioning displayed a broad idea of the competencies the research panel finds important of management. I analyzed the responses to guide the research study into a consensus among the participants. The open-ended questions of the first round allowed for a more specific look into the competencies and strategies that would be beneficial to management. The data were placed into categories and created into statements for the following rounds of questions. As the responses were collected, the statements were altered to fit the new data received. There were over 111 statements collected from the participant panel. These statements were analyzed and categorized into the 81 statements used for the next round of data collection. The statements used in Round 2 are included in Appendix E.

Guided questions were used in this study to narrow the topic so a consensus was more likely to be found (Heiko, 2012; Hsu & Sandford, 2007; James, & Warren-Forward, 2015). The consensus does not occur in every study as participants may continue to have

differing opinions and it is difficult to obtain. The findings from a study lacking consensus could still help in developing useful conclusions (Gupta & Clarke, 1996; Hsu & Sandford, 2007; James & Warren-Forward, 2015).

Statistical measures including central tendency and standard deviation were used to calculate the level of consensus among participants (Cleary et al., 2014; Lee-Jen Wu et al., 2014; Morgan, 2008). The inter-quartile range is commonly used by researchers to determine the consensus (Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). Most Delphi studies use statistical analysis when determining the median, range, and standard deviations of data (Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). The standard deviations and mean values are important elements for determining whether a consensus has occurred (Linstone & Turoff, 2011; von der Gracht, 2012). The mean, standard deviation, majority agreement, and ranges were used to determine the final outcome for this research study (Cleary et al., 2014; Lee-Jen Wu et al., 2014; Morgan, 2008). Statements with the least amount of resistance are the end goal of this study (Eycott et al., 2011; Gupta & Clarke, 1996).

The consensus was determined by the standard deviation, mean, participant agreement of 80% and interquartile scores (Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). The value of 3.9 was determined to be the baseline of participation agreement. The measurements used for determining consensus are:

- An 80% agreement from the participants was taken in to consideration.
- An interquartile range below 2.5 was taken for measuring consensus for each statement (Cleary et al., 2014; Lee-Jen Wu et al., 2014; Morgan, 2008).

- A standard deviation below 1.5 was recorded (Cleary et al., 2014; Lee-Jen Wu et al., 2014; Morgan, 2008).
- A mean score of greater than 3.9 was taken for measuring consensus for each statement

The statements that were given a value below 4 were removed from the questionnaire of the following round. The third round of data involved the participant panel evaluating the remaining competency statements and attempting to find the factors and statements with the highest amount of consensus. The statements that had over 80% participant consensus or over 3.9 points on the Likert scale are determined to have reached consensus (Linstone & Turoff, 2011; von der Gracht, 2012).

Evidence of Trustworthiness

Credibility

Rigor is an essential component of research studies as it strengthens the credibility of research methodologies (Haynes & Shelton, 2017; James & Warren-Forward, 2015). Researchers who value integrity, credibility, and methodology have the goal of reliable data (Cleary et al., 2014; James & Warren-Forward, 2015; Lee-Jen Wu et al., 2014; Strasser, 2017). Verification of data is another critical element in research as it backs up the validity of data and research conclusions. Improvements should be made to the data collection and verification procedures if the researcher has doubts about the quality of data collection (Skinner et al., 2015; Strasser, 2017). To ensure the credibility of my study and to address the disadvantages of the Delphi method, I set up a pilot study to test the Delphi process. I also reviewed and refined seed questions developed for Rounds 1, 2

and 3 with the committee. During my role as a researcher, I maintained the confidentiality and professionalism of our participants while communicating with participants during the recruitment phase, data collection phase, analysis phase, and reporting phase.

The Delphi technique has a unique approach to test the rigor of research studies by using the goodness criteria (de Loë et al., 2016; Mendoza, 2014). Data were collected from three rounds of questioning. The ultimate goal of the questioning process was to come to a consensus and guide the direction of the research study (Eycott et al., 2011; James & Warren-Forward, 2015). The panel was comprised of experts in different areas of the information security field to ensure a wide variety of opinions on the subject of managerial competencies. (Posey et al., 2014; Strasser, 2017). The result of the research study stated that there were specific managerial competencies were essential to managing security objectives for effective organizational performance with information security management practices. After each round was completed, panel participants had the option to include additional competencies they feel would help to manage security objectives for effective organizational performance with information security management. The data was analyzed, and feedback was generated for subsequent rounds of data collection.

Transferability

The fields of information security and risk management have nuances that separate them from other fields of business (Posey et al., 2014). The specific details may help find the managerial competencies that will enhance managerial abilities in organizing and aligning organizational resources to create an adequate information

security and risk management system to mitigate the risks from cyberattacks and data breaches.

Information security is a field that requires high-level expertise. The expertise was helpful on the expert participant panel as the goal from data collection is finding a consensus between participants. (Landeta, 2006; Linstone & Turoff, 2011; Meijering et al., 2013; Skinner et al., 2015; Strasser, 2017). The group consensus on the managerial competencies is more important than the opinions of an individual expert (Englander, 2016; James & Warren-Forward, 2015; McCusker & Gunaydin, 2015; Singh, 2015).

My role in the pilot and Delphi studies was to select the expert participants, restructure research questions based on feedback, and to maintain consistent communication with the participants. Researchers have often used pilot studies to determine the transferability of the Delphi method (Clibbens et al., 2012). Using a pilot exercise for the first round of questioning helps to increase the transferability of the Delphi method (Clibbens et al., 2012). The pilot study included a small panel of information security experts that validated the research instruments. The small size of the participant pool creates low transferability of the study. Thus, the results of the study may not be transferable given the small sample size and the sampling technique; however, the research process may be transferable to other fields of study.

Dependability

The expertise of participants, the anonymity of participants, the number of data collection rounds, consensus level, and processes are essential factors when conducting a research study. (Haynes & Shelton, 2017; James & Warren-Forward, 2015). Participants

with a high level of expertise will provide valuable data (Brady, 2015; Haynes & Shelton, 2017; Skinner et al., 2015; Strasser, 2017). There were three rounds of data collection for my study to achieve the 80% consensus among 12 participating experts on managerial competencies to mitigate organizational cybersecurity risk from cyberattacks.

The sample size of my research study comprised of experts in the field of information security. These participants have experience in the information security management field of mitigating risks from cyber attacks and breaches. The limitations of the study were that the participant criteria for a specific field of study make for a small participant pool. Various experts of the industry who come from different countries may have a different consensus on the topic of managerial competencies. (Linstone & Turoff, 2011).

Confirmability

An advantage of the Delphi technique was that the data is collected from the participants instead of the researcher who helps to decrease the chance of researcher bias. Collecting data this way helps reduce any pressure that the participants can feel from the researcher (Haynes & Shelton, 2017; James & Warren-Forward, 2015).

The confirmability could be found in a Delphi study by the calculation of group statistical summaries of the judgments, pilot testing, audit trail, methodical process, and electronic survey (Linstone & Turoff, 1975; Okoli & Pawlowski, 2004; Skulmoski et al.,2007). I have maintained all the audit trails retained, recorded all questions, responses, feedback, calculations, and coding for each round. The initial six seed questions were clearly defined with the alignment from the review of the literature in Chapter 2. The

expert participation provides a high level of reliability as their responses are backed with expertise (Landeta, 2006; Linstone & Turoff, 2011; Meijering et al., 2013; Skinner et al., 2015; Strasser, 2017).

One issue during research studies is the interference of researcher bias. Biases obscure the data collected which leads to unverified analysis and conclusions. It is important to reflect after every round of data collection to ensure the validity of results (Marshall, & Rossman, 2011; Mendoza, 2014). Allowing the participants to view the data helped to decrease biases during the research process (Rowe, & Wright, 1999; Thomas, & Magilvy, 2011; von der Gracht, 2012). Participants were able to alter their responses based on feedback from other panel participants. The goal for the result was a consensus on the best managerial competencies. The researcher must create research studies that reduce the potential of bias (Haynes & Shelton, 2017; James & Warren-Forward, 2015). I addressed the weakness of my research study by asking my committee to review my questions and pilot study.

Study Results

The purpose of this qualitative Delphi study was to explore the critical managerial competencies that senior managers need to align and integrate organizational resources such as people, process, and technology to manage information security and risk to prevent cyberattacks

Round 1

A total of 111 statements were collected from the participant panel during Round 1. The collected statements fell into six significant categories related to skills and

competencies needed for managing security objectives for effective organizational performance with information security management were:

1. Risk management strategies to recover from the effect of cyberattacks
2. Managerial competencies needed to mitigate the risks of cyberattacks
3. Type of managerial competencies that can be found by in a company that is prepared for the effect of cyberattacks, compared to the companies that are unprepared for cyberattacks
4. Common factors of cyberattacks that could have been prevented with the effective alignment of organizational resources such as people, process, and technology
5. Skills and expertise required to build a successful recovery program that can respond to cyberattacks
6. Impact of security frameworks

Round 2 questions were created based on the data that were collected and coded from Round 1. The recurring answers were turned into statements for further questioning. The Round 1 coding activity produced 81 themes that were used in the development of the Round 2 instrument 81 statements and reviewed with the committee before emailing it to all 12 participants for Delphi agreements. During Round 1, participants provided their responses in paragraphs with multiple statements; I had to reach out to many participants for clarifications to understand their intention to qualify each statement to validate before qualifying it for Round 2. The categorization list for the themed statements collected in Round 1 are listed in Table 5.

Table 5

Categorization List for Statements Collected in Round 1

No	Category	Number of Statements
1	Risk management strategies to recover from the effect of cyberattacks	22
2	Managerial competencies needed to mitigate the risks of cyberattacks	23
3	Type of managerial competencies that can be found by in a company that is prepared for the effect of cyberattacks, compared to the companies that are unprepared for cyberattacks	20
4	Common factors of cyberattacks that could have been prevented with the effective alignment of organizational resources such as people, process, and technology	15
5	Skills and expertise required to build a successful recovery program that can respond to cyberattacks	15
6	Impact of security frameworks	16

The 111 collected statements were put into an Excel spreadsheet and categorized by managerial competency. The collected themes are coded and listed in Table 6.

Table 6

Codes Collected from Round 1 Seed Questions

Sr.No	Code/Theme	Frequency
1	Risk Management	25
2	Competencies	21
3	Organizational Risk	11
4	Organizational Resources	10
5	Organizational Alignment	12
6	Regulatory Standards and Security Frameworks	25
7	Recovery from Cyber Security incident	33
8	Risk Mitigation	13
9	Regulations	6
10	New Technology	11
11	Domain Expertise	16
12	Security Controls	17
13	Training	8
14	Management Support	12
15	Security Policies	16

16	Security and Privacy	32
17	Awareness	11
18	Security Certifications	4

The collected data were grouped into 111 statements based on the answers obtained from the first round of data collection. The statements included in the first round were placed into groups of risk management strategies and security architecture, managerial and technical skills and competencies needed to mitigate the risks of cyberattacks, common factors for cyberattacks, alignment of organizational resources such as skilled people, well defined regulatory standards, security frameworks, matured processes, and technologies.

Round 2

The Round 1 data collection included 111 statements from the six open-ended questions. The 111 statements were analyzed and themed into 81 statements relating to the seed questions and fine-tuned for Round 2 survey. Appendix E contains the complete list of Round 2 questions sent to the participant panel. I did receive queries on eight statements from four participants on people and technology competencies.

Of the 81 statements sent to the participants, consensus was found on 77 statements in Round 2 survey. Questions 2 and 3 recorded two statements each lacking the criteria needed for consensus. The summary of consensus reached in Round 2 is listed in Table 7. The details of consensus and supporting statistical analysis is listed in Table 8. For each themed statement surveyed in Round 2 for measuring agreement judgement using the 5-point Likert scale.

Table 7

Round 1 Analysis: Themed Statements and Consensus Reached

Seed Question	Themed Statements	Consensus Reached
Q1	14	12
Q2	16	14
Q3	13	13
Q4	12	12
Q5	11	11
Q6	15	15

Table 8

Round 2: Participant Consensus on Round 2 Agreements

Statement	Question 1: How effective can organizational leaders and information security managers be when following traditional risk management strategies to recover from the effect of cyberattacks?	Mean	*SD*	%
1	Traditional risk management strategies & plans need to be updated to account for the changing technical and business environment.	4.83	0.39	97%
2	The risk impact can be managed efficiently, and recovery can begin with minimal impact on organization. If organizational leadership follows the strategy, standards, right policies, plans, and procedures according to the plan before and after an attack,	4.33	0.78	87%
3	The traditional risk management strategies used by organizational leaders and information security managers can be quite effective, if matured and tested risk management program would have already considered to mitigate risk if ever a cyberattack occurs	4.25	0.87	85%
4	Traditional Risk Management methods alone will not be effective if the leaders and security managers are following tradition risk management strategies to recover from the effects of Cyberattacks.	4.42	0.67	88%
5	Organizations need to conduct continuous monitoring and risk assessments and implement required security controls to address security threats and vulnerabilities.	5.00	0.00	100%
6	Organizational leaders, information stewards and security managers must adapt to tools and processes that will better equip the team, so they can stay ahead of the curve in the whole spectrum of threat and risk management.	4.67	0.65	93%
7	With increased vulnerability from all directions, leaders must have people, processes and technologies in place to proactively monitor, identify, diagnose, fix, and prevent cyberattacks.	4.83	0.39	97%
8	Traditional risk management strategies does not always address “cyberattacks” or “cyber security” and Leadership should continuously update their Risk Management strategy to address emerging cyber risks from new and emerging business processes and technologies	4.67	0.65	93%
9	Traditional risk management strategies may not be effective in the digital age due to the increased use of Open source code and the Cloud to develop/host applications/services containing sensitive data	3.92	0.67	78%
10	The principles of Information Security remain the same regardless of the change in technology. However, the speed, agility and complexity which has increased due to emerging technologies such as Cloud, IoT, Blockchain, self-driving cars, industrial automation, Blockchain/Cryptocurrency, Smart cities, etc.	4.58	0.67	92%
11	Need a major transformation in terms of security regulations, standards, policies, procedures, controls, and monitoring to address risks from emerging technologies	4.33	0.89	87%
12	Organizations need to embrace automation, AI, and analytics in order to be successful in prevention, detection and recovering from Cyber Attacks.	4.58	0.67	92%
13	Traditional risk management strategies will need to be tailored to address the dynamically changing threat and regulatory landscape	4.67	0.49	93%
14	Traditional risk management strategies are no longer effective in today’s dynamic ecosystems and landscapes with emerging cloud based infrastructure and technologies.	3.67	1.07	73%

(table continues)

Statement	Question 2: What managerial competencies are needed to mitigate the risks of cyberattacks? How do these competencies compare to the competencies required to handle traditional organizational risk?	Mean	*SD*	%
1	Equanimity in the face of a crisis, emotional intelligence, detail orientedness, intimate awareness of company's IT landscape and technologies, leadership qualities, and resourcefulness are needed as competencies.	4.25	0.62	85%
2	Deep understanding of business processes, digital assets such as applications, data, infrastructure, and people who support them and their potential vulnerabilities	4.58	0.51	92%
3	The ability to monitor and assess what is happening in the cybersecurity and cyber-threat world is essential due to the increase of technology. Mapping them to one's organization's risk processes and determining the gaps on a timely basis will be a best practice.	4.67	0.49	93%
4	As a manager, hacks are inevitable with the increased number of digital services. One has to manage the team and allow them to employ out of the box ideas to identify the new emerging threats and come up with innovative deterrent measures.	4.58	0.67	92%
5	Educate and train his/her teams and non-technical stakeholders on the risk management lifecycle and processes	4.67	0.49	93%
6	Competency includes the understanding of risk management programs within the organization and an understanding of risk mitigation options relevant to the respective area of responsibilities.	4.25	0.62	85%
7	Currently, organizations have not made cyber-centric competency a priority.	3.33	0.78	67%
8	Executive management, senior, and middle management should include cyber-security and risk management focused leadership competencies in their leadership to mitigate emerging cyber risks.	4.67	0.49	93%
9	Management should have an open and agile mindset to be able to adopt the effective ways of mitigating the risks of cyberattacks.	4.75	0.45	95%
10	Context setting, alignment at the leadership level for priorities, good program management, time management, and conflict resolution are all important for any risk management program	4.67	0.49	93%
11	Communication is an important, technical expertise goes a long way in helping the team to mitigate risks.	4.75	0.45	95%
12	Suddenly there has been a major transformation to cloud based systems, IoT adoption, mobility, etc. which have almost made traditional security controls ineffective.	3.58	0.67	72%
13	There is a necessity for modern leaders to help securely adopt emerging technology, understand the evolving regulatory landscape, and increase cross border transfers.	4.58	0.51	92%
14	Risk management methodology/frameworks need to be re-aligned with new threat landscape which did not exist in traditional environments.	4.58	0.51	92%
15	For an effective security management, there must be balance between emerging technologies, understanding the management and financial planning requirements, and understanding the big picture of how a new technology based eco-system will function.	4.67	0.49	93%
16	Mitigation of cyberattack risks requires a broader range of managerial competencies that traditional organizational risk due to the complexity of technologies involved. A management team of technical representation, financial and business representation is required. In traditional organizational risk, the technical representation is not likely needed.	4.25	0.62	85%

(table continues)

Statement	Question 3: What are the managerial competencies that can be found by in a company that is prepared for the effect of cyberattacks, compared to the companies that are unprepared for cyberattacks?	Mean	*SD*	%
1	Managers must have competencies such as superior communication, problem solving, teamwork, capability to define and implement processes, and the maturity to mentor and motivate the team to achieve individual, team and organizational goals.	4.58	0.51	92%
2	Leadership should demonstrate open mindedness, lack of bias, and maturity to provide and implement risk mitigation plans.	4.75	0.45	95%
3	Cybersecurity managers must have well-tested standards, frameworks, and industry best practices in place to address the known and emerging vulnerabilities in order to protect the organization from cyber threats and risk.	4.75	0.45	95%
4	Transparency amongst the management in handling cyberattacks is essential.	4.50	0.52	90%
5	Proper understanding of the risk management program within the organization is important when dealing with the impact of threats on a business.	4.58	0.51	92%
6	Managers should be required to have a proper understanding of risk management program within the organization.	4.50	0.52	90%
7	A well prepared leadership will have managerial competencies that place a priority on identifying threats. Such management also puts their organization's mission critical information and data security as their top most priority and will align their IT spending with the right objectives.	4.67	0.49	93%
8	A well trained and experienced leadership will have a robust disaster recovery plan and business continuity plan in place and will diligently conduct simulation drills throughout the organization to carry out the recovery tasks in case an incident occurs.	4.75	0.45	95%
9	An unprepared organization or leadership on the other hand will be unaware of the complex and changing threat landscape and may not have the right people, processes or technologies in place in the event of a cyberattack.	4.75	0.45	95%
10	Mangers must have an overall view of the organization assets, policies, and procedures. Managers also need to have a comprehensive "security policy" which has all the threat vectors considered.	4.58	0.51	92%
11	The most important security element is effective communication with C-Suite to ensure enough resources are allocated for cybersecurity resilience.	4.67	0.49	93%
12	Being aware of security protocols will ensure behaviors that protect the data of a company.	4.58	0.51	92%
13	A technical background is required to be able to make decisions and communicate to C level executives and external regulators	4.42	0.67	88%
Statement	Question 4: What are common factors of cyberattacks that could have been prevented with the effective alignment of organizational resources such as people, process, and technology with a cyber security framework focus?	Mean	*SD*	%
1	The surprise element of the cyberattack can be a major threat to the company in terms of direct and indirect consequences.	4.58	0.51	92%
2	The impact of a surprise attack can be addressed by proactively building well trained incident response team to reduce the detection, recovery, and mitigation	4.58	0.51	92%
3	The right governance structure consists of a core group with responsibilities for strategy, design and implementation of cybersecurity programs and policies.	4.58	0.51	92%

(table continues)

