Walden University
ScholarWorks

Walden Dissertations and Doctoral Studies

Walden Dissertations and Doctoral Studies Collection

2021

Maritime Cybersecurity Strategies for Information Technology Specialists

Angela Mizelle Griffin
Walden University

Follow this and additional works at: https://scholarworks.waldenu.edu/dissertations

 Part of the Databases and Information Systems Commons

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Angela Griffin

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. Jodine Burchell, Committee Chairperson, Information Technology Faculty
Dr. Cheryl Waters, Committee Member, Information Technology Faculty
Dr. Bob Duhainy, University Reviewer, Information Technology Faculty

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

Walden University
2021

Abstract

Maritime Cybersecurity Strategies for Information Technology Specialists

by

Angela Griffin

MS, American InterContinental University, 2006

BS, Elizabeth City State University, 2001

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2021

Abstract

Dependence on digital technology increases cyber-related risks for maritime industries. As a result, the U.S. Coast Guard network is challenged with maritime cybersecurity, both economically and for national security. Grounded in the general systems theory, the purpose of this multiple case study was to explore strategies information technology (IT) specialists use to implement standard practices for ensuring cyber security. The participants included six IT specialists who have successfully implemented standard practices for maritime organizations in Virginia and West Virginia. Data were collected from individual semistructured interviews and a review of 12 external organizational documents available to the public from IT specialists. The data were analyzed using thematic analysis, and three major themes emerged (a) adhering to network compliance, (b) promoting adopting cybersecurity standards and best practices, and (c) enhancing cybersecurity awareness and policies. One recommendation is for organizations to provide a strategic plan, incorporate network segmentation, and adopt crucial strategies as best practices. The implications for positive social change include the potential reduction of unauthorized exposure to maritime industry operations, improved cybersecurity awareness to better cyber-related practices, and privacy protections for the targeted population.

Maritime Cybersecurity Strategies for Information Technology Specialists

by

Angela Griffin

MS, American InterContinental University, 2006

BS, Elizabeth City State University, 2001

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2021

Dedication

I dedicate this doctoral study to my family. My late mother, Margie, played a significant role in the person I am today. My two sons, Rafeal Jr. and Ayden are why I continue to grow in education and my professional career. I want them to never give up on their hopes and dreams and continue to prevail in life. My sisters, Margita and Sherrick, continuously gave me support and always asked about my progress during this journey. I love them more than they know.

Acknowledgments

I want to thank my husband, Rafeal Sr., and my children, Rafeal Jr. and Ayden, for their moral support and understanding throughout my studies. I want to thank my sister Margita for always asking me about my paper and encouraging me to continue to move forward. I am also grateful to my committee chair, Dr. Jodine Burchell. She has been the most outstanding chair. She was always willing to meet with me and guide me in the right direction. Dr. Cheryl Waters and Dr. Bob Duhainy were the other members of my committee; I want to express my gratitude for their support.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

The maritime industry uses 90% of global world trade for buying and consuming goods (Jacq et al., 2018). According to Trimble et al. (2017), various risks are associated with the port industry. Svilicic et al. (2019) implied that maritime industries rely on computing and communication technologies and the need for cyber risk management of critical systems. However, little attention has been focused on the standards or regulations. Network cyber-related attacks and threats often occur, and most are unreported or undetected (Zăgan et al., 2018). According to Zhao et al. (2017), network attacks can cause additional costs, delays, and disruptions during the maritime industry's transportation process. In 2019, the U.S. Coast Guard (USCG) informed the maritime industry of an incident involving a ransomware attack that caused a maritime transportation security facility to shut down for 30 hours (Johnson, 2020).

Cybersecurity has represented a risk to the maritime industry since September 11, 2001, which has caused concern with the U.S. Congress (2006). As a result, the USCG issued a maritime cybersecurity strategy to identify standard practices in 2015 to be conducted by the Command, Control, Communication, Computers, and Information Technology (C4IT) service center information technology (IT) specialists (Zukunft, 2015). According to Oltsik et al. (2017), the federal government struggles with appealing to cybersecurity professionals for high-demand technical jobs such as cybersecurity. Also, the USCG identified workforce requirements had not been aligned with skills and

abilities to meet mission needs as of 2016, indicating that USCG standard practices have not been applied for maritime cybersecurity (Anderson, 2020).

Problem Statement

The increased dependence on digital technology has increased the cyber-related risks for maritime industries. The USCG network has been challenged with maritime cybersecurity both economically and in national security (Kessler et al., 2018). Lee and Wogan (2018) reported that 64% of maritime IT specialists are unprepared to handle cyber-related threats. The general IT problem is that USCG standard practices have not been applied adequately to protect the maritime industry from cyber threats on the USCG network. The specific IT problem is that some IT specialists lack strategies to implement the USCG standard practices needed to secure the USCG network for maritime industries from cyber-related threats.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the different strategies IT specialists have used to implement the USCG standard practices to secure the USCG network for maritime industries from cyber-related threats. The study population was IT specialists who have applied USCG standard practices for maritime sectors to protect the USCG network from cyber-related threats from two IT departments in the C4IT center. The IT specialists are in USCG's Operations Support Center (OSC) in Virginia and West Virginia. Possible implications for positive social change include the potential reduction of unauthorized exposure to maritime industry operations, improved

cybersecurity awareness to better cyber-related practices, and privacy protections for the targeted population.

Nature of the Study

The most appropriate method for this study was the qualitative method. The qualitative method involves in-depth exploration and perspectives of individuals while accounting for real-world conditions (Baškarada, 2014). Using the qualitative method in this study was appropriate because of the need to understand the challenges associated with creating the standard practices for cyber-related factors and examining the consequences of the strategies' success or failure. In the quantitative method, a researcher uses objective data measurements, such as survey instruments, predetermined hypotheses as a basis for the problem statement, and statistical techniques (Corner, 2002). A quantitative method was not appropriate for this study because a predetermined hypothesis and statistical data were not needed to explore why this IT problem occurs. A mixed-method methodology allows researchers to examine a phenomenon using quantitative and qualitative data (McKusker & Gunaydin, 2014). The mixed-method methodology was not appropriate for this study because quantitative statistical data were not suitable in conjunction with qualitative data to explore the IT phenomenon in this study. The qualitative method allowed the data collection process to explore the strategies used to implement USCG standard practices and provide the necessary context while exploring the phenomena into the USCG network's challenges to secure the USCG network for maritime from cyber-related threats.

The most appropriate design for this study was a multiple case study. A multiple case study design allows a researcher to explore a complex IT phenomenon in the real-world context of various bounded systems (Weishapl et al., 2018). A multiple case study was appropriate because the IT specialists' strategies were explored within the bounds of the C4IT and OSC departments of the USCG. Phenomenology is used to study the human experience and applies to the lived experiences of the IT phenomenon (Du Plessis, 2018). Phenomenology was not an appropriate design for this study because the researcher focused on the organization's strategy of implementing USCG standard practices, not the human experience or perceptions of the IT phenomenon. An ethnographic design would have focused on studying culture by gaining a different perspective of individuals part of that culture (Hanson et al., 2011). Ethnography was inappropriate for this study because it would not focus on participants as part of a culture and capture only their perspectives on the IT phenomenon. The multiple case study design was appropriate because it allowed the researcher to explore the strategies used by numerous IT specialists employed in the USCG organization at two different locations.

Research Question

What strategies do IT specialists use to implement standard practices to secure the USCG network for maritime cybersecurity from cyber-related threats?

Interview Questions

1. What methods and tools have IT specialists used to prevent cyber-related threats from the federal organizations' network for maritime?

2. How would those methods and tools secure the federal organizations' network for maritime security successfully?
3. What methods have IT specialists used that have failed to prevent cyber-related threats from the federal organizations' network for maritime?
4. What challenges have IT specialists faced in implementing strategies?
5. What metrics do IT specialists use to assess the vulnerabilities or ensure the federal organizations' network is secure for maritime?
6. As an IT specialist, what is your role if a breach or threat is identified?
7. What type of training or certifications has been identified through cybersecurity awareness policies at your organization?
8. What additional information, processes, or documentation would you like to provide that may help in this research study?

Conceptual Framework

In 1937, biologist Ludwig von Bertalanffy established general systems theory (GST; Pouvreau, 2014). Von Bertalanffy (1972) introduced GST as a way of thinking or an approach to studying a complex system. According to von Bertalanffy (1972), a system is the interaction of related instruments influencing the cooperation of all parts. Fundamental principles of this theory are (a) objects, the variables within the system; (b) the attributes of the system and its objects; (c) the interrelationship between objects in a network; and (d) the existence of a system within an environment (von Bertalanffy, 1972). Organizational, social, human, and technology are the subsystems that form the interrelationship for the overall system (von Bertalanffy, 1972).

For this study, the USCG network was the overall system. IT specialists, infrastructure, strategies, and the USCG standard practices work together as the system's internal components to secure the USCG network for maritime cybersecurity from cyber-related threats. Blokland and Reniers (2020) noted that GST is an essential foundation for security and safety. According to Ahokas et al. (2017), the growing pressure for countermeasures against cyber-related threats for maritime has policymakers adopting general cybersecurity strategies. This growing pressure for countermeasures against cyber-related threats affects the maritime cybersecurity for the USCG network. The connections between the IT specialists, infrastructure, policies, and USCG standard practices are essential for the IT specialists to secure the USCG network for maritime cybersecurity adequately.

Definition of Terms

Cyber-related threat: An attempt to damage, disrupt, or gain unauthorized access to a computer or electronic communications network (Zăgan et al., 2018).

Information technology (IT) specialist: An individual whose work involves all IT activities for a federal government organization that ensures confidentiality, integrity, and availability of the system, network, and data (Amiri et al., 2018).

Maritime industry: Goods and cargo are transported using ships across waterways, such as ocean and sea (Greiman, 2019).

Assumptions, Limitations, and Delimitations

Assumptions are thoughts, expectations, or beliefs that have not been proven but are necessary to conduct research (Marshall & Rossman, 2016). Uprichard and Dawney

(2019) noted that assumptions are concepts imposed on a study accepted as accurate. In this study, I assumed the IT specialists documented standard practice to protect the USCG network systems. I also assumed the IT specialist experiences would reflect in a manner that would give the strategies needed to implement USCG practices while providing accurate and unbiased responses to the interview questions. The third assumption was that the IT specialists representing the targeted population were knowledgeable about the maritime industry, cybersecurity, and USCG standard practices.

Limitations are potential weaknesses within a study beyond researchers' control and may result in additional research (Hall & Martin, 2019). Greener (2018) implied that limitations might impact the validity and disrupt the findings' trustworthiness. The first limitation of this study was that the research was limited to two locations for participation with the population focused on the OSC of USCG in Virginia and West Virginia. The results may not be transferable to other federal agencies. The second limitation was the study participants; IT specialists may not respond to other IT specialists at other federal agencies. The third limitation was that the participants might develop strategies based on their local infrastructure, which may be different from other locations.

Delimitations are the boundaries that set the tone for the research study. A researcher may use delimitations to guarantee their study is within the scope and complete the research (Bloomberg & Volpe, 2018). The first delimitation was the study focused on the strategies used by IT specialists to protect the maritime network. The second delimitation for this study was interviewing the participants and using their experiences and backgrounds, which only included government employees. The third

delimitation of this study was that the population target was in West Virginia and Virginia. Therefore, the scope limited the sample to specific areas, which may lead to future studies.

Significance of the Study

Contribution to Information Technology Practice

The increase of cyber-related attacks has caused the USCG to redefine the strategies and procedures used to implement standard practices that may protect the maritime network from threats. The contribution of this study may provide senior leadership with insight into the strategies the IT specialists use or may adopt within the two organizations of the USCG. Senior leaders and IT specialists must implement standard practices to secure the maritime network from cyber-related threats properly. The growing number of new technologies, security vulnerabilities, and threats increasingly become a problem for USCG (Zukunft, 2015). Securing organizations' networks minimizes the risks of identity theft, malware, and other cyber-related issues. This study was significant to IT practice in that it may provide a practical model for IT specialists to establish strategies to implement USCG standard practices. The various data collection methods may increase the reliability of USCG standard practices among IT specialists while reducing cyber-related threats and preventing identity thefts nationally and economically for maritime industries.

Implications for Social Change

Jensen (2017) acknowledges that the maritime industry lacks a standardized approach to cybersecurity; therefore, internal components, such as IT specialists,

infrastructures, and strategies working together to implement USCG standard practices to secure the network within a USCG organization are essential. This study has implications for potential positive social change in economic stability, port security, and consumer trust for the targeted population. By contributing strategies and standardized practices, improving the cyber-related threats will secure the USCG network and create safer maritime industries.

A Review of the Professional and Academic Literature

This qualitative multiple case study was conducted to explore the strategies IT specialists use to standardize practices beneficial to secure the USCG network and reduce the cybersecurity threats against the USCG network for the maritime industry. GST was the theory selected to understand the conceptual framework better. This study provided a critical analysis of the primary research question: What strategies do IT specialists use to implement the USCG standard practices needed to secure the USCG network for maritime cybersecurity from cyber-related threats? A review of the professional or academic literature in this study served to identify research or knowledge gaps in the research. I conducted a systematic literature review using comprehensive online library search methods. The evidence gathered was to formulate a research question by analyzing, collecting, reporting, and synthesizing data (Cooper, 2020). The literature review includes 302 journals, articles, and books on security and GST. The primary resources were the Walden University Library, Google Scholar, IEEE Explore, ACM Digital Library, EBSCOHost Academic Search, ProQuest Central, SAGE, and Academic Search Complete. The following keywords were used for searches: *cybersecurity, GST,*

cyber-related threat, complexity theory, chaos theory, network security, United States Coast Guard, Maritime Transportation Security Act of 2002, Maritime Industry, *information technology (IT) specialist, Security and Accountability for Every Port Act (SAFE) of 2006, risk management, diffusion of innovation, information security, senior leadership,* and *cybersecurity strategies*. Of the 357 references, 330 (92%) were peer-reviewed, as confirmed by Ulrich's database, and 314 were published within five years of the anticipated graduation date.

Table 1

Summary of Research Articles Consulted in the Literature Review

Sources of review for the professional and academic literature	Number
Total number of references	357
Total number of references published within the last 5 years	314
Total number of peer-reviewed references	330
Percentage of peer-reviewed references	92%
Percentage of references published within 5 years	87%

The contents in the literature review are (a) GST, (b) evolution of GST, (c) supporting theories, (d) contrasting theories, (e) cybersecurity threats, (f) network system security, (g) risk management, (h) organizational cybersecurity strategies, (i) senior leadership, and (j) change management for network protection.

General Systems Theory

The purpose of this study was to explore strategies IT specialists use to develop USCG network standard practices to protect the maritime industries from cyber-related

attacks from a systems perspective. In the literature review, the conceptual framework selected was GST. Ludwig von Bertalanffy introduced GST at a seminar on philosophy in Chicago in 1937 (Ramage & Shipp, 2020). However, in 1946, GST was released for considerations of organisms as a system emphasizing biology. GST unifying a framework for interdisciplinary science was based on the idea that systems have a set of similar properties and characteristics regardless of discipline (Johnson, 2018). The idea was to apply the organizational features discovered for organisms at various levels for analysis (von Bertalanffy, 1968). Von Bertalanffy's (1968) theory for GST is outlined as follows:

> 1. A general tendency toward integration in the various sciences, natural, and social is ordinarily present.
>
> 2. Integration with sciences, nature, and society seems to be centered in a general theory of systems.
>
> 3. Nonphysical fields of science may be an essential target for the theory.
>
> 4. Developing unifying principles running general system theory enables researchers to understand the components and dynamics of systems to interpret problems and develop balanced intervention strategies. (p. 38)

As von Bertalanffy defined, these GST approaches and concepts can be applied to all sciences connected with systems. Von Bertalanffy (1972) also noted that the examination of networks and their interactions is complex and dynamic. The concept of integration is cause and effect and explains the growth and change (von Bertalanffy, 1968). According to Rousseau (2017), one of the early aspirations of GST centered around a theory to support the divide between subject-oriented and object-oriented

disciplines. GST has contributed to many disciplinary fields; therefore, its approach provides a robust framework for the complexities of a system (Schneider et al., 2017). For that reason, the GST supports exploring standard practices and strategies used by IT specialists to prevent cyber-related threats to the maritime network.

Throughout the years, von Bertalanffy (1972) evaluated a system as a whole and its relationships and interactions with other systems, such as open and closed systems, systems thinking, entropy, and a holistic approach. According to Schneider and Trapp (2018), open systems dynamically connect and respond to changes in the environment, whereas closed systems are insensitive to environmental changes (Davis, 2017). Systems thinking focuses on how the system's constituent parts act together in networks of interactions (Buchanan, 2019). Entropy is when a system breaks down if not properly managed. Von Bertalanffy (1968) noted that entropy measures disorder or decay in a system. A holistic approach is when the complete system and its parts function as designed (Soomro et al., 2016). The ability to handle changes, adaptation allows systems the ability the flexibility to change. Organizations cope with the complexity of their environment to survive (Wallis & Valentinov, 2017).

Implementing GST may assist IT specialists and senior leadership in adapting to environmental and cyber-related changes. In addition, IT specialists can use GST to develop a holistic understanding of the environment and systems to control their components (Sayin, 2016). The integration of security measures such as cyber-related employee training, authentication, encryption, IDS, patching practices, and a reliable security plan would assist IT specialists in resolving cyber-related threats. Therefore, I

examined the strategies IT specialists use to implement the USCG standard practices needed to secure the USCG network for maritime industries from cyber-related threats in this study.

GST applied to this study. The theory aligns with the security of the network and strategies needed to implement best practices to prevent cyber-related threats. GST was a significant theory used in the research of protection for the system's network. In the following section, I discuss the evolution of GST, its relationship to previous literature, supporting and contrasting theories, and how GST has been reviewed and used over time.

Evolution of General Systems Theory

Von Bertalanffy proposed GST to unify different branches of systems theory within science: biology, cybernetics, economics, software engineering, artificial intelligence, and mathematics (Scott, 2019). In the early 19th and 20th centuries, Kast and Rosenzweig (1972) revealed that researchers revised systems theory to accommodate social systems, communication, and other forms of holistic thinking. The unification of science was what von Bertalanffy (1950) was hoping to produce with the GST. Before GST, there was a lack of theory to study relationships in systems (von Bertalanffy, 1972). GST has evolved to describe the correlated practices across many different systems (Simola, 2018). Teece (2018) asserted that GST has evolved due to the increased need to know more about complex systems. Also, changes to the organizational environment with a holistic approach in the investigation of the phenomena. For a system to be successful, an IT specialist should use the holistic approach to review and analyze every aspect of the network to determine any security threats within the system. Von

Bertalanffy recognized that an organization needs to interact with its external environment, while a holistic approach could solve organizational problems (Chikere & Nwoka, 2015). The fundamental principles of GST form the basis for typical organizations, which process some form of information/input and generate some output (Chandler et al., 2016).

The system's input and output involve crossing boundaries that define the system. An open system receives input from the environment and releases output to the environment. In contrast, a closed system occurs only among the system components and not with the environment (Turner & Baker, 2019). Therefore, in this study, the target organization, USCG, can be classified as an open system because inputs are obtained from their environment. Also, based on an extensive literature review, I discovered that the USCG network could be observed through GST. The GST framework could be used to enhance an understanding of relationships in organizations and, afterward, develop strategies to improve the organization (von Bertalanffy, 1972). Organizations should also secure and protect physical structures, processes, and other significant organizational assets to protect their information and infrastructure (Yasin et al., 2018). Adequate security should incorporate a holistic approach while IT specialists and senior leadership begin developing organizational security policies to protect the components from unauthorized access.