Statement	Question 4: What are common factors of cyberattacks that could have been prevented with the effective alignment of organizational resources such as people, process, and technology with a cyber security framework focus?	Mean	*SD*	%
4	The effective use of processes and training programs – the company must introduce strong training programs that ensure team members are aware of the company's business processes, infrastructure, and critical digital assets, as well as cybersecurity vulnerabilities, threats, risks, and necessary controls for risk mitigation.	4.75	0.45	95%
5	Having the right group of resources in various teams with required expertise and clear roles and responsibilities, industry recognized cybersecurity frameworks, regulatory standards, well-defined processes with global best practices and periodic review of processes as part of risk management and standardized adoption of technologies and technical solutions within the company can help mitigate threats.	4.58	0.51	92%
6	Lack of coordination and senior leadership support, weak access controls, lack of encryption for sensitive data, non-application of patches, insecure remote communication, ineffective recovery processes, poor user security awareness, lack of layered defense approach are known common factors responsible for cyberattacks on any organization	4.75	0.45	95%
7	With the effective alignment of organizational resources such as people, process, and technology with a cyber security framework focus, an effective information security awareness and training, strong governance measures to define, implement and manage policies and processes, properly architected, implemented and managed technology infrastructure would be key to avoid cyberattacks.	4.58	0.51	92%
8	Social Engineering attack, Social media attack and Malware attacks must have specialized security controls.	4.58	0.51	92%
9	Cyberattacks that are triggered through phishing, denial-of-service (DOS), general virus/malware and other modes can be prevented with having the right controls in place. In general, human factor, compliance and policy related aspects, external/cloud, bring your own device related factors can be effectively prevented with a well devised and implemented cyber security framework.	4.58	0.51	92%
10	Cyberattacks can be internal or external. A process must be kept in place to stop the attacks or prevent it. The manager needs to make sure the team follows process and has the required ongoing training to stay current in trends of technology, attacks and tools	4.67	0.49	93%
11	Lack of Security Awareness and enablement of organizational users to acknowledge security as a shared responsibility, Not defining KPI's which help in measurement of Security control effectiveness, insufficient allocation of security controls and define process for prevention, detection and response to cyberattacks, failure to identify alternate mechanism how business can continue during response/recovery of cyber security attacks.	4.42	0.67	88%
12	If more effective alignment existed across the organization, common factors of cyberattacks could be reduced. Some of these negative factors include: Not prioritizing and allocating required resources to security projects	4.17	0.72	83%

(table continues)

Statement	Question 5: What are the types of expertise that should be recruited by companies to build a successful recovery program that can respond to cyberattacks?	Mean	*SD*	%
1	The best qualities of a successful candidate include being a team player, being detail oriented, having security domain expertise, and programming expertise.	4.33	0.65	87%
2	It all starts with recruiting the right people who are competitive and have the right background in the industry. This involves relevant security certifications, experience in effectively implementing mitigation plans, experience in effectively handling a cyberattack, and the ability to develop short term and long term plans to address the attack.	4.50	0.67	90%
3	Teams comprising of employees with competent expertise will always play a pivotal role during any crisis. Employees with clearly defined roles and responsibilities will ensure an effective tandem at work during crisis.	4.58	0.51	92%
4	Crisis Managers/Incident Handling Managers/BCP & DR Managers must have competencies such Network and IT infrastructure, Cloud, Enterprise Architects and Application architecture, Security infrastructure, IAM, Log analysis, Forensic, and leadership and communication to mitigate the risk from cyberattacks.	4.33	0.65	87%
5	The types of expertise that should be recruited by companies to build a successful recovery program would include risk management, business continuity and disaster recovery, cyber security assessment, regulatory compliance and cyber security frameworks, system security architecting, implementation, management and monitoring, system security vulnerabilities testing, and governance, risk and compliance	4.58	0.51	92%
6	Solid understanding of IT fundamentals, sufficient coding skills, understanding of architecture, administration and operating system are required from candidates.	4.17	0.72	83%
7	For a successful recovery program, one must recruit people with expertise covering business continuity planning, behavioral change management, malware detection, IT forensics, risk analysis and mitigation, threat modeling, and Cloud security.	4.42	0.67	88%
8	Security Operations Center SMEs who can do Threat Hunting, Incident response, Forensic analysis, Threat Intelligence are essential to the performance of a company.	4.33	0.78	87%
9	Skilled employees should have the right certifications in security, coding skills, architecture and operational expertise, and excellent oral and written skills.	4.17	0.58	83%
10	Investment in domain specialization for the core team which includes incident response, network security, etc, and Ethical Hackers. All these roles can handle different aspects of security issues.	4.75	0.45	95%
11	Unfortunately a recovery program often results in a loss of data. Management should include technical knowledge and effective communication in their response to crisis.	4.33	0.65	87%
Statement	Question 6: What advantages or disadvantages exist in defining cyber security risk and controls frameworks?	Mean	*SD*	%
1	Frameworks keep everybody on the same page as they comprehensively cover all aspects of the cyber security risks.	4.58	0.51	92%
2	Various frameworks are in practice to guide the industry. Frameworks help to understand systems and recognize risks in order to adopt the customized risk management methodologies to minimize the risk for a better ROI and measureable effectiveness.	4.83	0.39	97%
3	Frameworks are guiding practices, their intentions vary from country to country, industry to industry, one should not blindly follow them.	4.83	0.58	97%

(table continues)

Statement	Question 6: What advantages or disadvantages exist in defining cyber security risk and controls frameworks?	Mean	*SD*	%
4	Identification of risks in a timely manner per type of asset and their classification. assist in risk assessment, useful for risk mitigation and deriving residual risk, real time risk monitoring and reporting	4.67	0.49	93%
5	A traditional approach may slow down countermeasures against sophisticated APT's and socially engineered attacks.	4.08	0.79	82%
6	Cyber security frameworks provide organizations with an opportunity to identify areas where existing processes may be strengthened, or where new processes can be implemented.· Frameworks would help to guide key decision points about risk management activities through the various levels of an organization from senior executives, to business and process level, and implementation and operations as well. Frameworks help to align with various regulatory compliance requirements	4.67	0.49	93%
7	Lack of resources to manage the framework implementation and maintenance would cause a disadvantage for the system.	4.33	0.65	87%
8	The cyber-security framework should include the core functions to identify, protect, detect, respond and recover. It has to be a comprehensive framework that will enable organization to meet the security challenges faced today.	4.58	0.51	92%
9	The advantages of having a well-defined cyber security risk and controls framework is that it equates to one's ability to proactively monitor threats and recover attacks in a seamless and effective manner, thus minimizing the overall business loss.	4.75	0.45	95%
10	Frameworks provide great advantages. One big disadvantage is they may be too broad for an organization & costly to implement verbatim. So we may need to modify the framework to suite our needs..	4.67	0.49	93%
11	Using controls framework help organizations to be clear in what cyber security risks they are trying to prevent and help ensure everyone within the organization is on the same page to jointly identify, prevent, detect, respond and recover from cyber security incidents and associated risks	4.75	0.45	95%
12	There are more advantages than disadvantages to having cyber security risk and control framework in place Frameworks help the organization to have controls in place to stop attacks and provides management a sense of security both internally and externally.	4.58	0.51	92%
13	Cyber Security Frameworks allow for structured implementation of controls and allow to comprehensively cover all aspects of the cyber security risks. Align with industry best practices which clients/partners can be assured of having verifiable minimum security controls in place.	4.67	0.49	93%
14	However frameworks have certain disadvantages. Efficiency of frameworks depends on how an organization has interpreted security controls and if there is room for flexibility to enhance controls for any modernization/transformation initiatives. Any rigidity can hinder innovation, maturity and adoption of emerging technologies.	4.67	0.49	93%
15	The advantages are in discussing, documenting and defining frameworks. If more material exists, if more scenarios are reviewed and documented, there will be a greater awareness to cyber security risks and controls.	4.75	0.45	95%

Round 3

During Round 3, four out of 68 statements scored below the consensus standard. 64 statements reached consensus and 68 statements were used to understand the managerial competencies that can improve the efficiency of management. Appendix F contains all of the questions from Round 3.

The participant panel was able to rank the competencies that they found to be important in effective management during Round 3. A total of 64 of the 68 statements reached consensus on useful managerial competencies. The details of consensus and supporting statistical analysis are listed in Table 11 for each themed statement surveyed in Round 3 for measuring importance judgement using the 5-point Likert scale.

Table 9

Round 3: Participant Consensus on Importance Judgment

Statement	Question 1: How effective can organizational leaders and information security managers be when following traditional risk management strategies to recover from the effect of cyberattacks?	Mean	*SD*	%
1	The enterprise cyber risk can be minimized if organizational leaders follow the strategy, standards, policies, plans, and procedures according to the information security management plan before and after an attack.	4.8	0.4	97%
2	Organizations need to conduct continuous monitoring and risk assessments and implement required security controls to address cyber threats, vulnerabilities, and cyber risks.	4.8	0.4	97%
3	Organizational leaders and security managers must adapt to tools and processes that will better equip the team, such that they can stay ahead of the issues in cyber threats, vulnerabilities, and cyber risks.	4.7	0.7	93%
4	With increased cyber threats, vulnerabilities, and cyber risks, leaders must have people, processes and technologies in place to proactively monitor, identify, diagnose, fix, and prevent cyberattacks.	4.8	0.5	95%
5	Leadership should frequently update their risk management strategy to address current and emerging cyber threats, vulnerabilities, and cyber risks.	4.7	0.5	93%
6	The principles of information security remain the same regardless of the change in technology. However, the speed and agility must increase to address persistent threats from emerging technologies such as Cloud, IoT, Blockchain, self-driving cars, industrial automation, Blockchain/Cryptocurrency, Smart cities, etc.	4.2	0.8	83%
7	Organizations need to embrace new technologies such as automation, artificial intelligence, and analytics to be successful in the prevention, detection, and recovery from cyberattacks.	4.3	0.9	85%
8	Risk management strategies must be tailored to address the dynamically changing cyber threats, vulnerabilities, and cyber risks.	4.6	0.5	92%
Statement	Question 2: What managerial competencies are needed to mitigate the risks of cyberattacks?	Mean	*SD*	%
1	Leaders need to have emotional intelligence to handle crisis situations regarding cyberattacks.	3.9	1.1	78%
2	Leaders must have an understanding of the organization related regulatory standards and requirements to support cyber risk management efforts with required resources such as people, process, and technology.	4.7	0.5	93%
3	The ability to monitor and assess what is happening in the cybersecurity is essential due to the increased use of technology.	4.3	0.6	85%
4	To bring awareness, leaders must support internal training and awareness programs on current and emerging cyber threats, vulnerabilities, and cyber risks to all employees.	4.5	0.7	90%
5	Cybersecurity competency includes the understanding of cyber risk management programs within the organization and an understanding of cyber risk mitigation options relevant to the respective area of responsibilities.	4.3	0.7	87%
6	Executive management, senior, and middle management should include cybersecurity and risk management focused leadership competencies in their leadership to mitigate current and emerging cyber threats, vulnerabilities, and cyber risks.	4.1	1.0	82%
7	Management needs to be able to adopt effective ways of mitigating the risks of cyberattacks.	4.4	0.8	88%

(table continues)

Statement	Question 2: What managerial competencies are needed to mitigate the risks of cyberattacks?	Mean	*SD*	%
8	Communication is an essential skill for leaders to understand and convey current and emerging cyber threats, vulnerabilities, and cyber risks to stakeholders.	4.8	0.4	97%
9	Leaders need to adopt emerging technologies and understand the evolving regulatory policies to manage current and emerging cyber threats, vulnerabilities, and cyber risks.	4.4	0.7	88%
10	Risk management frameworks need to be re-aligned with the current and emerging vulnerabilities, cyber threats, and cyber risks	4.7	0.5	93%
11	For effective security management of risk from emerging technologies, there must be a process for evaluating and assessing risk from emerging technologies and risk mitigation controls.	4.5	0.5	90%
12	Leaders must have an understanding of the organization's IT infrastructure, applications, systems, and data of the organization to support cyber risk management efforts with required resources.	4.6	0.7	92%
Statement	Question 3: What are the managerial competencies that can be found in a company that is prepared for the effect of cyberattacks, compared to the companies that are unprepared for cyberattacks?	Mean	*SD*	%
1	Managers must have competencies such as effective communication, problem solving, teamwork, capability to define and implement processes, and the maturity to mentor and motivate individuals and teams to achieve organizational goals.	4.3	0.8	85%
2	Cybersecurity managers must have relevant experience on industry specific regulatory and information security standards, frameworks, and industry best practices in place to address the current and emerging cyber threats, vulnerabilities, and cyber risks.	4.3	0.6	85%
3	Proper understanding of risk management programs within the organization is important when addressing the effects of current and emerging cyber threats, vulnerabilities, and cyber risks.	4.5	0.5	90%
4	A well-prepared leadership will have managerial competencies that place a priority on identifying current and emerging cyber threats, vulnerabilities, and cyber risks. Such management also puts their organization's mission critical information and data security as their top most priority and will align their IT spending to meet organization objectives.	4.6	0.5	92%
5	A well trained and experienced leadership will have a tested and verified recovery plan in place in case of a cyberattack	4.3	0.8	85%
6	Managers must have an overall view of the organization, people, process, and technology to manage current and emerging vulnerabilities, cyber threats, and cyber risks to an acceptable level in the organization	4.4	0.7	88%
7	The most important security element is effective communication with senior leadership to ensure enough resources are allocated for addressing current and emerging cyber threats, vulnerabilities, and cyber risks.	4.8	0.5	95%
8	The cybersecurity background and knowledge of senior leaders will help the organization to make decisions, implement required security controls and communicate with stakeholders.	3.8	1.0	75%
9	The most important and critical success factor in cybersecurity management is the effective communication with senior leadership to ensure enough resources are allocated for cybersecurity management programs.	4.7	0.5	93%

(table continues)

Statement	Question 4: What are common factors of cyberattacks that could have been prevented with the effective alignment of organizational resources such as people, process, and technology with a cyber security framework focus?	Mean	*SD*	%
1	The effects of a surprise attack can be addressed by proactively building well-trained incident response teams to identify, protect, detect, respond, and recover from cyberattacks	4.4	0.5	88%
2	The right governance structure should be in place with a core group with responsibilities for strategy, design, and implementation of cybersecurity programs.	4.3	0.7	87%
3	Leaders must introduce strong training programs that ensure cybersecurity management team members are aware of the company's people, processes, and technology.	4.5	0.5	90%
4	Having the right group of resources in various teams with the required expertise and clear roles and responsibilities, within the company can help to mitigate current and emerging cyber threats, vulnerabilities, and cyber risks.	4.4	0.5	88%
5	Having the industry recognized cybersecurity frameworks, regulatory standards, and policies within the company can help mitigate current and emerging cyber threats, vulnerabilities, and cyber risks.	4.3	0.5	87%
6	Senior leadership support is a well-known known factor for mitigating risk from cyberattacks.	4.4	0.7	88%
7	Coordination between various teams responsible for cybersecurity, strong security controls, and encryption for sensitive data are known factors for mitigating risk from cyberattacks.	4.6	0.7	92%
8	Application of security patches, secure remote communication, effective recovery processes, and user security awareness are known factors for mitigating risk from cyberattacks.	4.8	0.4	97%
9	A defense in-depth approach is a known strategy for mitigating cyber risks from cyberattacks.	4.7	0.5	93%
10	The effective alignment of organizational resources such as people, process, and technology with a cybersecurity framework focus are essential in mitigating cyber risks from cyberattacks.	4.4	0.5	88%
11	Social engineering, social media, and malware attacks must be addressed by enforcing training and awareness programs, along with specialized security controls.	4.4	0.7	88%
12	Cyberattacks that are triggered through phishing, denial-of-service (DOS), general virus/malware and other modes can be prevented by having the right security controls in place.	4.4	0.7	88%
13	Cyberattacks can be internal or external. A process must be kept in place to mitigate or prevent cyberattacks.	4.8	0.5	95%
14	Leaders need to make sure the team follows established processes and has the required training to stay current on trends in technology and cybersecurity.	4.6	0.7	92%
15	It is the shared responsibility of leadership, employees, and business partners to build security awareness and implement security protocols.	4.6	0.5	92%
16	Common factors of cyberattacks could be reduced by effective alignment of resources such as people, process, and technology.	4.5	0.5	90%

(table continues)

Statement	Question 5: What are the types of expertise that are needed by companies to build a successful recovery program that can respond to cyberattacks?	Mean	*SD*	%
1	The best qualities of a successful candidate include being a team player, being detail oriented, having security domain expertise, and having programming expertise.	4.3	0.6	85%
2	Cybersecurity starts with recruiting the right people who have the right background in the industry to develop short term and long term plans to address current and emerging cyber threats, vulnerabilities, and cyber risks.	4.3	0.5	87%
3	The relevant security certifications, experience in effectively implementing mitigation plans, experience in effectively handling a cyberattack, and the ability to develop short term and long term plans to address the cyberattack.	4.1	0.8	82%
4	Teams comprising of employees with cyber security expertise will always play a pivotal role during and after cyberattacks.	4.4	0.5	88%
5	Crisis managers/incident handling managers/BCP & DR managers must have a resources with competencies such as IT infrastructure, cloud, enterprise architecture, application architecture, security infrastructure, IAM, log analysis, forensic, and leadership and communication to mitigate the risk from cyberattacks.	4.4	0.7	88%
6	The types of needed expertise to build a successful recovery program include: risk management, business continuity and disaster recovery,·cybersecurity assessment, regulatory compliance and cybersecurity frameworks, system security architecting, implementation, management and monitoring,·system security vulnerabilities testing, governance, risk and compliance	4.3	0.8	87%
7	Solid understanding of IT fundamentals, computer programming skills, understanding of data architecture, system administration are required from candidates.	4.1	0.7	82%
8	For a successful recovery program, leaders must recruit people with expertise covering business continuity planning, change management, malware detection, IT forensics, risk analysis and mitigation, threat modeling, and cloud security.	4.3	0.5	85%
9	Security operations center SMEs that can do threat hunting, incident response, forensic analysis, and threat intelligence are essential to the operation and business continuity of a company.	4.3	0.7	87%
10	Skilled employees should have the right certifications in security, coding skills, architecture and operational expertise, and excellent oral and written skills.	3.9	0.8	78%
11	Investment in domain specialization for the core team should include incident response, network security, and ethical hackers. All of these roles can handle different aspects of security issues.	4.3	0.7	87%
12	Management competencies should include technical knowledge and effective communication in their response to crisis.	4.4	0.8	88%

(table continues)

Statement	Question 6: What advantages or disadvantages exist in defining cybersecurity risk and controls frameworks?	Mean	*SD*	%
1	Frameworks keep everybody informed as they comprehensively cover all aspects of cybersecurity risks.	4.3	1.0	85%
2	Various frameworks are in practice to guide the industry. Frameworks help to understand systems and recognize risks to adopt customized risk management methodologies to minimize risks.	4.3	0.5	85%
3	Cybersecurity frameworks provide organizations with an opportunity to identify areas where existing processes may be strengthened or where new processes can be implemented.	4.4	0.5	88%
4	Lack of resources to manage the framework implementation and maintenance may increase threats, vulnerabilities, and risk to the organization.	3.9	1.2	78%
5	The cybersecurity framework should include the governance, competencies, challenges, and best practices to identify, protect, detect, respond and recover.	4.4	0.7	88%
6	The advantages of having a well-defined cybersecurity risk and controls framework is that it equates to the ability to proactively monitor threats and recover from attacks in an effective manner, thus minimizing the overall business loss.	4.3	0.8	85%
7	Using controls framework will help organizations to be clear on what cybersecurity risks that they are trying to prevent and help to minimize associated risks.	4.3	0.6	85%
8	Using controls framework will help organizations to identify, prevent, detect, respond, and recover from cyber threats, vulnerabilities, and cyber risks.	4.5	0.5	90%
9	Using cybersecurity frameworks will help in the implementation of controls and allow for comprehensive coverage of all aspects of cybersecurity risks.	4.5	0.5	90%
10	Advantages in using security frameworks are in risk assessments, selection of controls and implementation to respond and recover from cyber threats, vulnerabilities, and cyber risks.	4.6	0.5	92%
11	The security framework has to be comprehensive to enable the organization to handle current and emerging cyber threats, vulnerabilities, and cyber risks.	4.3	0.7	87%

The consensus statements made in this round showed the high importance that organizations should place on building skills and competencies needed for managing security objectives for effective organizational performance. In Round 1, the numbers of themed statements are 111 and only 81 were qualified for Round 2. Only 72% of Round 1 statements were qualified for Round 2 survey to get the Delphi agreement judgement rankings on a 5-point Likert scale, and 77 statements out of 81 met the requirements of consensus criteria. Only 68 statements out of 81 of Round 2 statements were qualified for Round 3 survey to get the Delphi importance judgements rankings on a 5-point Likert scale. Participants reached consensus on 64 statements on importance judgement. The Round 3 consensus reached statements represent only 80% of the Round 2 and 58% of Round 1 statements. The analysis of the third round of data is listed in Appendix E. The participants also had the chance to provide details on their ranking.