According to Rousseau (2017), organizations depend on GST principles to reflect fundamental assumptions and scientific theories. Applying the principles, researchers should analyze cyber-related issues as a whole system within an organization, allowing

researchers to observe strategies in different areas. These strategies affect multiple systems and networks. Therefore, researchers could use GST in various views, such as adaptive governance, self-organization, and complexity thinking. These views reinforce the theory and increase the system's integrity (Van Assche et al., 2019). Tzafestas (2017) suggested that researchers use GST to contribute to many areas in developing a system.

In contrast, Micó et al. (2016) explored GST and suggested researchers use GST to state the relationships of input variables of a system. The relationship and interaction of these variables are essential to determine the effects on the system as a whole. Yurtsevena et al. (2016) evaluated GST and examined the holistic approach as a process used by a system as a complete functioning unit using the foundations of GST, cybernetics, and soft system method.

Additionally, researchers use GST to explain communications, roles, and responsibilities in a system (Mania-Singer, 2017). GST recognizes the importance of feedback, which involves external changes coming into a system and the components of adjusting the environment (Teece, 2018). IT specialists using strategies to protect the maritime network against cyber-related issues could be considered one of the responsibilities or parts of the overall system. IT specialists can use GST to determine network strategies and decide the external effects of internal operations (Malecic, 2017). The internal strategy and procedures of the maritime network affect the external maritime ports and the USCG as a whole. Each system has a role and responsibility and affects the organization differently. Even though the effects are different, each part of the system is essential to the sustainability of the entire organization. Maritime is the organization and

the input variables are the different components that aid in the success or failure of the network.

Strategies for success are critical for the maritime network because IT specialists use them to manipulate input variables to increase the organization's sustainability, which would be considered an open system. Von Bertalanffy (1968) noted that at the center of GST are open systems and systems thinking. In 1987, Barry Richmond was credited as the originator of *systems thinking* (Arnold & Wade, 2017). Geoffrey Vickers identified systems thinking as the approach to problem solving by revealing the factors and interdependencies of complex situations (Buchanan, 2019). The problems to solve, such as cyber-related attacks, would be viewed as parts of the overall system with the outcomes or events contributing to further unintended consequences (Masys, 2015). The study of relationships described by von Bertalanffy (1972) is still the foundation, but the expansion of the theory is more inclusive of a variety of complex systems (Mania-Singer, 2017). Researching strategies through GST explores the interactions within the system and insight into the theory's critical components. A systemic approach for security issues determines the need for a scientific direction as systematic generalized knowledge about all aspects of security (Malyuk & Miloslavskaya, 2016). Addressing the systemic approach provides a reason GST researchers can adapt and grow the theory. Gorzeń-Mitka and Okręglicka (2014) noted that researchers trace the roots of modern complexity and systemic approach to the birth of GST. GST is a versatile theory to explain any system of all sizes (Yurtsevena et al., 2016).

Analysis of Theories

To explore the research and access my findings through foundational content, past and current research, along with the trends and innovations in the security of cyber-related threats, I used the GST as the conceptual framework for this study. The GST is focused on the nature of complex systems and is a framework researchers use to explore or describe the interdependence of objects working in isolation. GST was chosen as the conceptual framework to explain the phenomena and explore the strategies used by IT specialists to implement USCG standard practices to protect the maritime network. Several supporting and contrasting theories relate to the GST introduced by von Bertalanffy in 1937 (Pouvreau, 2014). The theories include complexity theory, chaos theory, grey systems theory, and diffusion of innovation theory.

Supporting Theories

Complexity Theory

Complexity theory is a system with the chaos that reconciles the essential unpredictability of organizations with an emergency of distinctive patterns (Jacobs, 2019). Complexity theory is a subset of systems theory that appeared in the literature in the 1930s and 1940s (Stacey, 2011). Mason and Staude (2009) asserted that complexity theory suggests that the interaction of a system's components will result in patterns producing unexpected behavior. Kivak (2017) described complexity theory to uncover the unpredictable elements of a complex system and how they adapt to the changes in their environments. Waldrop (1992) and Kivak (2017) concurred that complex systems must be adaptable, and organizations must react to change. In the literature of the past

two decades, complexity theory challenges traditional senior leadership assumptions (Johansen, 2018). According to Koopmans (2017), complexity has a paradigm shift that replaces traditional logical positivism with assumptions and methodological priorities. Öztürk and Kızılkaya (2017) noted that complexity is not a methodology but a way of thinking and a way of seeing the world. Complexity theory affects different disciplines, such as (a) knowledge management, (b) strategy, (c) leadership, and (d) information technology (Turner & Baker, 2019).

Complexity increased because of the probabilities of specific outcomes and randomness of occurrences, which reduces uncertainty, such as entropy (Koopmans, 2017). Maritime networks faced challenges that included changing operational requirements, cultural differences, available resources, and interactions with internal and external customers. Maritime IT specialists operate in an unpredictable environment; they face challenges on a day-to-day basis. Grounded in complexity theory, IT specialists should interpret new environmental events and adjust accordingly. The complexity theory builds on GST's principles. However, the complexity theory emphasizes inter-relationships and interdependence. The complexity theory differs from GST, as it operates on the principle that the whole is different from the sum of its parts. In contrast, GST follows the principle that the whole is greater than the sum of its parts (Turner & Baker, 2019). Therefore, the complexity theory was not appropriate for the study because it believes the whole is different from its parts, and GST believes in system holism.

Chaos Theory

Edward Lorenz introduced chaos theory in 1963 for a mathematical model (Resler, 2016). Chaos is the science of the global nature of systems, and chaos theory identifies a complex system as having many interrelated parts that are dynamic and continuously changing (Rand et al., 2018). The chaos theory suggests that the behavior of complex systems can follow the rules, but the future state remains unpredictable (Ruelle, 1991). Dhillon and Ward (2002) proposed chaos theory for information systems. Organizations and other researchers have shown that chaos theory is a consistent approach to information technology and organization management (Mbengue et al., 2018). Chaos theory may characterize the behavior of systems based on their descriptions and predictions of the outcomes. However, Hayles (2018) asserts that chaos theory rejects speculation and seeks order and predictability, albeit without established causal and deterministic patterns and models. Besides, Rand et al. (2018) mentioned that chaos theory implies that a long-term prediction is nearly impossible, even if researchers know the system's behavior rules.

Chaos theory points to the importance of developing guidelines and decision rules while achieving the organization's goals (Amiri et al., 2018). An organization is a body of people who share a purpose, vision, or mission, considered nonlinear, dynamic systems (Goulielmos, 2019). Kozlowski (2018) define organizations as complex dynamic systems that exist in a context, evolve, and adapt as situational demands unfold. Planning and acknowledging chaos in the internal and external environment could enable IT specialists and senior leadership to do standard practices and implement strategies that

contribute to their success. Complexity theory is similar to chaos due to unpredictability; however, chaos suggests an order to the randomness, and complexity does not (Kivak, 2017). Therefore, chaos theory was not appropriate for this study. The GST does not have random behavior but shows patterns of behavior.

Contrasting Theories

Grey Systems Theory

Ju-Long Deng first proposed the grey systems theory in 1982 (Ju-Long, 1982) to explain incomplete or unknown information. Some researchers call it the black and white method because the theory looks at the internal and external components that automatically form within an organization. Those components are unpredictable and make it difficult to predict the outcome (Scarlat & Delcea, 2016). Researchers use grey systems theory as a tool to analyze and observe small sample sizes that lack information to make long-term predictions, according to Liu et al.(2016). Researchers use grey systems theory to fill the space where information is missing and predict future outcomes (Meng et al., 2017). Researchers use grey systems theory in various ways to predict or estimate the outcome of a system such as an organization for security concerns. Otero (2019) determined that researchers use grey systems theory to quantify the importance of system changes and the organizations' goals and objectives. Researchers use these techniques and concepts for decision making and future predictions.

The USCG maritime network sustainability research is extensive. Sustainability can successfully maintain, grow, and survive (Warren & Szostek, 2017). Different researchers define sustainability as preventing adverse effects on the overall system (Bird

& Davis-Nozemack, 2018; Tuntivivat et al., 2018). The sustainability of organizations is a continuously evolving study, and there are contrasting views. These contrasting views are prevalent due to the nature of organizations using different strategies for success depending on the type of cyber threats or even the location and the various definitions of sustainability. It is important to view an organization in various capacities to determine if there are strategies implemented by IT specialists to protect the maritime network and that are cross-disciplinary.

Additionally, grey systems theory is difficult to view as a lens for qualitative research. Much of the research uses grey theory as a quantitative theory to predict numerical results when there is a lack of information. Lack of information can lead to unclear results, and grey systems theory has grown to predict outcomes even with small sample sizes. Liu et al. (2016) determined that researchers use grey systems theory to predict short and long-term results. Researchers can apply grey systems to a variety of areas that lack information to develop precise details. Researchers use grey theory to solve uncertain problems that lack information (Liu et al., 2016). In contrast, GST is used to solve problems where elements are known. The difference between the grey systems theory and GST is that the overall system is examined in a qualitative theory using real-life experiences for the GST.

Diffusion of Innovation Theory

E.M. Rodgers developed the diffusion of innovation theory in 1962, and it has been widely used in the social sciences (Matthews, 2017). The diffusion of innovation uses the communication process to accelerate the acceptance of innovation (Rogers,

2003). Diffusion is a social process that occurs in response to learning about an innovation (Dearing & Cox, 2018). This theory enables examining how certain behaviors are adopted and focuses on perceived innovation attributes (Mohammadi et al., 2018). Additionally, researchers use this theory to determine how organizations accept innovation is accepted (Harvey, 2016).

The diffusion process of technologies and innovations is complex, and it follows a set of stages (Rogers, 2010). Rogers (2010) stated that the five steps of diffusion of innovation are (a) knowledge, (b) persuasion, (c) evaluation, (d) implantation, and (e) adoption.

Chile (2018) notes that diffusion of innovation focuses on minor changes and does not draw a significant conclusion on the broader theory. Damanpour (2020) mentioned that the diffusion of innovation in organizations uses generation and adoption. The diffusion of innovation theory only focuses on innovation (Gupta et al., 2017). Researchers acknowledge that the process of confirmation is very long and challenging. Researchers of government policies have used diffusion of innovation and believe the effectiveness can be more important than knowledge of actual outcomes (Dearing & Cox, 2018). According to Leake (2019), the primary aim of diffusion of innovation is to help organizations perceive concepts, habits, or new technologies. Maritime network security is very diverse and can be more substantial than just innovation. Since this theory only encompasses a part rather than the whole study, it is not relevant to this study.

Cybersecurity Threats

Cybersecurity is considered a significant challenge for an organization because of the cyber-related threats (De Oliveira Albuquerque et al., 2016). Farahbod et al. (2020) stated that the average cost to address a malicious insider's attack is $2.4 million and 50 days. Additionally, the average number of days to resolve a ransomware attack is 23 days. The organization must focus on the primary weaknesses of its business practices, culture, and IT systems (Yang et al., 2016). Cybersecurity is the collection of tools, policies, guidelines, risk management, training, and best practices used to protect an organization's systems (Kosiński et al., 2019). As the impact of cyber-related threats continues to grow, the complexity of the system and network security results in organizations facing continuing challenges.

Alves and Morris (2018) mentioned that classic cybersecurity issues are interconnected from malicious adversaries. Cassidy (2017) indicated it has been difficult to obtain general statistics on all cyber-related maritime incidents and small-scale attacks. The lack of cyber awareness and the erroneous classification of the cyberattack presents cybersecurity risks (Tam & Jones, 2019). In 2018, the dependence on the stability and security of networks within an organization demanded detection for cyber-related threats (Moskal et al., 2018). According to Škrjanc et al. (2018), networks are vulnerable to interruption by adversaries, insider threats, and cybercriminals. Burns et al. (2017) suggested that human behavioral actions by the employees impact the system's confidentiality, availability, and integrity.

Organizational system flaws and weaknesses have been identified as cybersecurity issues (Padayachee, 2016). Cyber-related security for systems involves the vulnerability of the system. The vulnerability of a system is the weakness in a system that renders it open to exploitation by a given threat (Edgar & Manz, 2017). The U.S. Department of Homeland Security (DHS, 2018) suggests that cybersecurity is the agency's core mission, which results in the USCG cyber-related strategy. The USCG treats the security of cyber-related threats as a significant strategic priority (Chatterjee & Thekdi, 2020). Cyber-related risks can occur in various forms on a system's network (Edgar & Manz, 2017). According to de Bruijn and Janssen (2017), a cybersecurity risk means futurizing threats and creating imaginary security. The government should be more specific when describing cybersecurity attacks, such as viruses, trojan horses, ransomware network backdoors, denial of service (DoS), or phishing attacks (Janakiraman et al., 2018). Wagner et al. (2017), network system administrators should protect the network by utilizing defensive mitigation strategies.

Table 2

Summary of Cybersecurity Attacks

Cybersecurity attack	Characteristics
Virus	Code that is attached malicious or unknown to other programs and runs when those programs are running (Shin et al., 2017).
Trojan horse	The program adds malicious subversive functionality to an existing program (Shin et al., 2017).
Ransomware network backdoor	The malicious code is entered on the network by an insider or third party (Kim et al., 2020).
Denial of service	A malicious attempt to make a network or computer unavailable to users (Alabady et al., 2020).
Phishing attack	An attacker impersonates an employee or customer using email with malware attached (Huang et al., 2018).

Network System Security

Information is a critical factor for enterprise assets. Security combines systems, operations, and internal controls to ensure the integrity and confidentiality of data and operation procedures in an organization. Confidentiality's purpose is to keep sensitive information from being disclosed to unauthorized recipients. Integrity ensures the information and programs are changed only in a specified and authorized manner (Anttila & Jussila, 2017). Availability's function ensures that system denial is not an option for authorized users, and prompt service is readily available (Ali & Awad, 2018). Laracy and Marlowe (2018) stated that security is a system property that implies protecting the information, operational, and physical elements from malicious intent. Network attacks

are subject to malicious sources divided into two categories: passive attacks and active attacks.

Passive attacks are the attempts made by malicious nodes to perceive the nature of activities and when an intruder intercepts data without disrupting the operation (Yang et al., 2018). Active attacks are when an intruder attempts to alter, inject, delete, or disrupt the network and gain access (Lykou et al., 2019). Network security is taking the physical and software preventative measure to protect the infrastructure from unauthorized access, misuse, malfunction, and destruction, creating a secure platform for applications and the overall network (Amrollahi et al., 2020). Therefore, the maritime network would be the system's property for the USCG.

Overview of Networks

The maritime network is considered an operational infrastructure based on the International Standards Organization (ISO) and Open Systems Interconnection (OSI) reference model. The ISO/OSI reference model has seven layers, and each layer defines the network protocols and allows communication across all types of networks. The seven layers are physical, data link, network, transport, session, presentation, and application.

1. Physical layer – sends and receives raw bitstreams from one network node to another, maintaining the physical connection between transmitter and receiver (Savalkar, 2018).
2. Data link layer – generates packets it receives from the network layer and provides them to the physical layer. This layer includes error detection and correction (Ahearne et al., 2019).

3. Network layer – deliver packets from source to destination across multiple network links (Aggarwal et al., 2019).
4. Transport layer – ensures the reliability of the transport of the sent data, and the message arrived intact and in order. Additionally, the transport layer breaks the data into smaller units for easier accessibility by the network layer (Aggarwal et al., 2019).
5. Session layer – establishes and terminates a session to maintain and synchronize the communication (Zhao et al., 2018).
6. Presentation layer – handles data format information for networked communications (Zhao et al., 2018).
7. Application layer – the top layer of the OSI model to provide the application-based services (Aggarwal et al., 2019)

Networks may fail due to various cyber-related attacks (Li et al., 2016). According to Donaldson et al. (2015), there are three main cybersecurity threats, and they are related to the confidentiality, integrity, and availability (CIA) triad:

1. Data threat targets the confidentiality of networks, databases, backups, applications servers, and systems administrators.
2. Alter Data threat targets the modification of data and damage to the organization's image, which, in return, harms the organization's integrity.
3. Denial access threat targets the denial of service, and the physical destruction of a system and network results in availability issues for the organization.

Wagner et al. (2017) noted that cyber-related threats had caused significant damage to enterprise networks in recent years. The Coast Guard has been working to mitigate cyber-related threats to U.S. ports and critical maritime infrastructure. Cyber-related threats for the maritime network have been a concern of leadership for years. According to Goss (2017), the USCG organization struggles to find a practical approach to improve security and procedures.

The Department of Defense (DoD) suggests adopting the National Institutes of Standards and Technology (NIST) Risk Management Framework (RMF) as an approach to improve security within the organization. A network is secure when it possesses the components of the confidentiality, integrity, and availability (CIA) model (Sosin, 2018). Rondelez (2018) stated that government leaders manage networks based on their experience. Network security is the usability and integrity of the organization's network and data. Organizations are dependent on secure systems but have become targets of backdoor intrusions (Alexander, 2017). Hubbard et al. (2017) stated that government networks must use the framework for improving critical infrastructure cybersecurity developed by the National Institute of Standards and Technology. There are combined layers of defenses, and each network security layer should implement policies and controls (Abdullahi, 2018).

The Cybersecurity Enhancement Act of 2014 addresses the risks of cyber threats. This act enhanced the reach of the NIST, which makes identifying and mitigating threats against this framework simpler. The core of the framework consists of the following functions: (a) identify, (b) protect, (c) detect, (d) respond, (e) recover (Dedeke, 2017).

The identify function is for the USCG to have the ability to detect all threats and obtain an understanding of how to secure the maritime network against the adverse effects of the possible threats. The protection aspect introduces the strategies and best practices the IT specialists and senior leadership will use to protect the maritime network. The detection component depends on the strategies and best practices to discover the threats and protect the system against cyber threats. The response functionality will be the security strategies or systems that will defend against the threats.

Kalloniatis et al. (2017) noted that organizations must appropriately indicate and execute system security requirements. Chitchyan et al. (2017) assert that security and privacy requirements depend on compliance, traceability, access control, verification, or usability. Kalloniatis et al. (2019) noted that system security is a constant concern with organizations. For example, a vast amount of data means that security breaches will lead to more severe consequences and losses via reputational damage, policy, best practices, legal liability, compliance, and ethical harms. Visner (2016) states that weak governance is the cause of the organizational crisis. Organizations with poor governance, unclear accountability, and responsibility put their systems and network security in jeopardy. Sosin (2018) mentioned that organizations must identify any cyber risks and have the goal of cybersecurity.

Identifying the cyber risks helps protect electronic information systems and networks from being attacked by threats and vulnerabilities (Sosin, 2018). The impacts of confidentiality, the integrity of data, or the availability of the systems alter the system's vulnerabilities (Jouini & Rabai, 2017). The vulnerabilities consist of flaws in a system,

which can be misused by attackers and significantly impact the network (Karchefsky & Rao, 2017). With vulnerabilities in a system, a threat may be revealed through a threat agent using the GST to produce undesired consequences.

As security gets more complicated for network security systems, organizations use approaches such as firewalls. Network security is part of the organization's information security infrastructure, such as physical security, personnel security, operations security, communication security, and social mechanism (Nieles et al., 2017). ISO specifies guidelines for network security and defines risk management as the coordinated activities to direct and control an organization concerning risk (Mayer & Aubert, 2020).