Summary

Chapter 4 contained the data collection and data analysis of the three rounds of the Delphi research study to identify the managerial competencies for managing security objectives for effective organizational performance with information security management. The results of the study evaluate the data collected from the expert participant panel in the field of information security and risk management. The results of this research demonstrate the expertise of the expert panel to identify the required managerial and technical competencies needed for managing the organizational information security risk from cyberattacks.

A total of 111 qualitative statements were collected by the first round of data collection during the Delphi study. The compiled statements have been placed into categories of risk management strategies and security architecture, managerial and technical skills and competencies needed to mitigate the risks of cyberattacks, common factors for cyberattacks, alignment of organizational resources such as skilled people, well defined regulatory standards, security frameworks, matured processes, and technologies.

Only 72% of Round 1 statements were qualified for Round 2 survey to obtain the Delphi agreement judgment rankings on a 5-point Likert scale, and 77 statements out of 81 were met the requirements of consensus criteria. Only 68 statements out of 81 of Round 2 statements were qualified for Round 3 survey to get the Delphi importance judgments rankings on a 5-point Likert scale. Participants reached consensus on 64 statements on importance judgment. The Round 3 consensus reached statements represent only 80% of the Round 2 and 58% of Round 1 statements.

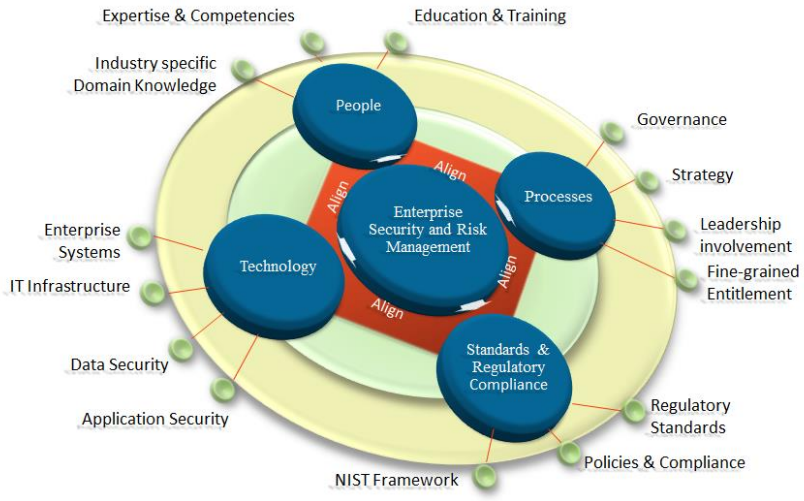

Figure 3. Pictorial view of the organizational alignment.

Key findings of the study included:

- Management involvement and support
- Communication with senior leadership on cyber risk and resource requirements
- Risk management strategies and planning to recover from the effect of cyberattacks
- Developing talent with managerial and technical competencies needed to mitigate the risks of cyberattacks
- Adopting best practices and lessons learned from peers in the industry to assess their strengths and weaknesses to prevent similar incidents and to improve future responses

- Proactively identifying common factors of cyberattacks that could have been prevented with the effective alignment of organizational resources such as people, process, and technology
- Skills and expertise required to build a successful recovery program that can respond to cyberattacks, and Impact of security frameworks

Chapter 5 contains the implications, data interpretations, limitations, recommendations, and the conclusion of this research study.

Chapter 5: Discussion, Conclusions, and Recommendations

The most challenging aspect of information security and risk management is addressing the issue at a higher level and aligning resources to manage information security risk in the company (Andreea, 2014; Bauer, & Bernroider, 2017; D'Urso, 2015; Harrison, 2016; Nicho, 2018). The purpose of this qualitative Delphi study was to explore what competencies senior managers need to align and integrate organizational resources to mitigate information security risks. A qualitative inquiry was chosen to conduct an in-depth study on a practicing information security and risk management expert population. The results of this study included consensus statements by the expert panel on six essential factors such as information security strategy, managerial and technical competencies, organizational competency and maturity of its information security management program, skills and expertise of the team, regulatory standards, and security frameworks. The results of this study show that (a) organizations should have a better understanding of the intricacies that cyberattacks have on its digital assets, (b) management support is essential for the risk management, (c) strategy and planning for managing information security risk is crucial, (d) managerial and technical competencies for management to align organizational resources, and (e) the maturity of the organization's information security management program should improve the organizational readiness for meeting challenges from cyberattacks.

In this chapter, I explain the results of the Delphi panel. I discuss the potential changes that can be made to build required managerial competencies to minimize the cyber risk from cyberattacks. The remaining sections of Chapter 5 include the

interpretations of the findings, limitations of the study, recommendations, and implications.

Interpretation of Findings

The results of this study included consensus statements by the participant panel on six central topics that produced 111 statements in Round 1 for a questionnaire with six open-ended qualitative questions. In Round 2, a total of 77 consensus statements were received from a panel of experts on enterprise information security risk management on agreements judgment measured using a 5-point Likert scale. A total of 64 consensus statements were received from a panel of experts on the enterprise information security risk management on importance judgment measured using a 5-point Likert scale in Round 3. In the second round, four of the 81 statements did not reach the consensus formula that consisted of a mean of 4.0 or greater, 80% agreement, interquartile range of less than 2.5 and *SD* less than 1.5. In the third round, four of the 68 statements did not reach the consensus formula that consisted of a mean of 4.0 or greater, 80% agreement, interquartile of less than 2.5 and *SD* less than 1.5. Table 12 contains the consensus summary of this Delphi study.

Table 10

Consensus from Rounds 2 and 3

Themed Statement Group	Round 1 Statements	Round 2 Statements	Round 2 Consensuses	Round 3 Statements	Round 3 Consensuses
Information security and strategy	22	14	12	8	8
Managerial competencies	23	16	14	12	11
Organizational maturity and competencies	20	13	13	9	8
Alignment of resources	15	12	12	16	16
Skills and expertise	15	11	11	12	11
Regulatory standards and security frameworks	16	15	15	11	10

Summary of Delphi Study Findings

I selected the NIST framework as the conceptual framework of my study because it showcases the ability of an organization to handle cyber threats (Dedeke, 2017; Hiller, & Russell, 2017; NIST, 2018; Pendley, 2018; Stewart, & Jürjens, 2017). Organizations that are at the lowest level of the NIST framework have insufficient security controls and will suffer greatly from cyber threats and attacks. The NIST security framework allows for structured implementation of controls and to comprehensively cover all aspects of cyber security risks. However, my study findings indicate that the NIST framework has certain disadvantages. The usefulness of the framework depends on how an organization has interpreted security controls and if there is room for flexibility to enhance controls for

any modernization/transformation initiatives. Any rigidity can hinder innovation, maturity, and adoption of emerging technologies. In Round 1, 15 participants responded with statements relating to the importance of frameworks, and all 15 statements met consensus.

Organizations that integrate and align people, process, and technology into the overall business process lower the costs of data breaches (McFadzean et al., 2011; Pooley, 2017; Scarfò, 2018). Companies that have an alignment gap between organizational resources have an increased amount of security risks (Cavusoglu, Cavusoglu, Son, & Benbasat, 2015). Nonalignment of organizational resources may lead to gaps in security controls, which expose organizational digital assets to cyberattacks and increased organizational risk (Verma et al., 2018). Twelve participants responded with statements relating to the importance of frameworks, and all 12 statements met consensus.

Senior management is responsible for the implementation and assurance of policies, procedures, and security controls across the organization (Hagen, Albrechtsen, & Hovden, 2008). It is a challenge for management to implement a change and controls in any organization (Jensen, 2017). Twenty-one themed statements were presented for judgment. Of the 14 statements for Question 1, 12 (85%) statements came to a consensus.

People, processes, and technology are the three main pillars of information security management of any organization to counter internal and external cyber threats. Technology draws the most focus from management and is treated with higher priority than human resources and processes (Ashenden, 2008; Bauer, & Bernroider, 2017;

Stewart, & Jürjens, 2017). Sixteen statements were presented for ranking the importance of resource alignment in managing cyber risk, all of which reached a consensus on the importance of resource alignment.

The core competency theory includes six competency areas of result orientation, interpersonal skills, personal accountability, flexibility, problem-solving, and planning and organization (Bass & Bass, 2009; Dulewicz & Higgs, 2005; Geoghegan & Dulewicz, 2008; Marx, 2017; Meng & Boyd, 2017). Participants responded with provided 16 themed statements. Of the 16 statements, 14 (85%) statements reached a consensus. The statements that reached a consensus included emotional intelligence, intimate awareness of company's IT landscape and technologies, leadership qualities, and resourcefulness are needed as competencies.

Determining an organizations asset value and its estimated risk is the first part of risks analysis (Grace et al., 2015; Hoyt & Liebenberg, 2015; Ramakrishna, 2015). Senior management owns the responsibility of protecting the organization from risk from cyberattacks (Shad & Lai, 2015; Soomro et al., 2015). Information security and risk management are a part of the overall organizational strategy and should be led by executive leaders who are familiar with the organizational landscape of the company (Murphy & Murphy, 2013; Safa et al., 2015; Soomro et al., 2015). Of the eight statements relating to this topic, all statements reached consensus. Participants stressed the importance of risk management. The literature also suggests technical competencies and minimal on general management skills for information security managers, but

nontechnical skills and technical skills are important to align organizational resources such as people, process, and technology to contain the organizational risk.

Based on the literature review, there is an information security and risk management skills shortage among noninformation security professionals and nontechnical skills such as leadership, communication, and project management skills shortage among information security professionals. Twelve statements were sent to the panel for ranking that focused on cybersecurity skills and knowledge in managing risk from cyberattacks. Of the 12 statements, 11 (91%) achieved consensus. Participants indicated that cybersecurity management starts with recruiting the right people who have the right background in the industry to develop short-term and long-term plans to address current and emerging cyber threats, vulnerabilities, and cyber risks.

The literature review, NIST security framework, and the key findings of the study indicateded that an organization's management needs to focus on greater risk assessments of critical technology infrastructures outside of the traditional risks. Threats are conducted by attackers seeking to disrupt the systems of an organization and stealing valuable data. Employees need to be trained to handle any incidents that may occur in the organization. Cybersecurity training on detection and identification may improve responses to cyber crime. The findings also pointed to integrating cybersecurity strategy with an organizational overall strategy, industry peers, and regulatory standards approach.

Delphi Round 1

The first round of the study provided six open-ended, seed questions to the participants. The original seed questions were derived from the literature review. Twelve participants of the 18 that agreed to join the study responded to the questionnaire. The initial six seed questions resulted in 111 statements corresponding to the five main themes in Table 6.

Information security and risk management strategy. The first open-ended seed question in Round 1 was to collect factors related to information security and risk management strategy. Twenty-two statements were submitted by the panel as factors to consider when responding information security strategy. The panel stated in agreement judgment that the risk management strategies and plans need to be updated regularly to account for changing technology and business environment. Information technology risk management strategies need to be integrated with enterprise risk management strategies to work as a cohesive self-corrective mechanism against cyberattacks.

Managerial competencies. The second open-ended seed question in Round 1 was to collect factors related to managerial competencies required for managing information security risk. Twenty-three statements were provided by the participants on managerial competencies required for managing information security risk. The panel stated that the managerial competencies should include the understanding of risk management programs within the organization. For effective security management, executive and middle management should posses cyber-security and risk management focused leadership competencies on managing emerging cyber risks.

Organizational maturity of information security and risk management. The third open-ended seed question in Round 1 was to collect factors related to organizational maturity of the information security and risk management for managing organizations information security risk. Twenty statements were provided by the participants on organizational maturity of information security and risk management. The panel agreements state that a prepared leadership will have managerial competencies that place a priority on identifying threats. Such control also puts their organization's mission-critical information and data security as their priority and will align their IT spending with the right objectives.

Alignment of organizational resources. The fourth open-ended seed question in Round 1 was to collect factors related to the alignment of organizational resources such as people, process, and technology for managing organizations information security risk. Fifteen statements were provided by the participants on the alignment of organizational resources required for managing information security risk. The panel's observation included the governance structure for creating a short-term and long-term strategy to manage the organization's cybersecurity risk. Lack of senior leadership support and resources for security and risk management, lack of layered defense approach for identifying threats, vulnerabilities, and required security controls are known common factors responsible for cyberattacks on any organization.

Skills and expertise. The fifth open-ended seed question in Round 1 was to collect factors related to the skills and knowledge required for managing organizations information security risk. Fifteen statements were provided by the participants on the

skills and expertise required for managing information security risk to acceptable goals of the organization. The panel stated that information security risk management starts with recruiting the right people who are competitive and have the right background in the industry. This involves relevant security certifications and experience will help in implementing mitigation plans, involvement in handling a cyberattack, and the ability to develop short-term and long-term plans to address the attack. Investment in domain specialization for the core team, which includes incident response and network security, and ethical hackers will help in building an expert team to manage cyber-risk.

Regulatory standards and security frameworks. The sixth open-ended seed question in Round 1 was to collect factors related to the regulatory standards and security frameworks required for managing organizations information security risk. Sixteen statements were provided by the participants on regulatory standards and security frameworks for managing information security risk to acceptable goals of the organization. The panel observed that the cybersecurity frameworks have to be comprehensive with use cases to enable organizations to customize security controls to meet their business specific requirements and security risks.

Delphi Round 2

The second round of the Delphi presented 81 themed statements analyzed from the first round of data collection. The statements were broken up by the six seed questions such the participants could have better clarity on the research subject. Of the 111 statements sent to the participants, the consensus was found on 77 (95%) of the 81statements.

Information security and risk management strategy. The first open-ended seed question in Round 1 was to collect factors related to information security and risk management strategy. For Question 1 focusing on information security and risk management strategy, 21 themed statements were presented for judgment. Of the 14 statements for Question 1, 12 (85%) statements came to a consensus. The panel highlighted that the leadership should continuously update their risk management strategy to address emerging cyber risks from new and emerging business processes and technologies, a strategy should drive the adaption of advanced tools such as artificial intelligence, machine learning, and analytics to be successful in prevention, detection, and recovering from cyberattacks. The speed and agility of technology adoption have to be increased to meet the security challenges from emerging technologies such as Cloud, IoT, Blockchain, and Bigdata.

Managerial competencies. The second open-ended seed question in Round 1 was to collect factors related to managerial competencies required for managing information security risk. Participants responded with provided 16 themed statements. Of the 16 statements, 14 (85%) statements reached a consensus. The statements that reached a consensus included emotional intelligence, intimate awareness of company's IT landscape and technologies, leadership qualities, and resourcefulness are needed as competencies. Understanding is also needed regarding business processes and digital assets such as applications, data, infrastructure, and people who support them and their potential vulnerabilities. Executive management, senior, and middle management should include cyber-security and risk management focused leadership competencies in their

leadership to mitigate emerging cyber risks. Risk management methodology/frameworks need to be realigned with the new threat landscape

Organizational competencies and the maturity of information security and risk management. The third seed question was to collect factors related to organizational maturity of the information security and risk management for managing organizations information security risk. Participants responded with 13 statements for analysis. Of the presented statements, 13 (100%) of the statements met consensus. The panel stated that managers must have competencies such as excellent communication, problem-solving, teamwork, the capability to define and implement processes, and the maturity to mentor and motivate the team to achieve individual, team and organizational goals. Cybersecurity managers must have the competency to develop and implement well-tested standards, frameworks, and industry best practices in place to address the known and emerging vulnerabilities to protect the organization from cyber threats and risk.

Alignment of organizational resources. The fourth question was to collect factors related to the alignment of organizational resources such as people, process, and technology for managing organizations information security risk. Participants responded with 12 statements for analysis. Of the presented statements, 12 (100%) of the statements met consensus. The responses that panel have provided include the effective use of processes and training programs—the company must introduce active training programs that ensure team members are aware of the company's business processes, infrastructure, and critical digital assets, as well as cybersecurity vulnerabilities, threats, risks, and necessary controls for risk mitigation.

Technical skills and expertise. The fifth question was to collect factors related to the skills and expertise required for managing organizations information security risk. Participants responded with 11 statements for analysis. Of the presented statements, 11 (100%) of the statements met consensus. The panel stated the importance of having well-trained employees that can manage cybersecurity risks. Organizations should invest their resources and time into building strong teams that can identify, mitigate, and plan for risks.

Regulatory standards and security frameworks. The sixth seed question was to collect factors related to the regulatory standards and security frameworks required for managing organizations information security risk. Participants responded with 15 statements for analysis. Of the presented statements, 15 (100%) of the statements met consensus. The panel stated that standards and frameworks are for guidance only; an organization needs to build its frameworks specific to the organization. Frameworks are guiding practices, their intentions vary from country to country, industry to industry, and one should not blindly follow them.

Delphi Round 3

The Round 3 questionnaire was developed to measure the importance of judgment based on agreement judgment measured in Round 2 survey. Only 68 (88%) of Round 2 consensus statements were identified for Round 3 and presented to the participants for judgment of a 5-point Likert scale to identify the most important competencies and attributes required for managing organization's risk from cyberattacks.

Information security and risk management strategy. Eight statements were ranked for their importance of risk strategy and addressing cyber risks. Of the eight statements, all (100%) statements reached consensus. Participants stressed the importance of an organizational leader's role in developing the strategy, standards, policies, plans, to minimize risk from cyberattacks. Organizational leaders and security managers must adapt to advanced tools and processes that will better equip the team, such that they can stay ahead of the issues in cyber threats, vulnerabilities, and cyber risks. With increased cyber threats, weaknesses, and cyber risks, leaders must have people, processes and technologies in place to proactively monitor, identify, diagnose, fix, and prevent cyberattacks.

Managerial competencies. Twelve statements were presented for ranking the importance of managerial competencies in managing cyber risk. Of the 12 statements, 11 (91%) statements reached a consensus on the importance of managerial competencies. The panel suggested that the leaders must have an understanding of the organization related regulatory standards and requirements to support cyber risk management efforts with required resources such as people, process, and technology. To bring awareness, leaders must support internal training and awareness programs on current and emerging cyber threats, vulnerabilities, and cyber risks to all employees.

Organizational competencies and the maturity of information security and risk management. Nine statements were presented for ranking the importance of organizational competencies and the maturity of its information security and risk management program in managing cyber risk. Of the nine statements, 8 (88%) statements

reached a consensus on the importance. The participants highlighted that managers must have competencies such as effective communication, problem-solving, teamwork, the capability to define and implement processes, and the maturity to mentor and motivate individuals and teams to achieve organizational goals.

Alignment of organizational resources. Sixteen statements were presented for ranking the importance of resource alignment in managing cyber risk. Of the 16 statements, all 16 (100%) statements reached a consensus on the importance of resource alignment. Building well-trained incident response teams to identify, protect, detect, respond, and recover will help in addressing cyberattacks. The right governance structure should be in place with a core group with responsibilities for strategy, design, and implementation of cybersecurity programs.

Technical skills and expertise. Twelve statements were sent to the panel For ranking that focused on cybersecurity skills and knowledge in managing risk from cyberattacks. Of the 12 statements, 11 (91%) achieved consensus. Participants indicated that cybersecurity management starts with recruiting the right people who have the right background in the industry to develop short term and long term plans to address current and emerging cyber threats, vulnerabilities, and cyber risks.

The relevant experience in effectively implementing mitigation plans, handling a cyberattack, and the ability to develop short term and long term plans to address the cyberattacks. Participants stressed the importance of expertise in governance, compliance, risk management, business continuity and disaster recovery, cybersecurity threats, vulnerability, control assessments, regulatory compliances, cybersecurity

frameworks, system security architecting, implementation, monitoring, and system level security vulnerabilities testing.

Regulatory standards and security frameworks. Eleven statements were presented for ranking the importance of regulatory standards and security frameworks in managing cyber risk. Of the 11 statements, 10 (90%) statements reached a consensus on the importance of security frameworks.

Cybersecurity frameworks provide organizations with an opportunity to identify areas where existing processes may be strengthened or where new processes can be implemented. The cybersecurity framework should include the governance, competencies, challenges, and best practices to identify, protect, detect, respond and recover.

Limitations of the Study

The research study had some limitations due to the defined criteria of the research participants being from a specific field and a narrow topic (Nowack et al., 2011). Industry experts in different parts of the U.S. may have come to a different consensus on the issue. The scope of the questions in the research study was also limited as I selected the specific competencies that would be debated by the panel.

The purpose of this study was to identify essential managerial competencies that can align the organizational resources while mitigating the impact of cyber attacks. I did not analyze the motive or reasoning behind the potential cyber attacks. There are still gaps in knowledge in the field of information security and cybersecurity management. The study also neglected to include additional ways the organization could be proactive

regarding the risks of the organization. The findings of this research study are dependent on the type of organization. Organizations with fewer security and data requirements may not be able to use the findings of the study for the benefit of their business. Organizations with high information security requirements would be able to apply the results of their study to their management style. Despite the differences between company sizes, organizations should seek to improve their managerial competency scope and maturity levels to meet present and future challenges of cyber-security challenges and risk.

The significant limitation of developing a panel without diverse thinking might skew the results of the study. A group that is too like-minded may be unable to debate and reach consensus. Experts can have differing opinions, but it is vital that they are rational and are able to debate their thoughts for rational discourse.

Recommendations

Recommendations were created based on the results of the qualitative Delphi study. The recommendation was designed to improve the understanding of the various competencies required for managing both the organization information security systems as well as handle the risks faced by the organization. This study focused on a variety of industries to have a holistic view of the impact of competencies on security controls. Six categories were studied to analyze managerial strategy and competencies.

Previous research studies have been conducted on the relationship between security regulations and data breaches of an organization. A gap remains on the people in charge of handling the security controls of an organization. This study may provide insight into useful managerial competencies that can help organizations manage the risk

of cyber attacks. New information on this subject can identify the best legal and regulatory frameworks to handle cyber risk.

Twelve expert panelists involved in this research study stated that the main challenges in managing organizational information security and risk from cyber attacks are lack of strategy, lack of leadership support, and lack of managerial and technical competencies. Future qualitative studies may further explain the reasoning of why specific managerial competencies needed for handling risk. The alignment of people, process, and technology by management should help in reducing the chances of cyberattacks (Chen et al., 2015; Kohnke et al., 2017). The organizations that integrate people, process, and technology into the overall business strategy should have lower costs from data breaches (McFadzean et al., 2011; Pooley, 2017; Scarfò, 2018).

Organizations need to address the security risks of big data for it to be used. (Olson & Wu, 2017; Tian, 2017). Improper alignment of resources lead to gaps in security controls. This leaves the organizational data vulnerable to risk. AI is a useful tool against the risk of cyber threats (Hess & Ludwig, 2018; Kumar et al., 2017; Lawless et al., 2017; Rosenberg, 2017).

Ninety-seven percent (97%) of this study's panel highlighted that the enterprise cyber risk could be reduced if organizational leaders follow the strategy, standards, policies, plans, and procedures according to the information security management plan and align corporate resources before and after an attack to mitigate the risk from cyberattacks. Ninety-three percent (93%) of this study's panel highlighted that the leadership must have an understanding of the organization related regulatory standards

and requirements to support cyber risk management efforts and align required resources such as people, process, and technology. Ninety-two percent (93%) of the panel highlighted that a well-prepared leadership would have managerial competencies that place a priority on identifying current and emerging cyber threats, vulnerabilities, and cyber risks. Such management also puts their organization's mission-critical information and data security as their first priority and will align their IT spending to meet organization objectives. Ninety-five percent (95%) of the panel highlighted that the most crucial security element is effective communication with senior leadership to ensure enough resources are allocated for addressing current and emerging cyber threats, vulnerabilities, and cyber risks. Eighty-seven percent (87%) of the panel highlighted that the cybersecurity starts with recruiting the right people who have the right background in the industry to develop short term and long term plans to address current and emerging cyber threats, vulnerabilities, and cyber risks. Eighty-three percent (83%) of the panel highlighted that the principles of information security remain the same regardless of the change in technology. However, the speed and agility must increase to address persistent threats from emerging technologies such as Cloud, IoT, Blockchain, self-driving cars, and industrial automation. Eighty-five percent (85%) of the panel highlighted that the organizations need to embrace new technologies such as automation, artificial intelligence, and analytics to be successful in the prevention, detection, and recovery from cyberattacks.

This study may provide additional support to specific competencies that have been used by organizational information security management system to manage risk.

Previous studies on the information security risk management competencies were limited to technical competencies and had little information on managerial competencies.

Implications

Technology is an essential part of day-to-day business organizations as it helps to conduct business operations as well as handle financial transactions. Due to the immense importance of technology in the modern business environment, it is important for companies to place a priority on cybersecurity. Having robust security protocols will increase the protection of valuable data. Any organization that fails at preventing data breaches will lose their goodwill in public for not doing their job in managing information security risk (Andreea, 2014; Bauer & Bernroider, 2017; Dionne, 2013; D'Urso, 2015; Harrison, 2016; Kushwaha, 2016; Marx, 2017; Nicho, 2018).

The managerial and technical competencies of organization leadership and information security risk management team have a critical role in developing a short term and long term information security management strategy and its implementation for adequate security controls for mitigating risk from cyberattacks. The research findings may contribute to the understanding of how information security could be pursued and how senior management may improve the utilization of organizational resources to mitigate information security risk and protect organizational financial performance. This study can be used as a basis for additional research to identify new management strategies competencies for aligning organizational resources and countermeasures and to enhance business practices that address information security risks and better returns on investment for information security risk from cyberattacks. The resources that work with

IT could use this information to understand better the variances that come with security threats.

Significance to Practice

This study may reduce the gap in the existing literature on the enterprise risk landscape due to rapid globalization, technology advancements, and dynamically changing regulatory environments. Today's organizations span across countries and are exposed to more significant threats from cyberattacks. The collaboration between federal regulators, business leaders, standards organizations, and academic institutions is one of the critical success factors in enhancing existing or developing new frameworks, standards, and policies for an effective information security risk management based on integrated system theory's system policy theory, and risk management theory and management system theory. The system will be developed based on individual business needs to minimize organizational risk and to improve financial performance. This study may help the organization leadership in aligning, people, process, and technology for achieving information security goals of the organization.

Recommendations for Information Security and Risk Management Teams

Company executives are often charged with the responsibility of leading organizations through challenging situations and achieve organizational short term tactical and long term strategic goals through vision, strategy, and leadership. Unlike traditional business risk management, information risk management requires both managerial and technical competencies. This study may reduce a gap in the understanding of managerial and technical competencies needed for aligning

organizational resources such as people, processes, and technology which are the cornerstone for building a matured enterprise information security and risk management program for effectively mitigating risks such as data breaches, service interruptions for mission-critical businesses, and other services such as hospitals, transportation, utilities, and energy, which essential services for community. Organizations across the world are experiencing interruptions due to unexpected cyberattacks. Researchers are predicting this trend to increase (Liu et al., 2018). Organizations need to take measures to handle the cybersecurity to identify and mitigate threats as well as the impact of those threats.

Significance to Theory

This study may be used for further research to identify new managerial and technical competencies to develop new countermeasures for mitigating risk from cyberattacks. The following may be significant contributions:

1. The gaps identified in management practices that are adopted in organizations using the cloud, internet of things, big data, blockchain, artificial intelligence, and machine learning to support business applications.
2. The findings may help senior management to oversee systems that protect data (Knapp & Ferrante, 2012). This study may also aid in identifying new or enhancing existing competencies and skills, regulatory standards, security frameworks, and the appropriate funding and resources for cybersecurity and risk management programs.
3. This study may also aid in identifying and exposing potential risks due to non-availability of managers with right managerial and technical competencies

that can result in poorly aligned resources and risk mitigation practices and exposed for cyberattacks.

4. This study may also aid in requesting to address gaps in regulatory standards and security frameworks to provide low-level details on new technology-specific security controls.

Significance to Social Change

A data breach that resulted in the leak of sensitive data has a more significant negative effect on organization performance than any other type of breach (Das et al., 2012; Edwards et al., 2016). The effects of data breaches can be devastating on a company and can result in bad media and bankruptcy. Findings may result in social change by reducing the number of data breaches from cyberattacks in the business world thus protecting organizations, employees, and the public from financial loss.

Having a large data leak makes company senior management look irresponsible and not doing due diligence when it comes to protecting themselves (Andreea, 2014; Bauer, & Bernroider, 2017; Dionne, 2013; D'Urso, 2015; Harrison, 2016; Kushwaha, 2016; Marx, 2017; Nicho, 2018). Risk management is the responsibility of senior management in making strategic decisions related to the organization's information security and risk. To measure the overall effectiveness of an organization's information security management controls using return on investment (ROI) using metrics such as finance, governance, information security incidents, and technology. Findings from this study may be used in organizations to train managers to build strong leaders with information security and risk management focused expertise to manage cybersecurity

threats, vulnerabilities, and risk. In the academic world, business and engineering schools may use the findings to introduce new courses to prepare students with industry-ready skills focused on information security and risk management. In organizations, information security and risk management teams may use my findings as a justification to request more funding for training and education to provide new competencies.

Senior management can effectively integrate the entire organization, people, process, and technology for effective information security management to minimize financial loss from cyberattacks and increase organization value to all stakeholders. A qualitative Delphi study was used for this research study. Findings of this study may result in a positive social change by reducing the number of data breaches from cyberattacks in the business world thus protecting organizations, employees, and the public from financial loss.

Conclusions

A review of the literature published within the last 5 years indicated that the risk from cyber attacks is increasing and the annual cost of data breaches was over $2.1 trillion globally by 2019 (Cheng et al., 2017; Cohen, 2017; Gartner, 2014; Juniper, 2017; Meisner, 2018). The general problem was that the risk from cyberattacks is increasing even with senior management involvement and increased capital expenditure on information security and risk management

This Delphi research study used the experience of information security practitioners, researchers, and cybersecurity incident responders as an instrument to understand and measure the competencies and expertise required to manage and mitigate

the risk from cyberattacks effectively. The expert participants used their information security experience to select the best competencies with the most payoffs. The research participants highlighted many critical attributes and competencies such as information security strategy, winning leadership support, and resource alignment. Therefore, based on the results of this study, organizations must explore ways to build maturity into organizational strategy, managerial competencies for aligning critical resources and should improve their enterprise information security and risk management programs through integration with a cybersecurity framework.

Senior management support is one of the critical success factors, but in reality, senior management is not practicing actively in information security management practices and delegating it to their subordinates in many organizations (Banks, 2016; Lee et al., 2016). The involvement and support of the company board and senior management should be more visible and proactive in establishing a strong and an effective security framework for information security and to improve the quality of security controls across the organization to mitigate the risk (Matta et al., 2016).

The security measures tend to be lax in companies where senior management does not participate actively in security measures. There should be a holistic approach to include business managers in security strategy development and implementation (Soomro et al., 2015). Lee et al. (2016) stated that the topic of the governance of IT and information security is one of the agenda items in corporate board meetings. The findings from this study could help organizations in the development of their information security practices and managerial competencies for aligning and integrating organizational

resources. The knowledge also provides insight such that a company can use it in developing their budget and organizational strategies (Garg et al., 2003). The most important objectives include security controls, risk management, and organizational policies. These factors should all be considered when implementing organizational policy.

References

Aasi, P., Rusu, L., & Leidner, D. (2017). IT organizational structure relationship with IT governance performance: Case of a public organization. In *Information Technology Governance in Public Organizations* (pp. 229-252). doi:10.1007/978-3-319-58978-7_10

Ahmad, W. A., & Mohammad, B. (2012). Can a single security framework address information security risks adequately? *International Journal of Digital Information and Wireless Communications, 2*(3), 222-230. Retrieved from http:/www.diwc.net

Ahmed, R., & Anantatmula, V. S. (2017). Empirical study of project manager's leadership competence and project performance. *Engineering Management Journal*, *29*(3), 189-205. doi:10.1080/10429247.2017.1343005

Ahmed, I., & Manab, N. A. (2016). Influence of enterprise risk management success factors on firm financial and non-financial performance: A proposed model. *International Journal of Economics and Financial Issues, 6*(3), 830-836. Retrieved from http://www.econjournals.com

Ali, S., Al Balushi, T., Nadir, Z., & Hussain, O. K. (2018). Risk management for CPS security. In *Cyber Security for Cyber Physical Systems* (pp. 11-33). doi:10.1007/978-3-319-75880-0_2

Alias, N. A. (2015). *Designing, developing and evaluating a learning support tool: A case of design and development research (DDR)*. Retrieved from http://www.srmo.sagepub.com

Amaral, L. A., Tiburski, R. T., de Matos, E., & Hessel, F. (2015). Cooperative middleware platform as a service for internet of things applications. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing* (pp. 488-493). doi:10.1145/2695664.2695799

American Psychological Association. (2010). *Publication manual of the American Psychological Association* (6th ed.). Washington, DC: Author.

Anderson, M. H., & Sun, P. Y. (2017). Reviewing leadership styles: Overlaps and the need for a new 'full-range'theory. *International Journal of Management Reviews*, *19*(1), 76-96. doi:10.1111/ijmr.12082

Andrade, R., Torres, J., & Flores, P. (2018, January). Management of information security indicators under a cognitive security model. In *Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual*, 478-483. doi:10.1109/CCWC.2018.8301745

Andreea, A. (2014). Risk assessment at enterprise level. *Analele Universităţii ConstantinBrâncuşi Din Târgu Jiu: Seria Economie, 1*(6), 107-109. Retrieved from http://www.utgjiu.ro

Andoh-Baidoo, F. K., & Osei-Bryson, K. (2007). Exploring the characteristics of internet security breaches that impact the market value of breached firms. *Expert Systems with Applications, 32*(3), 703-725. doi:10.1016/j.eswa.2006.01.020

Anthony, E. L. (2017). The impact of leadership coaching on leadership behaviors. *Journal of Management Development, 36*(7), 930-939. doi:10.1108/JMD-06-2016-0092

Anzengruber, J., Goetz, M. A., Nold, H., & Woelfle, M. (2017). Effectiveness of managerial capabilities at different hierarchical levels. *Journal of Managerial Psychology, 32*(2), 134-148. doi:10.1108/JMP-12-2015-0451

Ara, A., Al-Rodhaan, M., Tian, Y., & Al-Dhelaan, A. (2015). A secure service provisioning framework for cyber physical cloud computing systems. *International Journal of Distributed and Parallel Systems, 6*(1), 1-11. doi:10.5121/ijdps.2015.6101

Archer, N. (2012). Consumer identity theft prevention and identity fraud detection behaviours. *Journal of Financial Crime, 19*(1), 20-36. doi:10.1108/13590791211190704

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report, 13*(4), 195-201. doi:10.1016/j.istr.2008.10.006

Astuti, H. M., Muqtadiroh, F. A., Darmaningrat, E. W. T., & Putri, C. U. (2017). Risks assessment of information technology processes based on COBIT 5 framework: A case study of ITS service desk. *Procedia Computer Science, 124*, 569-576. doi:10.1016/j.procs.2017.12.191

August, T., August, R., & Shin, H. (2014). Designing user incentives for cybersecurity. *Communications of the ACM, 57*(11), 43-46. doi:10.1145/2629487

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security, 8*(2), 33-56. doi:10.1080/15536548.2012.10845654

Babu, M. S., Babu, A. M., & Sekhar, M. C. (2013). Enterprise risk management integrated framework for cloud computing. *International Journal of Advanced Networking and Applications, 5*(3), 1939-1950. Retrieved from http://www.ijana.in

Bachmann, B. (2017). Literature review: The evolution of ethical leadership. In *Ethical Leadership in Organizations* (pp. 27-63). doi:10.1007/978-3-319-42942-7_3

Bahtit, H., & Regragui, B. (2013). Risk Management for ISO 27005 decision support. *International Journal of Innovative Research in Science, Engineering and Technology, 2*(3), 530-538. Retrieved from http://www.ijirst.org/

Banks, N. (2016). Practice what you preach. *Computer Fraud & Security, 2016*(4), 5-8. doi:10.1016/S1361-3723(16)30035-5

Barafort, B., Mesquida, A. L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces, 54*, 176-185. doi:10.1016/j.csi.2016.11.010

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security, 59*, 9-25. doi:10.1016/j.cose.2016.02.007

Bass, B. M., & Bass, R. (2009). *The Bass handbook of leadership: Theory, research, and managerial applications*. New York, NY: Free Press.

Bauer, B. J., Richardson, T. M., & Marion, J. W. (2014). Project manager 'management competency' vs. 'technical competency': Which is more important to overall project management success? *International Journal of Engineering Research and*

Applications, 4(4). Retrieved from http://www.commons.erau.edu

Bauer, S., & Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 48*(3), 44-68.doi:10.1145/3130515.3130519

Benson, V., McAlaney, J., & Frumkin, L. A. (2018). Emerging threats for the human element and countermeasures in current cyber security landscape. In *Psychological and Behavioral Examinations in Cyber Security* (pp. 266-271). IGI Global.

Bernard, H. R., & Bernard, H. R. (2013). *Social research methods: Qualitative and quantitative approaches.* Thousand Oaks, CA: Sage.

Bertino, E., & Ferrari, E. (2018). Big data security and privacy. In *A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years* (vol. 31, pp. 425-439). Rende, Italy: Springer, Cham.

Bisogni, F. (2016). Proving limits of state data breach notification laws: Is a federal law the most adequate solution? *Journal of Information Policy, 6*(1), 154-205. doi:10.5325/jinfopoli.6.2016.0154

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM, 51*(4), 64=68. doi:10.1145/1330311.1330325

Borden, D. S., Shaw, G., & Coles, T. (2017). Consensus building in social marketing campaigns through the Delphi method. *Social Marketing Quarterly, 23*(4), 354-

367. doi:10.1177/1524500417732772

Brady, S. R. (2015). Utilizing and adapting the Delphi method for use in qualitative research. *International Journal of Qualitative Methods*, *14*(5), 1. doi:10.1177/1609406915621381

Brill, J. M., Bishop, M. J., & Walker, A. E. (2006). The competencies and characteristics required of an effective project manager: A web-based Delphi study. *Educational Technology Research and Development*, *54*(2), 115-140. doi:10.1007/s11423-006-8251-y

Brustbauer, J. (2016). Enterprise risk management in SMEs: Towards a structural model. *International Small Business Journal, 34*(1), 70-85. doi:10:1177/0266242614542853

Brynjolfsson, E., & McAfee, A. (2017). What's driving the machine learning explosion. *Harvard Business Review,* 3-11. Retrieved from http://www.hbr.org

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209. doi:10.1016/j.chb.2016.11.018

Caldwell, T. (2012). Reporting data breaches. *Computer Law & Security Review, 7*, 5-10. doi:10.1016/S1361-3723(12)70072-6

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431. doi:10.3233/JCS-2003-

11308

Capretz, L. F. (2014). Bringing the human factor to software engineering. *IEEE Software, 31*(2), 102-103. doi:10.1109/MS.2014.30

Cardinaels, E. (2015). Earnings benchmarks, information systems, and their impact on the degree of honesty in managerial reporting. *Accounting, Organizations and Society*, *52*, 50-62. doi:10.1016/j.aos.2015.09.002

Carden, L. L., Boyd, R. O., & Valenti, A. (2015). Risk management and corporate governance: Safety and health work model. *Southern Journal of Business and Ethics, 7*(1), 137-148. Retrieved from http://www.salsb.org

Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics, 20*, 701-715. doi:10.1007/s11948-014-9551-y

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, *52*(4), 385-400. doi:10.1016/j.im.2014.12.004

Chander, M., Jain, S. K., & Shankar, R. (2013). Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach. *Journal of Modelling in Management*, *8*(2), 171-189. doi:10.1108/JM2-10-2011-0054

Chang, S. E., & Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458.

doi:10.1108/02635570710734316

Chang, V. (Ed.). (2015). *Delivery and adoption of cloud computing services in contemporary organizations.* Hershey, PA: IGI Global.