Risk Management

Risk management is the process of establishing and maintaining information security within an organization. Risk management includes governances and policies; both should be considered along with the strategies for an organization (Goss, 2017). Kaušpadienė et al. (2019) stated that systemic risks are due to cybersecurity violations and a significant increase from their implementation. Risk management is the consistent application of techniques used to manage the uncertainties surrounding achieving an organization's objectives (O'Har et al., 2017).

Risk management provides an organizational framework to identify facets such as assets, threats, vulnerabilities, and controls (Brustbauer, 2016). Akinrolabu et al. (2019) suggested that risk management involves the process of identifying cyber-related threats, risk mitigation measures to identify an acceptable level. Organizations use risk

management to apply efficient countermeasures to strengthen system vulnerabilities (Abbass et al., 2019). The risk management process consists of four steps: (a) risk identification is understanding the organization's events and determining if any risk could potentially affect the overall goals (b) risk assessment is analyzing the risk concerning impact, dependencies, and timeframes for customers and organization; (c) risk mitigation is designed to manage, eliminate, or reduce the risk to an acceptable level; (d) risk monitoring is to track risk mitigation actions for progress continually and manage. Information security and risk management have a specific set of Federal Information Processing Standards (FIPS) and NIST Special Publications (SP) that holistically affect network system security.

1. FIPS 140-3 – *Security Requirements for Cryptographic Modules* specify the requirements a device that receives electronic process data through a network must meet if used by the federal government (Cooper & Schaffer, 2019).
2. FIPS 199 – *Standards for Security Categorization of Federal Information and Information Systems*, specifies the standard framework and understanding for organizations to promote effective management and oversight of information security programs while reporting to Office of Management and Budget (OMB) and Congress the status of the security policies, procedures, and practices (National Institute of Standards and Technology, 2017).
3. FIPS 200 – *Minimum Security Requirements for Federal Information and Information Systems* specifies minimum security requirements for information systems supporting federal governments and a risk-based process to select

security controls to satisfy the minimum-security requirements (National Institute of Standards and Technology, 2017).

4. SP 800-30 – *Guide for Conducting Risk Assessments* guide risk assessments for federal government systems and are used to identify, estimate, and prioritize risk for business processes for an organization (Supriyadi & Hardani, 2018)
5. SP 800-37 Revision 2 –*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* provides guidelines for privacy risk management processes to align the NIST cybersecurity framework and system life-cycle engineering processes (Pillitteri, 2019).

Information Security Risk Management Process

Information security risk management comes from applying technology where risks involve the security of the information (Wangen et al., 2018). Kuhn (2018) recognizes that risk management addresses cyber-related risks by extending safety management techniques to cyber-enabled techniques. Cyber-related threats occur when people, processes, and technology of cybersecurity risk management are missing or inadequate (Galinec et al., 2017). Halima et al. (2018) noted that risk management is a crucial discipline for making effective decisions and communicating the results within the organization. An organization should align people, processes, and technology to develop and implement security controls to mitigate risk from cyber-related threats (Verma et al., 2018).

Langner and Pederson (2013) noted that cybersecurity risk management is bound to fail because senior leaders are incentivized to underinvest in security measures. Many cybersecurity risk management methods focus on susceptibility to known exploits such as degradation, interruption, modification, fabrication, unauthorized use, and interception (Musman & Turner, 2018). Distributed denial of service (DDoS) attacks can cause degradation on a system's network. The degradation causes interruption on the system, and it becomes unusable. A modification to the system will occur when a change in the data, software, or hardware. An organization must be aware of the modification to ensure a cyber-related threat has not caused fabrication by inserting false information or components into the system.

Additionally, unauthorized use and interception could cause the other threats mentioned and give users elevated permissions (Musman & Turner, 2018). The federal government recognizes that risk management can assist in improving performance and is a continuous process. Federal organizations use impact levels such as high, moderate, and low to identify and categorize the impact of confidentiality, integrity, or availability of a system.

Organizational Cybersecurity Strategies

Organizations must recognize cyberattacks and respond by improving their security technologies (Asghari et al., 2015). Biswas and Mukhopadhyay (2018) suggested that organizations face a series of challenges to keep systems patched and a plan to reduce the risk of vulnerabilities. Organizations need to institute cybersecurity as a requirement to expand their threat and vulnerability management strategies to apply risk

mitigation measures. Nieles et al. (2017) noted that an organization's inability to select and implement appropriate security policies and procedures would likely harm the organization's mission.

Network security protection can include firewalls, penetration tests, and intrusion detection systems. De Oliveria Albuquerque et al. (2016) assert that cybersecurity connects an organization's policies, practices, and physical infrastructure. Organizations must secure and protect physical structures, processes, data, and infrastructure (Yasin et al., 2018). Rondelez (2018) noted that government organizations could increase the efficiency and effectiveness to protect the system infrastructure from cyber-related threats. Applying a holistic view of a cybersecurity strategy to protect the network and system includes corrective and preventive measures (Allodi & Massacci, 2017). Wagner et al. (2017) argued that cybersecurity systems have a mix of complexities, such as processes, hardware, and human actors, that make it difficult to predict the effects of policy changes on a network system.

The organization recognizes the need to closely monitor and enhance its risk management and internal security process using security governance procedures (Asgarkhani et al., 2017). Organizations can focus on leadership and processes to adapt approaches through layered security control to manage security risks (Young et al., 2016). Halima et al. (2018) state the risk management is a continuous process, not a one-time occurrence. Risk management is the critical discipline for senior leadership to make effective decisions and communicate the organization's results. While organizations use methods and techniques to protect data, infrastructure, and assets, they may still

experience successful cyberattacks (Jang-Jaccard & Nepal, 2014). Choi (2016) opined that skilled information security managers would improve the effectiveness of the organization.

According to Rick Van der et al. (2017), network specialists should be an organization's first line of defense against cyber-related threats. Asghari et al. (2015) agree that improperly trained employees are a significant risk to the organization due to little or no technical knowledge. Information Systems Audit and Control Association (ISACA, 2016) reported that there would be a shortage of two million cybersecurity professionals by 2019 because of the skills gap. DHS recognized the shortage and decided to develop and advance technical cybersecurity qualified professionals (DHS, 2012). The DHS developed a cybersecurity strategy framework to identify risks and vulnerabilities, mitigate cyber-related threats, and make the systems more secure and stable (DHS, 2018). Organizations rely on the assurance of their network security to prevent attacks by implementing security policies, allowing proactive measures in managing cyber threats (Smeets, 2018).

A cyber-related strategy is an essential organizational prerequisite to assessing the threat environment and establishing a comprehensive coordination and management process (Klaic, 2016). The holistic system approach can be applied when implementing cyber-related strategies. Organizational network systems should focus on cyber-related strategies such as training, policies, vulnerability mitigation, and the integration of security measures (Yang et al., 2016). Cyber-related strategies are not just preventing

adversaries from gaining access to the system. Cyber-related strategies also include the integrity and availability of the system and network security (Lagouvardou, 2018).

Organizations implementing cybersecurity should bring three key elements: education via training, policy, and technologies (Dawson, 2018). The training provides insight into innovative ways to teach cyber-related security and ensures the organization reviews governing strategies, tools, and techniques and understands the policy framework, including directives, standards, mandates, laws, and best practices (Dawson, 2018). The strategies provide the baseline for further guidance and direction for organizations to set their standard guidelines.

As technology is evolving, an organization needs to learn and adapt cybersecurity awareness for every individual. Dubosson et al. (2019) mentioned that silos in organizations can affect communication and prevent employees from sharing information and best practices. If security controls are not put into place to protect the network, cyber-related threats quickly rise (Soomro et al., 2016). Interdepartmental communication has been a factor in risk management, and senior management must establish and maintain a link between the silos. Senior leadership engagement to implement effective risk management strategies includes employees with capabilities and experience (Young et al., 2016).

Communication regarding maritime cyber-related issues is difficult to convey and develop policies and procedures. Al-Mohannadi et al. (2018) believe organizations, such as the government, should look for a more effective method to prioritize systems and the security required for such systems. IT specialists should be represented by senior

administrative levels within governments. Strengthening the systems' device vulnerabilities and security procedures are senior leadership applying risk management. Additionally, security awareness services help both IT employees and government organizations understand the weakness of the network.

Senior Leadership

Many organizations use IT for business operations and decision-making processes, which causes information security to be a significant concern for senior leadership. (Chu & So, 2020). James (2018) revealed that 95% of senior leaders recognized cyber-related threats as being an area of high importance, but 45% of them did not have formal strategies in place. The success of an information security program depends on the policy generated and the attitude of senior leadership toward securing the data and the infrastructure (Hu et al., 2012). Mishra et al. (2019) mentioned that senior leadership should protect the organization from cyber-related risks.

Senior leadership is responsible for becoming involved in strategic decision-making with the cybersecurity program to implement cybersecurity (Soomro et al., 2016). Senior leadership should understand the implications and limitations of all aspects of security policies. The chief information officer, information system security manager, and senior leadership own the decisions for accepting residual risks and evaluating them against additional security costs (Blum, 2020). According to Harrison and Jürjens (2017), senior leadership controls and directs activities to enhance information security awareness. In return, the lack of security awareness and deficiencies among employees is absent.

The most important reasons to implement effective standard practices and cybersecurity strategies include internal and external factors, internal or external information (Young et al., 2016). Standard practices and policies are not effective in an organization that lacks compliance. An organization's cybersecurity workforce with roles and responsibilities that include setup and maintenance of networks, operations, systems, and databases are exposed to new cyber-related threats every day. A significant function of the organization's strategic planning to prevent security breaches involves implementing standard practices, building a defense against future attacks (Soomro et al., 2016). Many organizations lack effective training programs or employees with expertise in cybersecurity (Young et al., 2016). Employee ignorance increases data breaches and data security vulnerabilities (Budke & Ferguson, 2017). Senior leadership would need to change their attitudes and engage their employees to aid in the success of the day-to-day operations to enhance a relationship for success within the organization (Komodromos et al., 2019).