Chaudhry, P. E., Chaudhry, S., & Reese, R. (2012). Developing a model for enterprise information systems security. *Economics, Management and Financial Markets, 7*(4), 587-599. Retrieved from http://www.addletonacademicpublishers.com

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

Chen, J. Q., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. *International Journal of Healthcare Management*, *10*(2), 135-146. doi:10.1080/20479700.2016.1270875

Chen, Y., Ramamurthy, K., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11-19. doi:10.1080/08874417.2015.11645767

Chio, C., & Freeman, D. (2018). *Machine learning and security*. Sebastopol, CA: O'Reilly Media.

Choi, T. M., & Lambert, J. H. (2017). Advances in risk analysis with big data. *Risk Analysis*, *37*(8), 1435-1442. doi:10.1111/risa.12 859

Cirani, S., Ferrari, G., & Veltri, L. (2013). Enforcing security mechanisms in the IP-based

internet of things: An algorithmic overview. *Algorithms*, *6*(2), 197-226. doi:10.3390/a6020197

Clayton, M. J. (1997). Delphi: A technique to harness expert opinion for critical decision-making tasks in education. *Educational Psychology*, *17*(4), 373-386. doi:10.1080/0144341970170401

Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: Does size matter? *Journal of Advanced Nursing, 70*(3), 473-475. doi:10.1111/jan.12163

Clibbens, N., Walters, S., & Baird, W. (2012). Delphi research: Issues raised by a pilot study. *Nurse Researcher*, *19*(2), 37-44. doi:10.7748/nr2012.01.19.2.37.c8907

Cohen, F. (2017). What's the big deal about big data loss (Actually theft)? *EDPACS*, *55*(6), 6-11. doi:10.1080/07366981.2016.1220227

Cole, Z. D., Donohoe, H. M., & Stellefson, M. L. (2013). Internet-based Delphi research: Case based discussion. *Environmental Management, 51*(3), 511-523. doi:10.1007/s00267-012-0005-5

Cook, A., Robinson, M., Ferrag, M. A., Maglaras, L. A., He, Y., Jones, K., & Janicke, H. (2018). Internet of Cloud: Security and privacy issues. In *Cloud Computing for Optimization:Foundations, Applications, and Challenges*, 271-301. Springer, Cham. doi:10.1007/978-3-319-73676-1_11

Cooper, D. R., & Schindler, P. S. (2011). *Business research methods.* Columbus, OH: McGraw-Hill.

Craig, A. N., Shackelford, S. J., & Hiller, J. S. (2015). Proactive cyber security: A

comparative industry and regulatory analysis. *American Business Law Journal,52*(4), 721-787. doi:10.1111/ablj.12055

Cram, W. A., Brohman, M. K., Chan, Y. E., & Gallupe, R. B. (2016). Information systems control alignment: Complementary and conflicting systems development controls. *Information & Management*, *53*(2), 183-196. doi:10.1016/j.im.2015.09.012

Creswell, J. W. (2009*). Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, CA: Sage.

Croft, L., & Seemiller, C. (2017). Developing leadership competencies. *New directions for student leadership*, *2017*(156), 7-18. doi:10.1002/yd.20267

Dabbagh, M., & Lee, S. P. (2014). An approach for integrating the prioritization of functional and nonfunctional requirements. *The Scientific World Journal 2014, 2014*, 1-13. doi:10.1155/2014/737626

Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science, 9*(3), 458-467. doi:10.1287/mnsc.9.3.458

Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to informationsecurity breach: A study using firm and attack characteristics. *Journal of Information Privacy & Security, 8*(4), 27-55. doi:10.1080/15536548.2012.10845665

Dave, D., Meruliya, N., Gajjar, T. D., Ghoda, G. T., Parekh, D. H., & Sridaran, R. (2018). Cloud security issues and challenges. In *Big Data Analytics*, 499-514. Springer, Singapore. doi:10.1007/978-981-10-6620-7_48

Dedeke, A. (2017). Cybersecurity framework adoption: Using capability levels for implementation tiers and profiles. *IEEE Security & Privacy*, (5), 47-54. doi:10.1109/MSP.2017.3681063

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. doi:10.1016/j.techfore.2015.12.009

Demek, K. C., Raschke, R. L., Janvrin, D. J., & Dilla, W. N. (2018). Do organizations use a formalized risk management process to address social media risk? *International Journal of Accounting Information Systems*, *28*, 31-44. doi:10.1016/j.accinf.2017.12.004

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, 56, 63–69. doi:10.1016/j.cose.2015.10.001

Dionne, G. (2013). Risk management: History, definition, and critique. *Risk Management and Insurance Review, 16*(2), 147-166. doi:10.1111/rmir.12016

Donohoe, H., Stellefson, M., & Tennant, B. (2012). Advantages and limitations of the Delphi technique: Implications for health education researchers. *American Journal of Health Education, 43*(1), 38. doi:10.1080/19325037.2012.10599216

Drucker, P. (2016). *The effective executive*. New York, NY: Routledge.

Dulewicz, V., & Higgs, M. (2005). Assessing leadership dimensions, styles and organizational context, *Journal of Managerial Psychology, 20*(2), 105-23.

doi:10.1108/02683940510579759

D'Urso, M. (2015). The cyber combatant: A new status for a new warrior. *Philosophy & Technology*. *28*(3), 475. doi:10.1007/s13347-015-0196-9.

Eberly, M. B., Bluhm, D. J., Guarana, C., Avolio, B. J., & Hannah, S. T. (2017). Staying after the storm: How transformational leadership relates to follower turnover intentions in extreme contexts. *Journal of Vocational Behavior*, *102*, 72-85. doi:10.1016/j.jvb.2017.07.004

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity*, *2*(1), 3–14. doi:10.1093/cybsec/tyw003

Englander, M. (2016). The phenomenological method in qualitative psychology and psychiatry. *International Journal of Qualitative Studies on Health and Well-being, 11*(1), 1-11. doi:10.3402/qhw.v11.30682

Everett, C. (2011). A risky business: ISO 31000 and 27005 unwrapped. *Computer Fraud & Security, 2011*(2), 5-7. doi:10.1016/S1361-3723(11)70015-X

Eycott, A. E., Marzano, M., & Watts, K. (2011). Filling evidence gaps with expert opinion: The use of Delphi analysis in least-cost modeling of functional connectivity. *Landscape and Urban Planning*, *103*(3-4), 400-409. doi:10.1016/j.landurbplan.2011.08.014

Fan, Y., Thomas, M., & Anantatmula, V. (2014). A longitudinal study of the required skills of project managers. *The Journal of Modern Project Management, 1*(3). doi:10.3963/jmpm.v1i3.24

Farhadi, M., Haddad, H., & Shahriar, H. (2018). Compliance of electronic health record

applications with HIPAA security and privacy requirements. In *Security and Privacy Management, Techniques, and Protocols*, 199-213. doi:10.4018/978-1-5225-5583-4.ch007

Faris, S., Hasnaoui, S. E., Medromi, H., Iguer, H., & Sayouti, A. (2014). Toward an effective information security risk management of university's information systems using multi agent systems, ITIL, ISO 27002, ISO 27005. *International Journal of Advanced Computer Science and Applications, 5*(6), 114-118. doi:10.14569/IJACSA.2014.050617

Farrell, M., & Gallagher, R. (2015). The valuation implications of enterprise risk management maturity. *Journal of Risk and Insurance, 82*(3), 625-657. doi:10.1111/jori.12035

Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences*, *256*, 57-73. doi:10.1016/j.ins.2013.02.036

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, *22*(5), 410-430. doi:10.1108/IMCS-07-2013-0053

Frame, J. D. (2003). *Managing projects in organizations: How to make the best use of time, techniques, and people*. San Francisco, CA: John Wiley & Sons.

Frydman, M., Ruiz, G., Heymann, E., César, E., & Miller, B. P. (2014). Automating risk analysis of software design models. *The Scientific World Journal, 2014*, 1-12. doi:10.1155/2014/805856

Gaff, B. M. (2015). BYOD? OMG! *Computer, 48*(2), 10–11. doi:10.1109/MC.2015.34

Gao, H., & Zhang, J. (2018). SOX Section 404 and corporate innovation. doi:10.1108/RAF-04-2016-0066

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security, 11*(2/3), 74-83. doi:10.1108/09685220310468646

Gartner. (2014, March 19). Gartner says the Internet of Things will transform the data center. Retrieved from http://www. gartner.com

Geoghegan, L., & Dulewicz, V. (2008). Do project manager's leadership competencies contribute to project success? *Project Management Journal, 39*(4), 58-67.

Ghani, H., Khelil, A., Suri, N., Csertán, G., Gönczy, L., Urbanics, G., & Clarke, J. (2014). Assessing the security of internet connected critical infrastructures. *Security & Communication Networks, 7*, 2713-2725. doi:10.1002/sec.399

Giorgi, A. P. (2002). The question of validity in qualitative research. *Journal of Phenomenological Psychology, 33*(1), 1-18. doi:10.1163/156916202320900392

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2016). Resilience of cyber systems with over-and underregulation. *Risk Analysis*, *37*(9), 1644-1651. doi:10.1111/risa.12729

Gochhayat, J., Giri, V. N., & Suar, D. (2017). Influence of organizational culture on organizational effectiveness: The mediating role of organizational communication. *Global Business Review*, *18*(3), 691-702. doi:10.1177/0972150917692185

Gordon, L. A., Loeb, M. P., & Lei, Z. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*(1), 33-56. doi:10.3233/JCS-2009-0398

Govindji, S., Peko, G., & Sundaram, D. (2017). A context adaptive framework for IT governance, risk, compliance and security. In *Context-Aware Systems and Applications, and Nature of Computation and Communication, 217,* 14-24. doi:10.1007/978-3-319-77818-1_2

Grace, M. F., Leverty, J. T., Phillips, R. D., & Shimpi, P. (2015). The value of investing in enterprise risk management. *Journal of Risk and Insurance, 82*(2), 289-316. doi:10.1111/jori.12022

Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294–1312. doi:10.1109/COMST.2015.2388550

Grahn, K., Westerlund, M., & Pulkkis, G. (2017). Analytics for network security: A survey and taxonomy. In *Information Fusion for Cyber-Security Analytics*, 175-193. doi:10.1007/978-3-319-44257-0_8

Gupta, U. G., & Clarke, R. E. (1996). Theory and applications of the Delphi technique: A Bibliography, (1975-1994). *Technological Forecasting and Social Change, 53*(2), 185-211. doi:10.1016/S0040-1625(96)00094-7

Haber, M. J., & Hibbert, B. (2018). Regulatory compliance. In *Privileged Attack Vectors*, 171-188. doi:10.1007/978-1-4842-3048-0_19

Hackett, R. (2016, Jun 15). Changing face of security. Retrieved from

http://www.fortune.com

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), 377-397. doi:10.1108/09685220810908796

Haislip, J. Z., Masli, A., Richardson, V. J., & Watson, M. W. (2015). External reputational penalties for CEOs and CFOs following information technology material weaknesses. *International Journal of Accounting Information Systems*, *17*, 1–15. doi:10.1016/j.accinf.2015.01.002

Harrison, A. E. (2016). Exploring millennial leadership development: A Rapid evidence assessment of information communication technology and reverse mentoring competencies. Retrieved from http://www.papers.ssrn.com

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing, 32*(4), 1008-1015. doi:10.1046/j.1365-2648.2000.t01-1-01567.x

Hasson, F., & Keeney, S. (2011). Enhancing rigour in the Delphi technique research. *Technological Forecasting and Social Change*, *78*(9), 1695-1704. doi:10.1016/j.techfore.2011.04.005

Haynes, C. A., & Shelton, K. (2017). *Delphi method in a digital age. Handbook of research on innovative techniques, trends, and analysis for optimized research methods*. Hershey, PA. IGI Global.

Heiko, A. (2012). Consensus measurement in Delphi studies: Review and implicationsfor future quality assurance. *Technological Forecasting and Social Change, 79*(8),

1525-1536. doi:10.1016/j.techfore.2012.04.013

Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society, 4*(4), 30-38. doi:10.1016/j.techsoc.2015.11.007

Heninger, W. G., Johnson, E. N., & Kuhn, J. R. (2017). The Association between IT material weaknesses and earnings management. *Journal of Information Systems.* doi:10.2308/isys-51884

Henry, K. (2017). Leadership frameworks for organizational systems. *Frameworks for advanced nursing practice and research: Philosophies, Theories, Models, and Taxonomies*, 269. New York, NY: Springer.

Hess, E. D., & Ludwig, K. (2018). The Smart machine age will require a new story about leadership. *Leader to Leader*, *2018*(87), 54-59. doi:10.1002/ltl.20344

Hiller, J. S., & Russell, R. S. (2017). Privacy in crises: The NIST privacy framework. *Journal of Contingencies and Crisis Management*, *25*(1), 31-38. doi:10.1111/1468-5973.12143

Hirsch, P. B. (2018). Tie me to the mast: Artificial intelligence & reputation risk management. *Journal of Business Strategy*, *39*(1), 61-64. doi:10.1108/JBS-11-2017-0160

Hogan, R. (2017). *Personality and the fate of organizations*. New York, NY: Psychology Press.

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, *22*(2), 242-260. doi:10.1108/JFC-09-2013-0055

Hornstein, H. A. (2015). The integration of project management and organizational change management is now a necessity. *International Journal of Project Management*, *33*(2), 291-298. doi:10.1016/j.ijproman.2014.08.005

Hosseinian-Far, A., Ramachandran, M., & Slack, C. L. (2018). Emerging trends in Cloud Computing, Big Data, Fog Computing, IoT and Smart Living. In *Technology for Smart Futures*, 29-40. doi:10.1007/978-3-319-60137-3_2

Houser, W. (2015). Could what happened to Sony happen to us? *IT Professional, 17*(2), 54-57. doi:10.1109/MITP.2015.21

Hoyt, R. E., & Liebenberg, A. P. (2015). Evidence of the value of enterprise risk management. *Journal of Applied Corporate Finance, 27*(1), 41-47. doi:10.1111/jacf.12103

Hsu, C., & Sandford, B. (2007). The Delphi technique: Making sense of consensus. *Practical Assessment, Research & Evaluation, 12*(10), 119-127. Retrieved from http://www.pareonline.net

Huckvale, K., Jose, T. P., Tilney, M., Benghozi, P., & Car, J. (2015). Unaddressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment. *13*. doi:10.1186/s12916-015-0444-y

Hughes, D. L., Rana, N. P., & Simintiras, A. C. (2017). The changing landscape of IS project failure: An examination of the key factors. *Journal of Enterprise Information Management*, *30*(1), 142-165. doi:10.1108/JEIM-01-2016-0029

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*, 615-660. doi:10.1111/j.1540-5915.2012.00361.x

Ibrahim, R., Boerhannoeddin, A., & Bakare, K. K. (2017). The effect of soft skills and training methodology on employee performance. *European Journal of Training and Development*, *41*(4), 388-406. doi:10.1108/EJTD-08-2016-0066

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computer and Security, 31*, 83–95. doi:10.1016/j.cose.2011.10.007

ISF. (2014). *Standard of good practice for information security: The definitive guide to enable information security compliance.* Retrieved from http://www.securityforum.org

Islam, S., Mouratidis, H., & Weippl, E. R. (2014). An empirical study on the implementation and evaluation of a goal-driven software development risk management model. *Information and Software Technology, 56*, 117-133. doi:10.1016/j.infsof.2013.06.003

James, D., & Warren-Forward, H. (2015). Research methods for formal consensus development. *Nurse Researcher*, *22*(3), 35. doi:10.7748/nr.22.3.35.e1297

Jayakumar, H., Raha, A., Kim, Y., Sutar, S., Lee, W. S., & Raghunathan, V. (2016). Energy-efficient system design for IoT devices. In *Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific*, 298-301. IEEE. doi:10.1109/ASPDAC.2016.7428027

Jensen, S. H. (2017). Frederick Winslow Taylor: The first change agent, from rule of

thumb to scientific management. *The Palgrave Handbook of Organizational Change Thinkers*, 1275. doi:10.1007/978-3-319-52878-6

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of things: Perspectives and challenges. *Wireless Networks, 20*, 2481-2501. doi:10.1007/s11276-014-0761-7

Jones, R. L., & Rastogi, A. (2004). Secure coding: Building security into the software development life cycle. *Information Systems Security, 5*, 29-39. doi:10.1201/1086/44797.13.5.20041101/84907.5

Juniper. (2017). Cybercrime will cost businesses over $2 trillion by 2019. Retrieved from http://www.juniperresearch.com

Kahtan, H., Bakar, N. A., & Nordin, R. (2014). Awareness of embedding security features into component-based software development model: A survey. *Journal of Computer Science, 10*, 1411-1417. doi:10.3844/jcssp.2014.14

Kaya, İ. (2018). Perspectives on internal control and enterprise risk management. In *Eurasian Business Perspectives*, *8*, 379-389. doi:10.1007/978-3-319-67913-6_26

Keeney, S., Hasson, F., & McKenna, H. (2006). Consulting the oracle: Ten lessons from using the Delphi technique in nursing research. *Journal of Advanced Nursing, 53*(2), 205-212. doi:10.1111/j.1365-2648.2006.03716.x

Kerzner, H., & Kerzner, H. R. (2017). *Project management: a systems approach to planning, scheduling, and controlling*. Hoboken, NJ: John Wiley & Sons.

Khan, H. H. (2014). Factors generating risks during requirement engineering process in global software development environment. *International Journal of Digital*

Information and Wireless Communications, 4(1), 63-78. doi:10.17781/P001084

Khaim, R., Naz, S., Abbas, F., Iqbal, N., & Hamayun, M. (2016). A review of security integration technique in agile software development. *International Journal of Software Engineering & Applications, 7*(3). doi:10.5121/ijsea.2016.7304

Khari, M. (2018). Comprehensive study of cloud computing and related security issues. In *Big Data Analytics*, *654*, 699-70. doi:10.1007/978-981-10-6620-7_68

Kierkegaard, P. (2012). Medical data breaches: Notification delayed is notification denied. *Computer Law & Security Review*, *28*(2), 163-183. doi:10.1016/j.clsr.2012.01.003

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

Kohnke, A., Shoemaker, D., & Sigler, K. (2017). *Implementing cybersecurity*. New York, NY: Auerbach.

Kumar, R., & Singh, H. (2015). A proactive procedure to mitigate the BYOD risks on the security of an information system. *ACM SIGSOFT Software Engineering Notes*, *40*(1), 1-4. doi:10.1145/2693208.2693231

Kumar, R., Pattnaik, P. K., & Pandey, P. (Eds.). (2017). *Detecting and mitigating robotic cyber security risks*. Hershey, PA: IGI Global.

Kushwaha, P. (2016). Amalgamation of the information security management system with business-paradigm shift. *International Journal of Computer Science and*

Information Security, *14*(1), 105-111. Retrieved from http://www.site.google.com

Lam, J. (2014). *Enterprise risk management: From incentives to controls* (2nd ed.). Hoboken, NJ: Wiley.

Landeta, J. (2006). Current validity of the Delphi method in social sciences. *Technological Forecasting and Social Change, 73*(5), 467-482. doi:10.1016/j.techfore.2005.09.002

Laureani, A., & Antony, J. (2017). Leadership characteristics for lean six sigma. *Total Quality Management & Business Excellence*, *28*(3-4), 405-426. doi:10.1080/14783363.2015.1090291

Lawless, W. F., Mittu, R., Sofge, D., & Russell, S. (Eds.). (2017). *Autonomy and artificial intelligence: A Threat or Savior?* Rende, Italy: Springer, Cham.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review, 37*(12), 1049–1092. doi:10.1108/MRR-04-2013-0085

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, *59*, 60–70. doi:10.1016/j.cose.2016.02.004

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431–440. doi:10.1016/j.bushor.2015.03.008

Lee-Jen Wu, S., Hui-Man, H., & Hao-Hsien, L. (2014). A comparison of convenience sampling and purposive sampling. *Journal of Nursing, 61*(3), 105.

doi:10.6224/JN.61.3.105

Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the castle model of cyber risk and cyber-security. *Government Information Quarterly*, *33*(1), 250-257. doi:10.1016/j.giq.2016.01.012

Leszczyna, R. (2018). A review of standards with cybersecurity requirements for smart grid. *Computers & Security*, *77*, 262-276. doi:10.1016/j.cose.2018.03.011

Lin, C., He, D., Kumar, N., Choo, K. K. R., Vinel, A., & Huang, X. (2018). Security and privacy for the Internet of drones: Challenges and solutions. *IEEE Communications Magazine*, *56*(1), 64-69. doi**:**10.1109/MCOM.2017.1700390

Linstone, H. A., & Turoff, M. (1975). *The Delphi method techniques and applications.*Boston, MA: Addison-Wesley.

Linstone, H. A., & Turoff, M. (2002). *Delphi method: Techniques and applications*. Reading, MA: Addison-Wesley.

Linstone, H. A., & Turoff, M. (2011). Delphi: A brief look backward and forward. *Technological Forecasting and Social Change, 78*(9), 1712-1719. Retrieved from http://www.sciencedirect.com

Liu, Q., Liu, T., Liu, Z., Wang, Y., Jin, Y., & Wen, W. (2018, January). Security analysis and enhancement of model compressed deep learning systems under adversarial attacks. In *Design Automation Conference (ASP-DAC), 2018 23rd Asia and South Pacific,* 721-726. doi:10.1109/ASPDAC.2018.8297407

Lo, K., Macky, K., & Pio, E. (2015). The HR competency requirements for strategic and functional HR practitioners. *The international Journal of Human Resource*

Management, *26*(18), 2308-2328. doi:10.1080/09585192.2015.1021827

Loo, R. (2002). The Delphi method: A powerful tool for strategic management. *Policing: An International Journal of Police Strategies & Management, 25*(4), 762-769. doi:10.1108/13639510210450677

Luna, S., & Pennock, M. J. (2018). Social media applications and emergency management: A Literature review and research agenda. *International Journal of Disaster Risk Reduction*, *28*, 565-577. doi:10.1016/j.ijdrr.2018.01.006

Lundqvist, S. A. (2015). Why firms implement risk governance: Stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy, 34*(5), 441-466. doi:10.1016/j.jaccpubpol.2015.05.002

Maamari, B. E., & Majdalani, J. F. (2017). Emotional intelligence, leadership style and organizational climate. *International Journal of Organizational Analysis*, *25*(2), 327-345. doi:10.1108/IJOA-04-2016-1010

Makhlouf, H. H. (2017). Managing the organization culture in domestic and foreign operations. *World Journal of Social Science*, *4*(1), 22. doi:10.5430/wjss.v4n1p22

Manogaran, G., Thota, C., Lopez, D., & Sundarasekar, R. (2017). Big data security intelligence for healthcare industry 4.0. In *Cybersecurity for Industry 4.0,* 103-126. doi:10.1007/978-3-319-50660-9_5

Martin, P. G., Tomkinson, N. G., & Scott, T. B. (2017). The future of nuclear security: Commitments and actions–power generation and stewardship in the 21st century. *Energy Policy*, *110*, 325-330. doi:10.1016/j.enpol.2017.08.038

Marshall, C., & Rossman, G. B. (2011). *Designing qualitative research.* Los Angeles,

CA: Sage.

Marx, T. G. (2017). The Impacts of company size on leadership. *Management and Organizational Studies*, *4*(1), 82. doi:10.5430/mos.v4n1p82

Mashal, I., Alsaryrah, O., Chung, T.-Y., Yang, C.-Z., Kuo, W.-H., & Agrawal, D. P. (2015). Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks*, *28*, 68–90. doi:10.1016/j.adhoc.2014.12.006

Mataracioglu, T., & Ozkan, S. (2011). Governing information security in conjunction with COBIT and ISO 27001. *International Journal of Network Security & Its Applications, 3*(4), 111-116. doi:10.5121/ijcsit.2011.3321

Matta, M., Cavusoglu, H., & Benbasat, I. (2016). Understanding the board's involvement in information technology governance. Retrieved from http://www.papers.ssrn.com

Mayfield, J., Mayfield, M., & Sharbrough, W. C. (2015). Strategic vision and values in top leader's communications: Motivating language at a higher level. *International Journal of Business Communication, 52*(1), 97-121. doi:10.1177/2329488414560282

Mbowe, J. E., Zlotnikova, I., Msanjila, S. S., & Oreku, G. S. (2014). A conceptual framework for threat assessment based on organization's information security policy. *Journal of Information Security, 5*, 166–177. doi:10.4236/jis.2014.54016

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion, 30*(7), 537-542. doi:10.1177/0267659114559116

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2011). Information assurance and corporate strategy: A Delphi study of choices, challenges, and developments for the future. *Information Systems Management, 28*(2), 102-129. doi:10.1080/10580530.2011.562127

McNeil, A. J., Frey, R., & Embrechts, P. (2015). *Quantitative risk management: Concepts, techniques and tools*. Princeton, NJ: Princeton University Press.

Meijering, J., Kampen, J., & Tobi, H. (2013). Quantifying the development of agreement among experts in Delphi studies. *Technological Forecasting & Social Change*, *80*(8), 1607-1614. doi:10.1016/j.techfore.2013.01.003

Meisner, M. (2018). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63-73. doi:10.12775/CJFA.2017.017

Mendenhall, M. E., Weber, T. J., Arna Arnardottir, A., & Oddou, G. R. (2017). Developing global leadership competencies: A process model. In *Advances in global leadership,* 117-146. doi:10.1108/s1535-120320170000010004

Mendoza, V. D. (2014). *Measurement, tips, and errors: Making an instrument design in risk perception*. Retrieved from http://www.srmo.sagepub.com

Meng, X., & Boyd, P. (2017). The role of the project manager in relationship management. *International Journal of Project Management*, *35*(5), 717-728. doi:10.1016/j.ijproman.2017.03.001

Mesquida, A. L., & Mas, A. (2015). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 security extension. *48*.

doi:10.1016/j.cose.2014.09.003

Mikkelson, A. C., York, J. A., & Arritola, J. (2015). Communication competence, leadership behaviors, and employee outcomes in supervisor-employee relationships. *Business and Professional Communication Quarterly, 78*(3), 336-354. doi:10.1177/2329490615588542

Mishra, N., Sharma, T. K., Sharma, V., & Vimal, V. (2018). Secure framework for data security in cloud computing. In *Soft computing: Theories and Applications*, *583*, 61-71. doi:10.1007/978-981-10-5687-1_6

Mohamad, B., Nguyen, B., Melewar, T. C., & Gambetti, R. (2018). Antecedents and consequences of corporate communication management (CCM): An Agenda for future research. *The Bottom Line*. doi:10.1108/BL-09-2017-0028

Morgan, D. L. (2008). *Sample. The Sage encyclopedia of qualitative research methods*. Thousand Oaks, CA: Sage.

Morreale, S. P., Valenzano, J. M., & Bauer, J. A. (2017). Why communication education is important: A third study on the centrality of the discipline's content and pedagogy. *Communication Education*, *66*(4), 402-422. doi:10.1080/03634523.2016.1265136

Morris, D. (2017, August). Elon Musk and AI experts call for total ban on robotic weapons. *Fortune*. Retrieved from http://www.fortune.com

Moore, T. (2017). On the harms arising from the Equifax data breach of 2017. *International Journal of Critical Infrastructure Protection*, 19, 47-48. doi.10.1016/j.ijcip.2017.10.004

Morse, E. A., Raval, V., & Wingender, J. R. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective, 20*(6), 263-273. doi:10.1080/19393555.2011.611860

Mukherjee, A. (2015). Physical-Layer Security in the Internet of Things: Sensing and communication confidentiality under resource constraints. *Proceedings of the IEEE*, *103*(10), 1747–1761. doi:10.1109/JPROC.2015.2466548

Müller, R., & Turner, R. (2010). Leadership competency profiles of successful project managers. *International Journal of Project Management*, *28*(5), 437-448. doi:10.1016/j.ijproman.2009.09.003

Müller, R., Geraldi, J., & Turner, J. R. (2012). Relationships between leadership and success in different types of project complexities. *IEEE Transactions on Engineering Management*, *59*(1), 77-90. doi:10.1109/tem.2011.2114350

Murphy, D., & Murphy, R. (2013). Teaching cybersecurity: Protecting the business environment. *Proceedings of the Information Security Curriculum Development Conference, USA*, 88- 93. doi:10.1145/2528908.2528913

Nehari-Talet, A. (2014). Risk management and information technology projects. *International Journal of Digital Information and Wireless Communications, 4*(1), 1-9. doi:10.17781/P001078

Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security*, *26*(1), 10-38. doi:10.1108/ICS-07-2016-0061

Ning, H., Liu, H., & Yang, L. T. (2015). Aggregated-Proof based hierarchical

authentication scheme for the Internet of Things. *IEEE Transactions on Parallel and Distributed Systems*, *26*(3), 657–667. doi:10.1109/TPDS.2014.2311791

NIST (2018). NIST Cybersecurity Framework. Retrieved from http://www.nist.gov

NIST (2013). NIST SP 800-53r4, Joint Task Force Transformation Initiative. Retrieved from http://www.nist.gov

Northouse, P. G. (2018). *Leadership: Theory and practice*. Thousand Oaks, CA: Sage.

Nowack, M., Endrikat, J., & Guenther, E. (2011). Review of Delphi-based scenario studies: Quality and design considerations. *Technological Forecasting and Social Change*, *78*(9*)*, 1603-1615. doi:10.1016/j.techfore.2011.03.006

Ohtera, S., Kanazawa, N., Ozasa, N., Ueshima, K., & Nakayama, T. (2017). Proposal of quality indicators for cardiac rehabilitation after acute coronary syndrome in japan: A modified Delphi method and practice test. *BMJ Open, 7*(1). doi:10.1136/bmjopen-2016-013036

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management*, *42*(1), 15-29. doi:10.1016/j.im.2003.11.002

Olson, D. L., & Wu, D. D. (2017). Data mining models and enterprise risk management. In *Enterprise Risk Management Models,* 119-132. Berlin, Heidelberg: Springer.

O'Neill, M. (2014). The Internet of Things: Do more devices mean more risks? Computer Fraud & Security, 2014(1), 16–17. doi:10.1016/S1361-3723(14)70008-9

Otero, A. R. (2015). An information security control assessment methodology for organization's financial information. *International Journal of Accounting*

Information Systems, *18*, 26–45. doi:10.1016/j.accinf.2015.06.001

Paape, L., & Speklé, R. F. (2012). The adoption and design of enterprise risk management practices: An empirical study. *European Accounting Review, 21*(3), 533-564. doi:10.1080/09638180.2012.661937

Papke-Shields, K. E., & Boyer-Wright, K. M. (2017). Strategic planning characteristics applied to project management. *International Journal of Project Management*, *35*(2), 169-179. doi:10.1016/j.ijproman.2016.10.015

Pattabiraman, A., Srinivasan, S., Swaminathan, K., & Gupta, M. (2018). Fortifying corporate human wall: A Literature review of security awareness and training. In *Information Technology Risk Management and Compliance in Modern Organizations,* 142-175. doi:10.4018/978-1-5225-2604-9.ch006

Pavlou, P. A., & El Sawy, O. A. (2006). From IT leveraging competence to competitive advantage in turbulent environments: The case of new product development. *Information Systems Research*, *17*(3), 198-227. doi:10.1287/isre.1060.0094

Pathari, V., & Sonar, R. M. (2013). Deriving an information security assurance indicator at the organizational level. *Information Management & Computer Security, 21*(5), 401-419. doi:10.1108/IMCS-02-2013-0011.

Pendley, J. A. (2018). Finance and accounting professionals and cyber security awareness. *Journal of Corporate Accounting & Finance*, *29*(1), 53-58. doi:10.1002/jcaf.22291

Pereira, C., Ferreira, C., & Amaral, L. (2017). IT Value management capability enabled with COBIT 5 Framework. In *European, Mediterranean, and Middle Eastern*

Conference on Information Systems, 431-446. doi:10.1007/978-3-319-65930-5_35

Pierce, E. M., & Goldstein, J. (2018). ERM and strategic planning: A change in paradigm. *International Journal of Disclosure and Governance*, *15*(1), 51-59. doi:10.1057/s41310-018-0033-3

Pierce, J., & Newstorm, J. (2015). *The managers bookshelf*. Englewood Cliffs, NJ: Prentice Hall.

Piggin, R. (2016). Cyber security trends: What should keep CEOs awake at night. *International Journal of Critical Infrastructure Protection, 13*, 1-3. doi:10.1016/j.ijcip.2016.02.001

Pooley, J. (2017). Information security in the modern enterprise. In *Computer and Information Security Handbook ,* 3-11. doi:10.1016/B978-0-12-803843-7.00001-6

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51*, 551-567. doi:10.1016/j.im.2014.03.009

Powell, C. (2003). The Delphi technique: Myths and realities. *Journal of Advanced Nursing, 41*(4), 376-382. doi:10.1046/j.1365-2648.2003.02537.x

Rabah, K. (2018). Convergence of AI, IoT, big data and blockchain: A review. *The Lake Institute Journal*, *1*(1), 1-18. Retrieved from http://www.jnl.thelakeinstitute.org

Raguseo, E. (2018). Big data technologies: An empirical investigation on their adoption, benefits and risks for companies. *International Journal of Information*

Management, *38*(1), 187-195. doi:10.1016/j.ijinfomgt.2017.07.008

Raina, R. (2010). Timely, continuous, & credible communication & perceived organizational effectiveness. *The Indian Journal of Industrial Relations*, *46*(2), 345-359. Retrieved from http://www.jstor.org

Ramakrishna, S. P. (2015). *Enterprise compliance risk management: An essential toolkit for banks and financial services*. Hoboken, NJ: Wiley.

Reddy, K. S. M., & Sunil, K. (2017). The realm of social sentiment analysis on big data. *International Journal*, *8*(5). doi:10.26483/ijarcs.v8i5.4080

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis & Management, 30*(2), 256-286. doi:10.1002/pam.20567

Rosenberg, S. (2017). Firewalls don't stop hackers: AI might, *Wired, September*. Retrieved from http://www.wired.com

Ross, R., Katzke, S., Johnson, A., Swanson, M., & Stoneburner, G. (2008). Managing risk from information systems an organizational perspective, NIST Special Publication 800-39. Retrieved from http://www.csrc.nist.gov

Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: Issues and analysis. *International Journal of Forecasting, 15*(4), 353-375. doi:10.1016/S0169-2070(99)00018-7

Rowe, G., & Wright, G. (2011). The Delphi technique: Past, present, and futureprospects-introduction to the special issue. *Technological Forecasting and Social Change, 787*, 1487-1490. doi:10.1016/j.techfore.2011.09.002

Rubino, M., Vitolla, F., & Garzoni, A. (2017). The impact of an IT governance framework on the internal control environment. *Records Management Journal*, *27*(1), 19-41. doi:10.1108/RMJ-03-2016-0007

Sabillon, R. (2018). A practical model to perform comprehensive cyber security audits. *Enfoque UTE*, *9*(1), 127-137. doi:10.29019/enfoqueute.v9n1.214

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T.(2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53, 65–78. doi:10.1016/j.cose.2015.05.012

Sagiroglu, S., & Sinanc, D. (2013). Big data: A review. In *Collaboration Technologies and Systems (CTS), 2013 International Conference on*, 42-47. IEEE. doi**:**10.1109/CTS.2013.6567202

Salkind, N. J. (2012). *Exploring research*. Boston, MA: Pearson.

Sanchez, O. P., & Terlizzi, M. A. (2017). Cost and time project management success factors for information systems development projects. *International Journal of Project Management*, *35*(8), 1608-1626. doi:10.1016/j.ijproman.2017.09.007

Scarfò, A. (2018). The Cyber security challenges in the IoT era. In *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks,* 53-76. doi:10.1016/B978-0-12-811373-8.00003-3

Schafer, B. (2016). Compelling truth: legal protection of the infosphere against big data spills. *Phil. Trans. R. Soc. A*, *374*(2083), 20160114. doi:10.1098/rsta.2016.0114

Schuttler, R. (2010). *Laws of communication: The intersection where leadership meets employee performance*. Hoboken, NJ: John Wiley & Sons.

Schuessler, J. H., Nagy, D., Fulk, H. K., & Dearing, A. (2017). Data breach laws: Do they work?. *Journal of Applied Security Research*, *12*(4), 512-524. doi:10.1080/19361610.2017.1354275

Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill-building approach12*. West Sussex, United Kingdom: John Wiley & Sons Ltd.

Shad, M. K., & Lai, F. (2015). A conceptual framework for enterprise risk management performance measure through economic value added. *Global Business and Management Research, 7*(2), 1-11. Retrieved from http://www.gbmr.ioksp.com

Sicari, S., Rizzardi, A., Grieco, A. L., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146-164. doi:10.1016/j.comnet.2014.11.008

Sieber, J. E. (2011). Beyond informed consent. *Journal of Empirical Research on Human Research Ethics, 6*(4), 1-2. doi:10.1525/jer.2011.6.4.1

Singh, M., Halgamuge, M. N., Ekici, G., & Jayasekara, C. S. (2018). A review on security and privacy challenges of big data. In *Cognitive computing for big data systems over IoT, 14*, 175-200. doi:10.1007/978-3-319-70688-7_8

Singh, K. D. (2015). Creating your own qualitative research approach: Selecting, integrating and operationalizing philosophy, methodology and methods. *Vision, 19*(2), 132-146. doi:10.1177/0972262915575657

Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems, 37*(2). doi:10.17705/1CAIS.03702

Skorodumov, B. I., Skorodummova, O. B., & Matronina, L. F. (2015). Research of human factors in information security. *Modern Applied Science, 9*(5), 287–294. doi:10.5539/mas.v9n5p287

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education, 6*(7), 1-21. doi:10.1.1.151.8144

Skulmoski, G. J., & Hartman, F. T. (2010). Information systems project manager soft competencies: A project-phase investigation. *Project Management Journal*, *41*(1), 61-80. doi:10.1002/pmj.20146

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2015). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. doi:10.1016/j.ijinfomgt.2015.11.009

Solomon, A., & Steyn, R. (2017). Leadership style and leadership effectiveness: Does cultural intelligence moderate the relationship? *Acta Commercii*, *17*(1), 1-13. doi:10.4102/ac.v17i1.453

Steinhoff, J. C., Price, L. A., Comello, T. J., & Cocozza, T. A. (2016). Ten steps to sustainable enterprise risk management. *The Journal of Government Financial Management, 65*(2), 12-18. Retrieved from http://www.kpmg-institutes.com

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: Aninstrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems, 30*(1), 71–92. doi:10.2308/isys-51257

Stevenson, D. H., & Starkweather, J. A. (2010). PM critical competency index: IT execs

prefer soft skills. *International Journal of Project Management*, *28*(7), 663-671. doi:10.1016/j.ijproman.2009.11.008

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security*, *25*(5), 494-534. doi:10.1108/ICS-07-2016-0054

Strang, K. D., & Strang, K. D. (2017). Needs assessment of international capacity building using a Delphi technique. *World Journal of Entrepreneurship, Management and Sustainable Development*, *13*(4), 286-302. doi:10.1108/WJEMSD-02-2017-0006

Strasser, A. (2017). Delphi method variants in information systems research: Taxonomy development and application. *The Electronic Journal of Business Research Methods*, *15*(2). Retrieved from http://www.ejbrm.com

Sturm, R. E., Vera, D., & Crossan, M. (2017). The entanglement of leader character and leader competence and its impact on performance. *The Leadership Quarterly*, *28*(3), 349-366. doi:10.1016/j.leaqua.2016.11.007

Tenable. (2018). Trends in security framework adoption. Retrieved from http://www.tenable.com

Thompson, E. C. (2017). *Social media, BYOD, IoT, and Portability*. In *building a HIPAA-compliant cybersecurity program,* 211-217. Berkeley, CA: Apress.

Thomas, E., & Magilvy, J. (2011). Qualitative rigor or research validity in qualitative research. *Journal for Specialists in Pediatric Nursing 16*(2*),* 151-155. doi:10.1111/j.1744-6155.2011.00283.x

Tian, Y. (2017). Towards the development of best data security for Big Data. *Communications and Network*, *9*(04), 291. doi:10.4236/cn.2017.94020

Tofan, D. C. (2011). Information security standards. *Journal of Mobile, Embedded and Distributed Systems*, *3*(3), 128-135. Retrieved from http://www.jmeds.eu

Touhill, G. J., & Touhill, C. J. (2014). *Cybersecurity for executives: A practical guide*. Hoboken, NJ: John Wiley & Sons.