Change Management for Network Protection

Examining subsystems and their place is an element of GST, a form of organizational change management (Bardarova & Simic, 2019). Change management is a continuously renovating process of an organization's system or structure. Change management depends on internal and external clients', customers', or employees' changing demands (Alhmeidiyeen, 2019). A holistic cybersecurity change management approach must accommodate all facets of network security. IT specialists and senior leadership should adapt to the increasing frequency and diversity of cyber-related threats.

However, it is a challenge to implement change in an organization (Jensen, 2017). Policymaking in the field of cybersecurity faces many paradoxes, such as control of a system, visibility of cybersecurity to customers, cost, and impact on the organization (de Bruijn & Janssen, 2017). The reassurance the Coast Guard needs to ensure the safety of the maritime network involves change management. Changes in the IT environment include the systems and applications resulting from a new or regulatory requirement or an update needed to enhance the current system's functionality (Masli et al., 2016). Quigley et al. (2015) mentioned that IT specialists and senior leadership often use message framing to communicate a complex problem directly and convincingly. De Bruijn and Janssen (2017) suggested that employees' and customers' attitudes and behaviors are affected by message framing and depend on receiving individuals' processing and traits.

Security policies and codes of conduct are frequently the main reasons, and senior leadership needs to control and guide employees, such as IT specialists' security behaviors. Li et al. (2016) suggested that humans play a role in ensuring the defenses are in place, cybersecurity attacks are detected immediately, and countermeasures are taken. The security policy must be updated and maintained within the organization. Also, Sohrabi Safa et al. (2016) suggested the security policies address the human element of information within the organizations. The organization plays a significant role in enhancing the capabilities of cybersecurity professionals (Park et al., 2016). The examination of management strategies and the importance placed upon risk factors of sensitive information offers insight for organizations (Aiken et al., 2016). Implementing a significant budget, strategies, and collaboration between the information system security

manager and information system security officer monitors the cybersecurity program implementation plan of the organization's assets, data, and infrastructure (Aiken et al., 2016). Federal senior leaders are responsible for familiarizing and complying with laws and regulations for information security and risk management (Nieles et al., 2017).

One solution is for organizations to implement secure firewalls for protection to eliminate the possibility of a breach (Ani et al., 2017). Firewalls are vital tools for network security that operate between the connection of an organization's internal and external network (Mihalos et al., 2019). Firewalls limit network access by providing barriers utilizing specific network packets to travel for incoming and outcoming traffic. However, Al-Yaseen et al. (2016) suggested that an intrusion detection system (IDS) provides support to protect organizations from cyber-related threats. IDS are critical for identifying and tracing network intruders (Ikram & Cherukuri, 2016). A top concern for organizations is cyber-related threats, a primary concern for protecting IT systems, networks, and financially sensitive data. Many organizations realize the severity of cybercrime and the importance of the implicit understanding of the security and weakness of their IT department (Aiken et al., 2016). Therefore, organizations must recognize violations, implement secure firewalls, and update their antivirus software to prevent attacks (Clarke & Knake, 2019).

The organization should run security checks and conduct a system backup daily. However, senior and executive managers still minimize their involvement, especially in aiding the IT department to engage managerial strategies to prevent breaches, cybercrimes, fraud, and omission to mistakes (Arief et al., 2015). All organizations need

government policies to aid organizations in developing an economic model, national regulations, and laws for companies to adopt secure systems to fight cyber-related threats (Trautman, 2016). Standardized practice methods with a holistic prevention strategy can avoid cyber-related risks (Albahar, 2017). The importance of this study encompasses IT specialists' strategies employed by USCG to defend the network for maritime industries from cyber-related threats.

Relationship of this Study to Previous Research

The purpose of this research study was to explore the strategies that IT specialists may use to implement best practices to secure the USCG network for maritime cybersecurity from cyber-related threats. Similar studies researched maritime cybersecurity and the efforts of the maritime industry. Zăgan et al. (2018) examined the risks associated with maritime cybersecurity. The researchers established maritime cybersecurity measures to protect the network and computer assets on the ships, terminals, and ports. The lack of education and training and a lack of resilience and prioritization causes the defense to fail when the maritime network is under a cyber-attack. Shapiro et al. (2018) examined the awareness of vulnerabilities such as trojan horse risks. Determining the acceptable level of risks for the maritime organization was discussed, including the risk assessment and mitigation strategy plans for cybersecurity. Shapiro et al. (2018) mentioned that security measures needed to protect the maritime industry from trojan horse attacks involve a combination of personnel security, physical security, and cybersecurity measures to provide a defense in depth (DiD). The defense-in-

depth method is a defensive strategy aimed to protect the effectiveness of defense installations for networks (Chierici et al., 2016)

Daum (2019) focuses on the different types of cyber-attacks from the perspective of the maritime industry using the International Maritime Organization (IMO) and maritime cyber risk management guidelines. The IMO sets the goal of cyber risk management to meet cybersecurity at an acceptable level concerning the costs and benefits. Bronk and Dewitte (2020) address issues of cybersecurity in the maritime system. The research discussed cybersecurity risk management and how DHS identified USCG as the lead agency for maritime safety and cybersecurity in 2015 (Bronk & Dewitte, 2020). The USCG strategy has two points: (a) assessment of risk through the promotion of cyber risk awareness and management, and (b) prevention via the reduction of vulnerabilities in the maritime system (Bronk & Dewitte, 2020). Rajamäki et al. (2019) discussed in a case study to develop a secure sharing support tool enabling personnel to coordinate and share cyber-sensitive information in real-time for the maritime domain. The research data were collected by participants with different roles, along with using documents and reports. Hopcraft and Martin (2018) presented that the maritime industry has risks such as hacking and outages. The researchers also mentioned that a cumulative body of literature documented maritime systems and the vulnerable range of cyber threats.

Transition and Summary

The purpose of this study was to explore the strategies IT specialists used to implement the USCG standard practices to secure the USCG network for maritime

cybersecurity from cyber-related threats. The extensive literature review helped establish an academic foundation for this study while critically analyzing the body of knowledge related to the research question. The literature review was broken down by theme to help guide the reader through extensive research on the study topic. The literature analysis also increased the understanding of cybersecurity strategies, network system security, risk management, organizational cybersecurity strategies, and change management.

In the conceptual framework for this study, GST describes holistic system thinking and complex systems. Section two of the study will explain the rationale for using qualitative, multiple case studies to explore IT specialists' strategies to secure the USCG network for maritime cybersecurity from cyber-related threats. Also, in Section 2, I describe in detail the role of the researcher, participant selection, population and sampling, data collection and analysis, and finally, how this study can ensure the reliability and validity of the study.

Section 2: The Project

In this section, the role of the researcher, the criteria for selecting the participants, population sampling, research design, and the research method are provided. Also, in this section, the justification of instruments for data collection tools and the consenting process for the research are discussed. The data analysis of the research quetion is provided in this section, and the reliability and validity of the study are presented as well.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the different strategies IT specialists use to implement the USCG standard practices to secure the USCG network for maritime industries from cyber-related threats. The population for this study included IT specialists who have applied the USCG standard practices for maritime industries to secure the USCG network from cyber-related threats. Participants were from two IT departments in the C4IT center and one IT department in the OSC of USCG in Virginia and West Virginia. Implications for positive social change that may result from this study include reducing unauthorized exposure to maritime industry operations and privacy protections for the targeted population.

Role of the Researcher

Qualitative researchers use people's perspectives, such as beliefs and experiences (Brink, 1993). Viswambharan and Priya (2016) stated that qualitative research describes and interprets a phenomenon from the individual or population being studied. My primary role as the researcher was to build a relationship with the study participants, collect data while maintaining objectivity, interpret the information, and minimize

personal bias to safeguard research quality and integrity (Nelson et al., 2015). A researcher is a key to obtaining data from participants, and the interview protocol process becomes essential when a researcher plans to be the primary research instrument (Taiwo, 2019). Researchers should be knowledgeable and prepared before scheduling a series of interviews and collecting data. Cumyn et al. (2018) mentioned that ethical conduct relies on researchers to research integrity and ethics.

During the data collection process, Yin (2018) noted that a researcher should adopt the following fundamental values: (a) asking the right questions, (b) being an active listener, (c) being adaptive, and (d) conducting research ethically. In this study, the data gathered was completed by conducting interviews and reviewing organizational documents. During the interview process, a record of the participants' responses was captured with their permission to promote open and detailed dialogue (Roulston, 2018). Proper implementation of research ethics ensures the protection of the rights and well-being of the participants (Tajir, 2018).

I have 20 years of IT experience, and of those 20 years, 15 years involved in cybersecurity, database management, and system engineering in the USCG. I also have 19 years of experience teaching mathematics, computer science, and cybersecurity. I had no relationship or contact with any participant before receiving official approval from the Walden University Institutional Review Board (IRB). I conducted my research in departments and states within the USCG different from my current workplace. I have worked in different IT departments within the USCG in various aspects that will give me

insight into the different viewpoints and strategies the IT specialists implemented to protect the maritime network for USCG.

Bias is the influence that provides a distortion in a study (Polit & Beck, 2020). According to Bourke (2014), it is reasonable to expect that a researcher's beliefs, political stance, and cultural background may affect the research process. I completed a web-based training course provided by the National Institutes of Health (NIH) and received a certificate protecting human research participants. Also, I adhered to all the ethical protocols presented in the Belmont Report provided by the U.S. Department of Health and Human Services (1979). The Belmont Report has guidelines for researchers to follow based on three fundamental principles: (a) justice, (b) respect, and (c) beneficence (U.S. Department of Health & Human Services, 1979). The principle of justice in research is a fair distribution of burdens and the potential benefits of participation. The second principle of respect allows the participants to volunteer and not force them to participate in the research. The third principle of beneficence maximizes benefits and minimizes harm to research participants (Tajir, 2018).