Trevelyan, E. G., & Robinson, P. N. (2015). Research paper: Delphi methodology in health research: How to do it?. *European Journal of Integrative Medicine*, *7,* 423-428. doi:10.1016/j.eujim.2015.07.002

Ulmer, R. R., Sellnow, T. L., & Seeger, M. W. (2017). *Effective crisis communication: Moving from crisis to opportunity*. Thousand Oaks, CA: Sage.

Ulrich, D., & Smallwood, N. (2005). HR's new ROI: Return on intangibles. *HumanResource Management, 44*(2), 137-142. doi:10.1002/hrm.20055

Ulrich, D., & Smallwood, N. (2012). What is talent? *Leader to Leader, 2012*(63) 55-61. doi:10.1002/ltl.20011

Undavia, J. N., Patel, A., & Patel, S. (2018). Security issues and challenges related to Big Data. In *Big Data management and the Internet of Things for improved Health Systems*, 86-101. doi:10.4018/978-1-5225-5222-2.ch006

Valentine, E. (2016). Governance of enterprise information and technology: A new core competency for boards of directors. *Journal of Risk Research*, *19*(1), 21–41. doi:10.1080/13669877.2014.940593

Vassakis, K., Petrakis, E., & Kopanakis, I. (2018). Big data analytics: Applications,

prospects and challenges. In *Mobile Big Data*, 3-20. doi:10.1007/978-3-319-67925-9_1

Veltsos, J. R. (2012). An analysis of data breach notifications as negative news. *BusinessCommunication Quarterly, 75*(2), 192-207. doi:10.1177/1080569912443081

Verma, D., Calo, S., & Cirincione, G. (2018). Distributed AI and security issues in federated environments. In *Proceedings of the workshop program of the 19th International conference on distributed computing and networking*. ACM. doi:10.1145/3170521.3170525

von der Gracht, H. A. (2012). Consensus measurement in Delphi studies: Review andimplications for future quality assurance. *Technological Forecasting and Social Change, 79*, 1525-1536. doi:10.1016/j.techfore.2012.04.013

Von Solms, B., & von Solms, R. (2018). Cybersecurity and information security–what goes where? *Information & Computer Security*, *26*(1), 2-9. doi:10.1108/ICS-04-2017-0025

Walker, R. (2013). *Winning with risk management*. Hackensack, NJ: World Scientific.

Watkins, S., & Calder, A. (2015). *IT governance: An international guide to data security and ISO 27001/ISO 27000.* London, England: Kogan Page.

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons*, *58*(6), 615–624. doi:10.1016/j.bushor.2015.06.005

Wei, Y., Samiee, S., & Lee, R. (2014). The influence of organic organizational cultures,

market responsiveness, and product strategy on firm performance in an emerging market. *Journal of The Academy Of Marketing Science*, *42*(1), 49-70. doi:10.1007/s11747-013-0337-6

Wieczorek-Kosmala, M. (2014). Risk management practices from risk maturity models perspective. *Journal for East European Management Studies*, 19(2), 133-159. Retrieved from http://www.hampp-verlag.de

Yeo, M. L., Rolland, E., Ulmer, J. R., & Patterson, R. A. (2014). Risk mitigation decisions for IT security. *ACM Transactions on Management Information Systems, 5*(1), 1-21. doi:10.1145/2576757

Yilmaz, A. K., & Flouris, T. (2017). Enterprise risk management in terms of organizational culture and its leadership and strategic management. In *Corporate risk management for international business*, 65-112. doi:10.1007/978-981-10-4266-9_3

Zhang, Z. K., Cho, M. C. Y., & Shieh, S. (2015, April). Emerging security threats and countermeasures in IoT. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, 1-6. ACM Press. doi:10.1145/2714576.2737091

Appendix A: List of Round 1 Questions

The following questions are used in this study regarding the best practices of organizational leadership, managerial competencies, information security, and risk management:

1. How effective can organizational leaders and information security managers be when following traditional risk management strategies to recover from the effect of cyberattacks?
2. What managerial competencies are needed to mitigate the risks of cyberattacks? How do these competencies compare to the competencies required to handle traditional organizational risk?
3. What are the managerial competencies that can be found by in a company that is prepared for the effect of cyberattacks, compared to the companies that are unprepared for cyberattacks?
4. What are common factors of cyberattacks that could have been prevented with the effective alignment of organizational resources such as people, process, and technology with a cyber security framework focus?
5. What are the types of expertise that should be recruited by companies to build a successful recovery program that can respond to cyberattacks?
6. What advantages or disadvantages exist in defining cyber security risk and controls frameworks?

   The reseach design contains additional details for the panel of cyber security experts and contains the first round of questioning.

Appendix B: Interview and Data Collection Protocol

Interview and data collection protocol	
Step	Description
1	IRB Approval: The data collection process will begin after getting approval from the Walden University Institutional Review Board
2	Prepare and send request for information security senior management volunteers about participating in study
3	Conduct a pilot study before the first round of data collection. Pilot studies will help to maintain the rigor of collected data
4	The survey will be emailed to participants for pilot test data collection
5	Adjust interview questions as needed according to results of pilot study
6	The survey will be emailed to participants for Round 1 data collection
7	Analysis of responses from Round 1
8	The survey will be emailed to participants for Round 2 data collection
9	Analysis of responses from Round 2
10	The survey will be emailed to participants for Round 3 data collection
11	Synthesize and analyze round 3
12	Verify responses for accuracy and data redundancy
13	Thank participants, and address any post-interview questions from participants
14	Save written interview on memory stick and create backup
15	Provide a complimentary copy of research study to each participant when study is complete and approved for distribution

Appendix C: Survey Instrument for Pilot Test

Competency list for Pilot Test

Please rate the importance of each of the listed competencies on the scale provided below using the following scale:

5 – Very Important
4 – Important
3 – Somewhat Important
2 – Somewhat Unimportant
1 – Not Important

Competencies

People competency family

Number	Competency Description	Competency Rank				
1	People and stake holder management	5	4	3	2	1
2	Goal setting and measurements	5	4	3	2	1
3	Performance management	5	4	3	2	1
4	Rewards and recognition	5	4	3	2	1
5	Training and awareness programs	5	4	3	2	1
6	Conflict resolution	5	4	3	2	1
7	Ethics and integrity	5	4	3	2	1
8	Social responsibility	5	4	3	2	1
9	Ownership and commitment	5	4	3	2	1
10	Vision and organizational strategy	5	4	3	2	1
11	Developing skilled resources	5	4	3	2	1

Process competency family

Number	Competency Description	Competency Rank				
1	Communication management at all levels	5	4	3	2	1
2	Organizational strategy alignment	5	4	3	2	1
3	Governance and regulatory compliance	5	4	3	2	1
4	Finance and budget management	5	4	3	2	1
5	Industry peer networking	5	4	3	2	1
6	Vendor management	5	4	3	2	1
7	Project management	5	4	3	2	1
8	Quality management	5	4	3	2	1
9	Customer support management	5	4	3	2	1
10	Resource planning and optimization	5	4	3	2	1
11	Risk management	5	4	3	2	1

Technology competency family

Number	Competency Description	Competency Rank				
1	Information technology and systems	5	4	3	2	1
2	Knowledge on organizational business applications	5	4	3	2	1
3	Information security domains	5	4	3	2	1
4	New and emerging technologies such as Internet of Things (IoT), AI, Big Data, and Advanced persistent threats (APTs)	5	4	3	2	1
5	Technology alignment with organizational goals	5	4	3	2	1
6	Communication and computing technology	5	4	3	2	1
7	New regulations and their impact on technology	5	4	3	2	1

Appendix D: List of Themes Collected during Literature Review

Themes Collected from Literature Review	
Themes	Literature Reference and Authors
Information security, risk management, strategy, governance, compliance, and policies	Articles on enterprise governance: (Carden et al., 2015; Cavusoglu et al., 2015; Chen et al., 2015; McFadzean et al., 2011), (Safa et al., 2015; Shad & Lai, 2015; Skorodumov, Skorodummova, & Matronina, 2015; Steinhoff et al., 2016), (Shad & Lai, 2015; Soomro et al., 2015). (Carden et al., 2015; Lundqvist, 2015). Articles on enterprise risk management competency: (Ahmed & Manab, 2016; Dionne, 2013; Lam, 2014; Lundqvist, 2015; McNeil, Frey, & Embrechts, 2015; Ramakrishna, 2015; Walker, 2013), (Andreea, 2014), (Brustbauer, 2016; Carden et al., 2015; Shad & Lai, 2015; Steinhoff, Price, Comello, & Cocozza, 2016), (Farrell & Gallagher, 2015; Grace, Leverty, Phillips, & Shimpi, 2015), (Grace et al., 2015; Hoyt & Liebenberg, 2015; Ramakrishna, 2015), (Mbowe et al., 2014; Nehari-Talet, 2014; O'Neill, 2014; Zhang et al., 2015), (Yilmaz & Flouris, 2017). Articles on information security risk management: (Archer, 2012; Ayyagari, 2012; Cheng et al., 2017), (Ayyagari, 2012), (Fenz et al., 2014), (Caldwell, 2012; Kierkegaard, 2012), (Caldwell, 2012; Romanosky et al., 2011), (Cavusoglu et al., 2015). (Holtfreter, & Harrington, 2015; Houser, 2015) (Cheng et al., 2017), (Cram et al., 2016), (Bodin et al., 2008), (Jensen, 2017), (Grahn, Westerlund, & Pulkkis, 2017; Schafer, 2016), (Kierkegaard, 2012), (McFadzean et al., 2011), (Pooley, 2017; Scarfò, 2018), (Morse et al., 2011), (Safa et al., 2015), (Soomro et al., 2015), (Chen et al., 2015; Kohnke et al., 2017). Articles on accountability: (Chaudhry et al. , 2012), (Chander, Jain, & Shankar, 2013), (Chen et al., 2015), (Hagen et al., 2008). Information Security Policies: (Hu et al., 2012; Soomro et al., 2015), (Hagen et al., 2008). Articles on information security controls: (Hagen et al., 2008), (Chang & Lin, 2007; McFadzean et al., 2011). (Cram et al., 2016), (Gordon, Loeb, & Lei, 2011; Pathari & Sonar, 2013), (McFadzean et al., 2011). McFadzean et al. (2011), (Makhlouf, 2017)
Managerial competencies, Organizational competencies and maturity of enterprise information security and risk management system	Articles on managerial competencies for information security management: (Ali, Al Balushi, Nadir, & Hussain, 2018; Kohnke et al., 2017; Pooley, 2017; Scarfò, 2018), (Anderson, & Sun, 2017; Anthony, 2017), (Ashenden, 2008; Bauer, & Bernroider, 2017; Stewart, & Jürjens, 2017), (Burns, Posey, Roberts, & Lowry, 2017), (Croft & Seemiller, 2017), (Drucker, 2016; Northouse, 2018), (Eberly, Bluhm, Guarana, Avolio, & Hannah, 2017; Ulrich & Smallwood, 2012), (Harrison, 2016; Lo et al., 2015), (Hogan, 2017; Mendenhall, Weber, Arna Arnardottir, & Oddou, 2017; Sturm, Vera, & Crossan, 2017), (Pattabiraman et al., 2018; Stewart, & Jürjens, 2017), (Pavlou & El Sawy, 2006; Wei, Samiee, & Lee, 2014)

(table continues)

Themes	Literature Reference and Authors
Managerial competencies, Organizational competencies and maturity of enterprise information security and risk management system (cont.)	Articles on communication competencies: (Anzengruber et al., 2017; Morreale, Valenzano, & Bauer, 2017), (Bachmann, 2017; Gochhayat, Giri, & Suar, 2017; Raina, 2010), (Henry, 2017). (Harrison, 2016; Lo et al., 2015; Northouse, 2018), (Mikkelson, York, & Arritola, 2015). Ulmer, Sellnow, & Seeger, 2017), (Mikkelson, York, & Arritola, 2015), (Mohamad, Nguyen, Melewar, & Gambetti, 2018; Solomon & Steyn, 2017), (Ulmer, Sellnow, & Seeger, 2017). Articles on project management competencies: (Bass, & Bass, 2009; Dulewicz & Higgs, 2005; Geoghegan & Dulewicz, 2008; Marx, 2017; Meng & Boyd, 2017), (Hughes, Rana, & Simintiras, 2017), (Kerzner & Kerzner, 2017; Müller & Turner, 2010; Müller, Geraldi, & Turner, 2012; Stevenson & Starkweather, 2010), (Maamari & Majdalani, 2017), (Meng & Boyd, 2017; Müller & Turner, 2010; Ulrich & Smallwood, 2012), (Pavlou & El Sawy, 2006; Wei et al., 2014), (Stevenson & Starkweather, 2010). (Ulrich & Smallwood, 2005).
Technical competencies	Articles on technical competencies: (Aasi et al., 2017; Cavelty, 2014; Islam, Mouratidis, & Weippl, 2014), (Astuti et al., 2017; Houser, 2015; Kushwaha, 2016; Piggin, 2016), (August, August, & Shin, 2014; Frydman, Ruiz, Heymann, César, & Miller, 2014; Ghani et al., 2014; Gisladottir et al., 2016), (Bertino & Ferrari, 2018; Choi & Lambert, 2017; Cook et al., 2018), (Dave et al., 2018), (Khari, 2018; Mishra, Sharma, Sharma, & Vimal, 2018), (Cavelty, 2014; Jing, Vasilakos, Wan, Lu, & Qiu, 2014; Kahtan, Bakar, & Nordin, 2014; Touhill, & Touhill, 2014), (Ghani et al., 2014; Jones & Rastogi, 2004), (Ghani et al., 2014; Jones & Rastogi, 2004; Khan, 2014; Touhill, & Touhill, 2014), (Dabbagh & Lee, 2014; Gisladottir et al., 2016; Kahtan et al., 2014; Mesquida & Mas, 2015), (Kushwaha, 2016), (Posey, Roberts, Lowry, & Hightower, 2014).
Skills and Expertise	Articles on emerging technology such as cloud, big data, artificial intelligence: (Andrade et al., 2018; Chio, & Freeman, 2018; Hirsch, 2018; Verma, Calo, & Cirincione, 2018), (Benson et al., 2018; Demek, Raschke, Janvrin, & Dilla, 2018; Luna & Pennock, 2018), (Bertino & Ferrari, 2018; Choi & Lambert, 2017; Undavia, Patel, & Patel, 2018), (Hess & Ludwig, 2018; Kumar et al., 2017; Lawless et al., 2017; Rosenberg, 2017), (Hirsch, 2018; Liu et al., 2018), (Olson & Wu, 2017; Tian, 2017), (Raguseo, 2018; Vassakis et al., 2018), (Singh, Halgamuge, Ekici, & Jayasekara, 2018; Undavia et al., 2018), (Verma et al., 2018). (Amaral, Tiburski, de Matos, & Hessel, 2015; Mashal et al., 2015), (Benson et al., 2018; Demek et al., 2018; Luna & Pennock, 2018), (Cirani, Ferrari, & Veltri, 2013; Ning et al., 2015; Sicari et al., 2015), (Gaff, 2015; Thompson, 2017), (Hosseinian-Far et al., 2018). (Jayakumar et al., 2016), (Kumar & Singh, 2015; Thompson, 2017), (Kumar & Singh, 2015; Thompson, 2017), (Lee & Lee, 2015; Weinberg et al., 2015; Hosseinian-Far et al., 2018), (Lin et al, 2018; Martin, Tomkinson, & Scott, 2017), (Sicari et al., 2015)
Information Security Standards and Frameworks	Information Security Standards and Frameworks (Ahmad & Mohammad, 2012; Zhang et al., 2015; Murphy & Murphy, 2013), (Barafort, Mesquida, & Mas, 2017; Leszczyna, 2018; Von Solms & von Solms, 2018), (Dedeke, 2017; NIST, 2018; Von Solms & von Solms, 2018; Watkins & Calder, 2015), (Ross, Katzke, Johnson, Swanson, & Stoneburner, 2008; Tenable, 2018), (Yeo, Rolland, Ulmer, & Patterson, 2014), (Zhang et al., 2015; Steinhoff et al., 2016; Shad & Lai, 2015; Soomro et al., 2015).

Appendix E: Round 2 Questionnaire

This questionnaire contains the themes analyzed from the data submitted by the experts in this study. In this round, you will evaluate the importance of the statement being made in regards to the question being asked. Please rate each statement by entering a number in the box next to it. The Likert scale being used is 5 = strongly agree, 4 = agree, 3 = slightly agree, 2 = disagree, 1 = strongly disagree.

	Question 1: How effective can organizational leaders and information security managers be when following traditional risk management strategies to recover from the effect of cyberattacks?	Rate
1	Traditional risk management strategies & plans need to be updated to account for the changing technical and business environment.	
2	The risk impact can be managed efficiently, and recovery can begin with minimal impact on organization. If organizational leadership follows the strategy, standards, right policies, plans, and procedures according to the plan before and after an attack,	
3	The traditional risk management strategies used by organizational leaders and information security managers can be quite effective, if matured and tested risk management program would have already considered to mitigate risk if ever a cyberattack occurs	
4	Traditional Risk Management methods alone will not be effective if the leaders and security managers are following tradition risk management strategies to recover from the effects of Cyberattacks.	
5	Organizations need to conduct continuous monitoring and risk assessments and implement required security controls to address security threats and vulnerabilities.	
6	Organizational leaders, information stewards and security managers must adapt to tools and processes that will better equip the team, so they can stay ahead of the curve in the whole spectrum of threat and risk management.	
7	With increased vulnerability from all directions, leaders must have people, processes and technologies in place to proactively monitor, identify, diagnose, fix, and prevent cyberattacks.	
8	Traditional risk management strategies does not always address “cyberattacks” or “cyber security” and Leadership should continuously update their Risk Management strategy to address emerging cyber risks from new and emerging business processes and technologies	
9	Traditional risk management strategies may not be effective in the digital age due to the increased use of Open source code and the Cloud to develop/host applications/services containing sensitive data	
10	The principles of Information Security remain the same regardless of the change in technology. However, the speed, agility and complexity which has increased due to emerging technologies such as Cloud, IoT, Blockchain, self-driving cars, industrial automation, Blockchain/Cryptocurrency, Smart cities, etc.	
11	Need a major transformation in terms of security regulations, standards, policies, procedures, controls, and monitoring to address risks from emerging technologies	
12	Organizations need to embrace automation, AI, and analytics in order to be successful in prevention, detection and recovering from Cyber Attacks.	
13	Traditional risk management strategies will need to be tailored to address the dynamically changing threat and regulatory landscape	
14	Traditional risk management strategies are no longer effective in today’s dynamic ecosystems and landscapes with emerging cloud based infrastructure and technologies.	