The Belmont report's foundation was used as an ethical framework for my study. I treated all participants with the utmost respect. I protected participants from any type of harm by maintaining their privacy and confidentiality throughout the study (U.S. Department of Health & Human Services, 1979). Additionally, I provided the participants with all the information necessary about the study to allow the participants to decide to participate voluntarily.

Researcher bias is a concern when performing a qualitative study and should be mitigated to ensure the reliability and validity of the study (Johnson et al., 2019). To ensure reliable data were collected and to reduce bias, I used the reflectivity process, data triangulation by interviewing several participants, document review, and member checking. According to Teusner (2016), the reflectivity process improves research quality and mitigates research biases. Buetow (2019) noted the importance of a researcher's awareness of unconscious bias with participants. Also, I collected the data from multiple sources, using interviews as the primary source and organizational documents such as cybersecurity manuals. At Walden University, member checking is a method of affirming transcribed data from interviews. Member checking assists in validating open-ended interview data (Birt et al., 2016). Therefore, member checking was used to validate the interview data. For this qualitative multiple case study, I used the interview protocol process and collected data from IT specialists working in IT. The interview protocol process included having a prepared set of interview questions and a written script that can be used repeatedly for each participant to ensure I captured the thick and rich description of the data.

Participants

In a multiple case study, a researcher must gain the trust of the gatekeeper by explaining the purpose, procedures, and organizational impact (Joseph et al., 2016). Kay (2019) noted that the gatekeeper provides formal approval for participants to be research subjects. Building a solid rapport with gatekeepers and participants is essential. Therefore, once I obtained IRB approval, I contacted possible gatekeepers of each

organization using LinkedIn, email, and telephone and discussed the study's purpose and the data collection process to ensure there were no company policy violations. In qualitative research, a multiple case study allows the research to have multiple views for a research problem through the participants (Rashid et al., 2019). Comparably, Roache and Kelly (2018) stated that participant selection in a multiple case study is significant in collecting relevant interpretations of specific experiences pertinent to the phenomenon for the research study.

Moser and Korstjens (2018) suggested that a researcher have access to knowledgeable participants about the event. Also, participants can articulate their expertise to answer the research question. Inclusion criteria state that the participants must possess specific characteristics, whereas exclusion criteria would deem a participant inappropriate to participate in the study (Whitehead & Whitehead, 2016). An eligibility criterion was critical to focus on a specific community for this study. Researchers should state the eligibility requirement criteria for selecting research participants (Malterud et al., 2016). For this study, the eligibility was defined for the requirements to align with the research question. The target population for this study was IT specialists. The research participants were selected because they specialize in or have experience with cyber-related strategies to protect the maritime network in West Virginia and Virginia. I used six participants to ensure data saturation was attained. Høyland et al. (2015) noted the importance of developing a strategy to evaluate and gain access to participants.

Onwuegbuzie and Collins (2017) suggested that researchers identify participants who possess specific characteristics. IT specialists were the focal point of the research

due to their similar job roles. Establishing and maintaining a working relationship with the participants was critical to the data collection process. Arsel (2017) noted that the interview procedures, expectations from the participants, and research background establish a rapport between participants and researcher. Høyland et al. (2015) suggested that researchers establish trust and a working relationship by keeping participant information confidential.

Research Method and Design

In this research study, I examined strategies implemented by IT specialists to secure the USCG network for maritime industries from cyber-related threats. The research method I chose for my study was qualitative methodology, and the research design was a multiple case study. The qualitative research method aims to understand phenomena in a real-world setting where the researcher does not attempt to manipulate the event of interest. Hayes et al. (2013) explained that the method selected for any research study should be chosen based on the research goals and the central research question. The research methodology and design adopted were aligned with the research question for this study.

Method

In this study, I chose the qualitative approach to understand a particular event and consider the quantitative, qualitative, and mixed-method research approaches. Qualitative research involves collecting data and interpreting those data based on patterns and trends exclusive to the participants of the study (Hancock, & Algozzine, 2017). According to

Palinkas et al. (2015), a qualitative research method explores and understands a phenomenon that implements evidence-based practice and identifies strategies.

A researcher uses a qualitative approach to help gather information and understand human behavior and perspectives (Kozleski, 2017). Also, qualitative research is inductive and uses a range of data collection and analysis techniques such as interviews and purposive sampling (Gopaldas, 2016). Azungah (2018) suggested using an inductive approach, using the participant experiences that drive the data analysis as the focus for the researcher. Also, the researcher is an instrument along with the participants who contribute to data interpretation and analysis (Denzin & Lincoln, 2008). As noted by Hammarberg et al. (2016), researchers defend the integrity of their work with trustworthiness, credibility, applicability, and consistency. I gathered data during the interviews to understand the participants' views, experiences, and motivations for the specific strategies to secure the USCG network for cyber-related threats by conducting this qualitative research study. The qualitative approach enabled the researcher to explore the strategies used by IT specialists to protect the USCG network from cyber-related threats.

The quantitative method is objective and involves collecting numerical data; the information is quantified and subjected to statistical treatment (Apuke, 2017). The quantitative research method is ideal when factual data are required to answer the research question (Hammarberg et al., 2016). Kiliańska-Przybyło (2018) noted that the quantitative research method is used to investigate answers to questions starting with *how many* or *how much*. I did not choose the quantitative method for this study as this was

typically a more objective approach, and the research question sought to understand human experiences.

The mixed-method research approach combines qualitative and quantitative viewpoints, data collection, analysis, and inference techniques (Schoonenboom & Johnson, 2017). Mixed-method research is a particular case of integration of diversity and divergence using open-ended and closed-ended approaches. In a mixed-method approach, the data are integrated, and the hypotheses should also be integrated (Almalki, 2016). Data integration enables researchers to seek a more panoramic view of the research while viewing the phenomena from different viewpoints (Shorten & Smith, 2017). In the mixed-method research approach, the combined methods assist the researcher in achieving the depth of the phenomenon. The mixed-method includes qualitative and quantitative approaches, but numerical data were not collected; therefore, the mixed-method research method would not have been appropriate.

Research Design

I considered three qualitative research designs: (a) case study, (b) phenomenology, and (c) ethnography. A case study is a research design with a holistic understanding of a phenomenon in its natural, real-life context (Yin, 2017). For this research study, I selected a multiple case study design to assist with the inquiry into the strategies used by IT specialists to protect the USCG network for maritime industries. A multiple case study allows for a more in-depth understanding of the phenomenon by comparing similarities and differences among cases (Heale & Twycross, 2018). According to Yin (2018), when conducting a multiple case study, a researcher should

collect data using the following sources of evidence: direct observation, participant observation, documentation, interviews, and physical artifacts.

Fagerholm et al. (2017) noted that a multiple case study helps improve the credibility of the findings within the study. Constantinou et al. (2017) explained that data saturation is a baseline for researchers to decide when to end data collection. Data saturation occurs when the themes or codes derived from the data set are repeated (Vaismoradi et al., 2016). In this qualitative multiple case study, I interviewed participants from a few organizations and reviewed organizational documents until no new information could be obtained from the data sets. A multiple case study allowed the researcher to collect data to explore IT specialists' strategies to implement best practices to protect the maritime network. I chose a multiple case study for my research to understand the phenomenon through multiple lenses and several sources of evidence.

Phenomenology is a research design that focuses on studying an individual's lived experience for a specific phenomenon (Neubauer et al., 2019). According to Harrison et al. (2017), in phenomenology, researchers commonly use open-ended interviews to explore and understand the phenomenon from the participants' perspectives. Researchers use the phenomenology approach to examine an experience subjectively lived (Sundler et al., 2019). The phenomenological design was not chosen for this study because the focus of this study did not revolve around lived experiences.

Ethnographic research design is conducted to understand the cultural contexts in which human action occurs (Whalen, 2018). Fetterman (2019) believed the ethnographic research design is focused on the predictable, daily patterns of human thought and

behavior. The focus of my research was not to explore the IT specialists' daily patterns or behaviors. Ethnographic researchers collect data through personal observation of participants of a cultural group in their natural setting (Schober et al., 2016). In this research study, the participants' workplace culture and direct observation were not the focal points of the research question. Also, this study did not revolve around any specific cultural group; therefore, ethnographic research was not chosen.

Constantinou et al. (2017) described data saturation as the baseline for researchers to decide when to end the data collection. Data saturation occurs when no new information can be derived from the data sets, and no further coding can be obtained. Thomas and Briggs (2016) suggested that data saturation is received when the data collection ends, and no new themes appear. In this qualitative multiple case study, I interviewed participants from a few organizations and reviewed organizational documents until no new information could be obtained from the data sets.

Population and Sampling

This qualitative multiple case study targeted the population of IT specialists located in Virginia and West Virginia of the United States. The IT specialists chosen were database administrators, systems administrators, and network administrators. Fusch et al. (2018) suggested that the recommended size of participants should include between six to twelve participants to create a diverse group. However, Yin (2017) indicated that a sample size between three and five is sufficient for a qualitative case study. To settle, Tran et al. (2016) stated that the number of participants depends on the purpose of research and the desired analytic level.

In qualitative research, Robinson (2014) believed the initial step towards data collection is to define the population of the study with the use of the inclusion and exclusion criteria. The selected population in this qualitative study included IT specialists with experience implementing USCG standard practices for maritime industries to ensure the USCG network was secured from cyber-related threats. Blaikie (2018) suggested that justifying a sample size in qualitative research indicates a tendency associated with assumptions, logic, forms of data, and data collection methods and analysis. For the sampling method, the researcher selected purposive sampling. Palinkas et al. (2015) suggested that purposive sampling is the preferred method for participant selection in a qualitative study. A purposive sample produces an example of information that aligns logically with the study participants (Etikan et al., 2016). Sarstedt et al. (2018) suggested that purposive sampling is also known as judgmental or selective sampling. Purposive sampling was used to select the research participants and focus on the organization implementing strategies to secure the maritime network. Researchers use purposive sampling to make an informed estimation about the probability of observing a given code at each sampling step (Van Rijnsoever, 2017).