	Question 2: What managerial competencies are needed to mitigate the risks of cyberattacks? How do these competencies compare to the competencies required to handle traditional organizational risk?	Rate
1	Equanimity in the face of a crisis, emotional intelligence, detail orientedness, intimate awareness of company's IT landscape and technologies, leadership qualities, and resourcefulness are needed as competencies.	
2	Deep understanding of business processes, digital assets such as applications, data, infrastructure, and people who support them and their potential vulnerabilities	
3	The ability to monitor and assess what is happening in the cybersecurity and cyber-threat world is essential due to the increase of technology. Mapping them to one's organization's risk processes and determining the gaps on a timely basis will be a best practice.	
4	As a manager, hacks are inevitable with the increased number of digital services. One has to manage the team and allow them to employ out of the box ideas to identify the new emerging threats and come up with innovative deterrent measures.	
5	Educate and train his/her teams and non-technical stakeholders on the risk management lifecycle and processes	
6	Competency includes the understanding of risk management programs within the organization and an understanding of risk mitigation options relevant to the respective area of responsibilities.	
7	Currently, organizations have not made cyber-centric competency a priority.	
8	Executive management, senior, and middle management should include cyber-security and risk management focused leadership competencies in their leadership to mitigate emerging cyber risks.	
9	Management should have an open and agile mindset to be able to adopt the effective ways of mitigating the risks of cyberattacks.	
10	Context setting, alignment at the leadership level for priorities, good program management, time management, and conflict resolution are all important for any risk management program	
11	Communication is an important, technical expertise goes a long way in helping the team to mitigate risks.	
12	Suddenly there has been a major transformation to cloud based systems, IoT adoption, mobility, etc. which have almost made traditional security controls ineffective.	
13	There is a necessity for modern leaders to help securely adopt emerging technology, understand the evolving regulatory landscape, and increase cross border transfers.	
14	Risk management methodology/frameworks need to be re-aligned with new threat landscape which did not exist in traditional environments.	
15	For an effective security management, there must be balance between emerging technologies, understanding the management and financial planning requirements, and understanding the big picture of how a new technology based eco-system will function.	
16	Mitigation of cyber attack risks requires a broader range of managerial competencies that traditional organizational risk due to the complexity of technologies involved. A management team of technical representation, financial and business representation is required. In traditional organizational risk, the technical representation is not likely needed.	
	Question 3: What are the managerial competencies that can be found by in a company that is prepared for the effect of cyberattacks, compared to the companies that are unprepared for cyberattacks?	Rate
1	Managers must have competencies such as superior communication, problem solving, teamwork, capability to define and implement processes, and the maturity to mentor and motivate the team to achieve individual, team and organizational goals.	
2	Leadership should demonstrate open mindedness, lack of bias, and maturity to provide and implement risk mitigation plans.	

3	Cybersecurity managers must have well-tested standards, frameworks, and industry best practices in place to address the known and emerging vulnerabilities in order to protect the organization from cyber threats and risk.	
4	Transparency amongst the management in handling cyberattacks is essential.	
5	Proper understanding of the risk management program within the organization is important when dealing with the impact of threats on a business.	
6	Managers should be required to have a proper understanding of risk management program within the organization.	
7	A well prepared leadership will have managerial competencies that place a priority on identifying threats. Such management also puts their organization's mission critical information and data security as their top most priority and will align their IT spending with the right objectives.	
8	A well trained and experienced leadership will have a robust disaster recovery plan and business continuity plan in place and will diligently conduct simulation drills throughout the organization to carry out the recovery tasks in case an incident occurs.	
9	An unprepared organization or leadership on the other hand will be unaware of the complex and changing threat landscape and may not have the right people, processes or technologies in place in the event of a cyberattack.	
10	Mangers must have an overall view of the organization assets, policies, and procedures. Managers also need to have a comprehensive "security policy" which has all the threat vectors considered.	
11	The most important security element is effective communication with C-Suite to ensure enough resources are allocated for cybersecurity resilience.	
12	Being aware of security protocols will ensure behaviors that protect the data of a company.	
13	A technical background is required to be able to make decisions and communicate to C level executives and external regulators	
	Question 4: What are common factors of cyberattacks that could have been prevented with the effective alignment of organizational resources such as people, process, and technology with a cyber security framework focus?	Rate
1	The surprise element of the cyberattack can be a major threat to the company in terms of direct and indirect consequences.	
2	The impact of a surprise attack can be addressed by proactively building well trained incident response team to reduce the detection, recovery, and mitigation	
3	The right governance structure consists of a core group with responsibilities for strategy, design and implementation of cybersecurity programs and policies.	
4	The effective use of processes and training programs – the company must introduce strong training programs that ensure team members are aware of the company's business processes, infrastructure, and critical digital assets, as well as cybersecurity vulnerabilities, threats, risks, and necessary controls for risk mitigation.	
5	Having the right group of resources in various teams with required expertise and clear roles and responsibilities, industry recognized cybersecurity frameworks, regulatory standards, well-defined processes with global best practices and periodic review of processes as part of risk management and standardized adoption of technologies and technical solutions within the company can help mitigate threats.	
6	Lack of coordination and senior leadership support, weak access controls, lack of encryption for sensitive data, non application of patches, insecure remote communication, ineffective recovery processes, poor user security awareness, lack of layered defense approach are known common factors responsible for cyber attacks on any organization	
7	With the effective alignment of organizational resources such as people, process, and technology with a cyber security framework focus, an effective information security awareness and training, strong governance measures to define, implement and manage	

	policies and processes, properly architected, implemented and managed technology infrastructure would be key to avoid cyberattacks.	
8	Social Engineering attack, Social media attack and Malware attacks must have specialized security controls.	
9	Cyber attacks that are triggered through phishing, denial-of-service (DOS), general virus/malware and other modes can be prevented with having the right controls in place. In general, human factor, compliance and policy related aspects, external/cloud, BYOD (Bring your own device) related factors can be effectively prevented with a well devised and implemented cyber security framework.	
10	Cyberattacks can be internal or external. A process must be kept in place to stop the attacks or prevent it. The manager needs to make sure the team follows process and has the required ongoing training to stay current in trends of technology, attacks and tools	
11	Lack of Security Awareness and enablement of organizational users to acknowledge security as a shared responsibility, Not defining KPI's which help in measurement of Security control effectiveness, insufficient allocation of security controls and define process for prevention, detection and response to cyber attacks, failure to identify alternate mechanism how business can continue during response/recovery of cyber security attacks.	
12	If more effective alignment existed across the organization, common factors of cyberattacks could be reduced. Some of these negative factors include: Not prioritizing and allocating required resources to security projects	
	Question 5: What are the types of expertise that should be recruited by companies to build a successful recovery program that can respond to cyberattacks?	Rate
1	The best qualities of a successful candidate include being a team player, being detail oriented, having security domain expertise, and programming expertise.	
2	It all starts with recruiting the right people who are competitive and have the right background in the industry. This involves relevant security certifications, experience in effectively implementing mitigation plans, experience in effectively handling a cyberattack, and the ability to develop short term and long term plans to address the attack.	
3	Teams comprising of employees with competent expertise will always play a pivotal role during any crisis. Employees with clearly defined roles and responsibilities will ensure an effective tandem at work during crisis.	
4	Crisis Managers/Incident Handling Managers/BCP & DR Managers must have competencies such Network and IT infrastructure, Cloud, Enterprise Architects and Application architecture, Security infrastructure, IAM, Log analysis, Forensic, and leadership and communication to mitigate the risk from cyberattacks.	
5	The types of expertise that should be recruited by companies to build a successful recovery program would include · Risk Management · Business Continuity and Disaster recovery · Cyber Security Assessment · Regulatory compliance and cyber security frameworks · System security architecting, implementation, management and monitoring · System security vulnerabilities testing · Governance, Risk and Compliance	
6	Solid understanding of IT fundamentals, sufficient coding skills, understanding of architecture, administration and operating system are required from candidates.	
7	For a successful recovery program, one must recruit people with expertise covering business continuity planning, behavioral change management, malware detection, IT forensics, risk analysis and mitigation, threat modeling, and Cloud security.	
8	Security Operations Center SMEs who can do Threat Hunting, Incident response, Forensic	

	analysis, Threat Intelligence are essential to the performance of a company.	
9	Skilled employees should have the right certifications in security, coding skills, architecture and operational expertise, and excellent oral and written skills.	
10	Investment in domain specialization for the core team which includes incident response, network security, etc, and Ethical Hackers. All these roles can handle different aspects of security issues.	
11	Unfortunately a recovery program often results in a loss of data. Management should include technical knowledge and effective communication in their response to crisis.	
	Question 6: What advantages or disadvantages exist in defining cyber security risk and controls frameworks?	Rate
1	Frameworks keep everybody on the same page as they comprehensively cover all aspects of the cyber security risks.	
2	Various frameworks are in practice to guide the industry. Frameworks help to understand systems and recognize risks in order to adopt the customized risk management methodologies to minimize the risk for a better ROI and measureable effectiveness.	
3	Frameworks are guiding practices, their intentions vary from country to country, industry to industry, one should not blindly follow them.	
4	Identification of Risks in a timely manner per type of asset and their classification. • Assist in Risk Assessment • Useful for Risk Mitigation and deriving Residual Risk • Real Time Risk Monitoring and Reporting	
5	A traditional approach may slow down countermeasures against sophisticated APT's and socially engineered attacks.	
6	Cyber security frameworks provide organizations with an opportunity to identify areas where existing processes may be strengthened, or where new processes can be implemented. · Frameworks would help to guide key decision points about risk management activities through the various levels of an organization from senior executives, to business and process level, and implementation and operations as well · Frameworks help to align with various regulatory compliance requirements	
7	Lack of resources to manage the framework implementation and maintenance would cause a disadvantage for the system.	
8	The cyber-security framework should include the core functions to identify, protect, detect, respond and recover . It has to be a comprehensive framework that will enable organization to meet the security challenges faced today.	
9	The advantages of having a well-defined cyber security risk and controls framework is that it equates to one's ability to proactively monitor threats and recover attacks in a seamless and effective manner, thus minimizing the overall business loss.	
10	Frameworks provide great advantages. One big disadvantage is they may be too broad for an organization & costly to implement verbatim. So we may need to modify the framework to suite our needs..	
11	Using controls framework help organizations to be clear in what cyber security risks they are trying to prevent and help ensure everyone within the organization is on the same page to jointly identify, prevent, detect, respond and recover from cyber security incidents and associated risks	
12	There are more advantages than disadvantages to having cyber security risk and control framework in place Frameworks help the organization to have controls in place to stop attacks and provides management a sense of security both internally and externally.	
13	Cyber Security Frameworks allow for structured implementation of controls and allow to comprehensively covering all aspects of the cyber security risks. Align with industry best practices which clients/partners can be assured of having verifiable minimum security controls in place.	

14	However frameworks have certain disadvantages. Efficiency of a framework depends on how an organization has interpreted security controls and if there is room for flexibility to enhance controls for any modernization/transformation initiatives. Any rigidity can hinder innovation, maturity and adoption of emerging technologies.
15	The advantages are in discussing, documenting and defining frameworks. If more material exists, if more scenarios are reviewed and documented, there will be a greater awareness to cyber security risks and controls.

Appendix F: Round 3 Questionnaire

In this last round, please evaluate the ***IMPORTANCE*** of the statement being made in regards to how it would influence the organization. Please rate each statement by entering a number in the box next to it. The Likert scale being used is 5 = Very Important, 4 = Important, 3 = Moderately Important, 2 = Slightly Important, 1 = Not important.

	Question 1: How effective can organizational leaders and information security managers be when following traditional risk management strategies to recover from the effect of cyberattacks?	Rank
1	The enterprise cyber risk can be minimized if organizational leaders follow the strategy, standards, policies, plans, and procedures according to the information security management plan before and after an attack.	
2	Organizations need to conduct continuous monitoring and risk assessments and implement required security controls to address cyber threats, vulnerabilities, and cyber risks.	
3	Organizational leaders and security managers must adapt to tools and processes that will better equip the team, such that they can stay ahead of the issues in cyber threats, vulnerabilities, and cyber risks.	
4	With increased cyber threats, vulnerabilities, and cyber risks, leaders must have people, processes and technologies in place to proactively monitor, identify, diagnose, fix, and prevent cyberattacks.	
5	Leadership should frequently update their risk management strategy to address current and emerging cyber threats, vulnerabilities, and cyber risks.	
6	The principles of information security remain the same regardless of the change in technology. However, the speed and agility must increase to address persistent threats from emerging technologies such as Cloud, IoT, Blockchain, self-driving cars, industrial automation, Blockchain/Cryptocurrency, Smart cities, etc.	
7	Organizations need to embrace new technologies such as automation, artificial intelligence, and analytics to be successful in the prevention, detection, and recovery from cyberattacks.	
8	Risk management strategies must be tailored to address the dynamically changing cyber threats, vulnerabilities, and cyber risks.	
	Question 2: What managerial competencies are needed to mitigate the risks of cyberattacks?	Rank
1	Leaders need to have emotional intelligence to handle crisis situations regarding cyberattacks.	
2	Leaders must have an understanding of the organization related regulatory standards and requirements to support cyber risk management efforts with required resources such as people, process, and technology.	
3	The ability to monitor and assess what is happening in the cybersecurity is essential due to the increased use of technology.	
4	To bring awareness, leaders must support internal training and awareness programs on current and emerging cyber threats, vulnerabilities, and cyber risks to all employees.	
5	Cybersecurity competency includes the understanding of cyber risk management programs within the organization and an understanding of cyber risk mitigation options relevant to the respective area of responsibilities.	
6	Executive management, senior, and middle management should include cybersecurity and risk management focused leadership competencies in their leadership to mitigate current and emerging cyber threats, vulnerabilities, and cyber risks.	

7	Management needs to be able to adopt effective ways of mitigating the risks of cyberattacks.	
8	Communication is an essential skill for leaders to understand and convey current and emerging cyber threats, vulnerabilities, and cyber risks to stakeholders.	
9	Leaders need to adopt emerging technologies and understand the evolving regulatory policies to manage current and emerging cyber threats, vulnerabilities, and cyber risks.	
10	Risk management frameworks need to be re-aligned with the current and emerging vulnerabilities, cyber threats, and cyber risks	
11	For effective security management of risk from emerging technologies, there must be a process for evaluating and assessing risk from emerging technologies and risk mitigation controls.	
12	Leaders must have an understanding of the organization's IT infrastructure, applications, systems, and data of the organization to support cyber risk management efforts with required resources.	
	Question 3: What are the managerial competencies that can be found in a company that is prepared for the effect of cyberattacks, compared to the companies that are unprepared for cyberattacks?	Rank
1	Managers must have competencies such as effective communication, problem solving, teamwork, capability to define and implement processes, and the maturity to mentor and motivate individuals and teams to achieve organizational goals.	
2	Cybersecurity managers must have relevant experience on industry specific regulatory and information security standards, frameworks, and industry best practices in place to address the current and emerging cyber threats, vulnerabilities, and cyber risks.	
3	Proper understanding of risk management programs within the organization is important when addressing the effects of current and emerging cyber threats, vulnerabilities, and cyber risks.	
4	A well-prepared leadership will have managerial competencies that place a priority on identifying current and emerging cyber threats, vulnerabilities, and cyber risks. Such management also puts their organization's mission critical information and data security as their top most priority and will align their IT spending to meet organization objectives.	
5	A well trained and experienced leadership will have a tested and verified recovery plan in place in case of a cyberattack	
6	Managers must have an overall view of the organization, people, process, and technology to manage current and emerging vulnerabilities, cyber threats, and cyber risks to an acceptable level in the organization	
7	The most important security element is effective communication with senior leadership to ensure enough resources are allocated for addressing current and emerging cyber threats, vulnerabilities, and cyber risks.	
8	The cybersecurity background and knowledge of senior leaders will help the organization to make decisions, implement required security controls and communicate with stakeholders.	
9	The most important and critical success factor in cybersecurity management is the effective communication with senior leadership to ensure enough resources are allocated for cybersecurity management programs.	
	Question 4: What are common factors of cyberattacks that could have been prevented with the effective alignment of organizational resources such as people, process, and technology with a cyber security framework focus?	Rank
1	The effects of a surprise attack can be addressed by proactively building well-trained incident response teams to identify, protect, detect, respond, and recover from cyberattacks	
2	The right governance structure should be in place with a core group with responsibilities for strategy, design, and implementation of cybersecurity programs.	

3	Leaders must introduce strong training programs that ensure cybersecurity management team members are aware of the company's people, processes, and technology.	
4	Having the right group of resources in various teams with the required expertise and clear roles and responsibilities, within the company can help to mitigate current and emerging cyber threats, vulnerabilities, and cyber risks.	
5	Having the industry recognized cybersecurity frameworks, regulatory standards, and policies within the company can help mitigate current and emerging cyber threats, vulnerabilities, and cyber risks.	
6	Senior leadership support is a well-known known factor for mitigating risk from cyberattacks.	
7	Coordination between various teams responsible for cybersecurity, strong security controls, and encryption for sensitive data are known factors for mitigating risk from cyberattacks.	
8	Application of security patches, secure remote communication, effective recovery processes, and user security awareness are known factors for mitigating risk from cyberattacks.	
9	A defense in-depth approach is a known strategy for mitigating cyber risks from cyberattacks.	
10	The effective alignment of organizational resources such as people, process, and technology with a cybersecurity framework focus are essential in mitigating cyber risks from cyberattacks.	
11	Social engineering, social media, and malware attacks must be addressed by enforcing training and awareness programs, along with specialized security controls.	
12	Cyberattacks that are triggered through phishing, denial-of-service (DOS), general virus/malware and other modes can be prevented by having the right security controls in place.	
13	Cyberattacks can be internal or external. A process must be kept in place to mitigate or prevent cyberattacks.	
14	Leaders need to make sure the team follows established processes and has the required training to stay current on trends in technology and cybersecurity.	
15	It is the shared responsibility of leadership, employees, and business partners to build security awareness and implement security protocols.	
16	Common factors of cyberattacks could be reduced by effective alignment of resources such as people, process, and technology.	
	Question 5: What are the types of expertise that are needed by companies to build a successful recovery program that can respond to cyberattacks?	Rank
1	The best qualities of a successful candidate include being a team player, being detail oriented, having security domain expertise, and having programming expertise.	
2	Cybersecurity starts with recruiting the right people who have the right background in the industry to develop short term and long term plans to address current and emerging cyber threats, vulnerabilities, and cyber risks.	
3	The relevant security certifications, experience in effectively implementing mitigation plans, experience in effectively handling a cyberattack, and the ability to develop short term and long term plans to address the cyberattack.	
4	Teams comprising of employees with cyber security expertise will always play a pivotal role during and after cyberattacks.	
5	Crisis managers/incident handling managers/BCP & DR managers must have a resources with competencies such as IT infrastructure, cloud, enterprise architecture, application architecture, security infrastructure, IAM, log analysis, forensic, and leadership and communication to mitigate the risk from cyberattacks.	
6	The types of needed expertise to build a successful recovery program include:	

	· Risk management · Business continuity and disaster recovery · Cybersecurity assessment · Regulatory compliance and cybersecurity frameworks · System security architecting, implementation, management and monitoring · System security vulnerabilities testing · Governance, risk and compliance	
7	Solid understanding of IT fundamentals, computer programming skills, understanding of data architecture, system administration are required from candidates.	
8	For a successful recovery program, leaders must recruit people with expertise covering business continuity planning, change management, malware detection, IT forensics, risk analysis and mitigation, threat modeling, and cloud security.	
9	Security operations center SMEs that can do threat hunting, incident response, forensic analysis, and threat intelligence are essential to the operation and business continuity of a company.	
10	Skilled employees should have the right certifications in security, coding skills, architecture and operational expertise, and excellent oral and written skills.	
11	Investment in domain specialization for the core team should include incident response, network security, and ethical hackers. All of these roles can handle different aspects of security issues.	
12	Management competencies should include technical knowledge and effective communication in their response to crisis.	
	Question 6: What advantages or disadvantages exist in defining cybersecurity risk and controls frameworks?	Rank
1	Frameworks keep everybody informed as they comprehensively cover all aspects of cybersecurity risks.	
2	Various frameworks are in practice to guide the industry. Frameworks help to understand systems and recognize risks to adopt customized risk management methodologies to minimize risks.	
3	Cybersecurity frameworks provide organizations with an opportunity to identify areas where existing processes may be strengthened or where new processes can be implemented.	
4	Lack of resources to manage the framework implementation and maintenance may increase threats, vulnerabilities, and risk to the organization.	
5	The cybersecurity framework should include the governance, competencies, challenges, and best practices to identify, protect, detect, respond and recover.	
6	The advantages of having a well-defined cybersecurity risk and controls framework is that it equates to the ability to proactively monitor threats and recover from attacks in an effective manner, thus minimizing the overall business loss.	
7	Using controls framework will help organizations to be clear on what cybersecurity risks that they are trying to prevent and help to minimize associated risks.	
8	Using controls framework will help organizations to identify, prevent, detect, respond, and recover from cyber threats, vulnerabilities, and cyber risks.	
9	Using cybersecurity frameworks will help in the implementation of controls and allow for comprehensive coverage of all aspects of cybersecurity risks.	
10	Advantages in using security frameworks are in risk assessments, selection of controls and implementation to respond and recover from cyber threats, vulnerabilities, and cyber risks.	
11	The security framework has to be comprehensive to enable the organization to handle current and emerging cyber threats, vulnerabilities, and cyber risks.	