This study's sampling strategy was the homogeneous sampling technique because the general nature of the research question was to explore the strategies used by IT specialists to prevent cyber-related threats on the USCG network for maritime industries. The homogeneous sampling technique is a purposive sampling that researchers use to understand a particular group with similar traits (Barglowski, 2018). Before collecting data, the researcher selected the homogeneous sampling technique to obtain one specific

group with the same occupation within the organization's hierarchy. The eligible participants were contacted through the LinkedIn network or telephone. Semistructured interviews were used to allow the participants to share their experiences on the research topic.

Data saturation is the concept by which further data collection does not lead to any new emergent themes (Saunders et al., 2018). The data analysis software was used to assist in relying upon the participant responses to each interview question. Data saturation in this study was achieved by collecting multiple data sources, which includes interviews and document reviews until no new information can be uncovered through data collection. The interviews were a source for collecting data in this qualitative multiple case study. The location and timing of the interview could impact the quality of the data; therefore, I allowed the participants to select the method of communication: telephone or video conference. Fritz and Vandermause (2018) stated that quality email interviews would improve the interviewing experience for the participant and researcher. Furthermore, organization documents focused on strategies to prevent cyber-related threats against the USCG network to ensure the rich and thick data were captured for this study.

Ethical Research

Ethical consideration is crucial in a qualitative research study due to the study process (Arifin, 2018). The moral protection of human subjects was essential; therefore, ethical research will be conducted in this study. I invited potential participants to participate in the study via LinkedIn, email, or phone after receiving IRB approval, 02-

09-21-0530481 from Walden University. I ensured the participants received a copy of the informed consent form, detailing the following: the purpose of the study, confidentiality, information on non-payment for participation, the researcher's contact information, and the right to withdraw without consequence. The process for withdrawal was explained to the participant, and if they were unwilling to participate at any time during the process, we could stop the interview. No participant was reluctant to participate, therefore removing the participant from the interview process was not conducted. As noted by Chiumento et al. (2016), the informed consent process will ensure that the rights of all participants are not violated. According to Hallinan et al. (2016), the informed consent process enables individuals to voluntarily decide about participation with a clear understanding of the research. Every participant in the study was required to read and sign the informed consent form before participating. The signed copy was given to the participant, and another copy was saved along with the research documents. The signed informed consent form and research documents will be saved on an encrypted SATA external hard drive for five years.

In this study, I ensured that the participants did not receive any incentives, rewards, or payments to participate in this study. Also, to ensure no harm or risks came to the participants of this study, all the IRB legal and ethical requirements outlined by Walden University were followed. The identities of all participants and the organization of the study will be kept confidential. I used code names to replace the actual names of the participants to protect the identity of the participants and the participating

organizations, with Participant A, Participant B, Participant C, Participant D, Participant E, Participant F, Organization A, and Organization B.

Data Collection

Data collection gathers and measures information using a systematic process to answer the central research questions (Kabir, 2016). The information obtained during the data collection process assisted with the meaning, concepts, and definition of phenomena (Dettori & Norvell, 2018). I discussed how the data would be collected using the interview protocol (see appendix B) with the participants. The interview protocol helps improve the reliability of the multiple case study research (Yin, 2017). Furthermore, the data collection methodology was discussed in the following subsections: instruments, data collection techniques, and data analysis techniques.

Instruments

In qualitative research, data collection methods include documents, participant observation, interviews, physical artifacts, archival records, and questionnaires (Yin, 2017). There are four types of interviews: structured, semistructured, in-depth, and focus group (Hamilton & Finley, 2019). According to Crick (2020), the researcher should be the primary data collection instrument in the qualitative research process. In this multiple case study, I requested the participants share organizational documents relating to cyber-related guidelines during the semistructured interviews. In semistructured interviews, the researcher can collect open-ended data and explore participants' thoughts, feelings, and beliefs about the research topic (DeJonckheere & Vaughn, 2019).

Semistructured interviews for this study were open-ended interview questions. The researcher used the interview protocol as guidance to conduct the semistructured interviews. The interview protocol assists the researcher in gathering rich and thick data from the participants. Yeong et al. (2018) stated that a reliable interview protocol is crucial to obtaining qualitative data, increasing the effectiveness of the interview process. The interview protocol (see Appendix B) included the interview questions used during the semistructured interview. Yin (2017) noted that open-ended questions allowed the researcher to have the appropriate instrument for gathering information from participants. Peters and Halcomb (2015) suggested that open-ended interviews assist in the understanding of the phenomenon by focusing on the research question.

I was the primary data collection instrument for this study, gathered all required data sources, and met with the participants to conduct semistructured interviews. Baral (2017) noted that the researcher becomes a human data collection instrument by monitoring and gathering data from interviews. Holtrop et al. (2018) suggested aligning interview questions with the conceptual framework. Pathak and Intratat (2016) expressed that semistructured interviews are the best data collection method for qualitative research to benefit from an open framework. The semistructured interviews enabled me to have two-way communication with each participant to ask follow-up questions to contribute to data collection. In the semistructured interview approach, the participant has flexibility, freedom, and the decision approval of the information disclosed for the interview questions (Pathak & Intratat, 2016). Furthermore, the interview protocol (Appendix B)

ensured that credibility, confirmability, and reliability were enforced, as Kallio et al. (2016) suggested.

As noted by Yin (2017), documentation can expand further and confirm the data collected from the interviews; thus, the organizational documents were best used to explain the data collected during the interview process in detail. The organizational documents used for the study include all the organization's documents relating to cyber-related guidelines and network security. The review of the organizational documents used content analysis to quantify and analyze themes and patterns relevant to IT specialists' strategies to secure the USCG network for maritime industries from cyber-related threats.

Member checking is the technique that allows the participants to confirm the accuracy of my interpretations from the data collected (Iivari, 2018). Birt et al. (2016) denoted that member checking improves the study because participants can identify incorrect interpretations provided by the researcher. I used member checking with participants, and the participants validated my interpretation of the interview data to ensure all accounts were understood for the open-ended interview questions. Sharing the summary of the interview data allowed the participants to validate their responses and make any corrections. Caretta (2016) noted that member checking ensures accuracy during data analysis and data triangulation within a qualitative study. Triangulation aims to enhance the process of qualitative research by using multiple approaches to understand the research topic.

Data Collection Technique

In this qualitative study, I conducted semistructured interviews and documented reviews to better understand experiences through interaction with participants as my data collection techniques. There are several methods for collecting data in a qualitative study (Clark & Vealé, 2018). The data collection techniques included analyzing the organizational documents relevant to the study topic and semistructured interviews. I used the ZOOM video conference for the semistructured interviews to conduct the open-ended questions.

Taylor et al. (2017) suggested that interview protocols guide the researcher in creating procedures and conducting interviews. The interview protocol contained open-ended and closed questions that aligned with the research question. The interview protocol provided the framework from the beginning and end of this study and was a valuable tool for reliability and validity (Yeong et al., 2018). The data collection approach for this study allowed the participants the autonomy of expression to express their practices, beliefs, or opinions while providing reliable and comparative qualitative data. Before starting the data collection for my study, I ensured the IRB and authorization required by Walden University were obtained. Once IRB approval was given to engage with the participants, I began recruiting participants by contacting the gatekeepers with the participant eligibility criteria. Gatekeepers have a pivotal role in ensuring that researchers gain access to potential participants for research (McFadyen & Rankin, 2016). Once the participants were identified, I asked for the participant's consent using

the consent form described in detail in Appendix C; I also initiated the interview protocol guide (Appendix B).

The participants were given the options on how they would like to conduct the semistructured interview. The options were telephone or video-teleconference. Building a rapport and establishing comfortable interactions between the participants and the researcher was crucial in advancing the interview (McGrath et al., 2019). Document analysis was used to review organizational documents related to cybersecurity strategies to protect organizational networks from cyber-related threats. However, I collaborated with gatekeepers for each location, Virginia and West Virginia. The participants were identified, and permission was obtained to access relevant documentation such as standard operating procedures, policies, guidelines, and strategies. The relevant documents provided were all accessible by the public.

The process of identifying and gaining access to the participants was necessary to conduct semi-interviews and review organizational documents (Moser & Korstjens, 2018). Once the participants were identified, I contacted the interview participants by email to schedule the interviews. I used Atlas.ti to capture similar occurrences within the data to identify codes and patterns. The transcribed interview was member-checked by the participant to ensure accuracy. The interview recordings were transcribed into a readable format, using Microsoft Word. The transcriptions allowed the researcher to assess the impact of any missing data due to unanswered interview questions. In the transcriptions, the names and organizations were hidden to ensure privacy and confidentiality. I loaded the data in Atlas.ti qualitative data analysis (QDA) software to

provide the thematic analysis and coding. I contacted the interviewees after the initial interviews to confirm that what was expressed was captured through the member checking process.

I used reliability and validity as a data collection instrument and member checking, and data triangulation for this study. According to Houghton et al. (2015), member checking includes talking with members to gather information, decipher and translate the interview data, and provide participants copies of the decoded data to guarantee the exactness of data captured during the interview. I provided each participant with a copy of my interpretation as a follow-up interview. Madill and Sullivan (2018) noted that member checking is a technique with ideas and perspectives shared by interviewees to ensure that they are captured correctly by the researchers. Therefore, in member checking, any misunderstandings were corrected and updated in this qualitative study. The member checking process helps to ensure reliability and validity within the research process (Simpson & Quigley, 2016).

There are advantages and disadvantages to the use of data collection techniques in this study. The interview method had advantages in obtaining depth information. Ciocănel et al. (2018) stated that face-to-face interviews help build trust between the researcher and the participant. Gill and Baillie (2018) mentioned that telephone interviews are a helpful alternative to face-to-face interviews. However, a disadvantage was that the participant and researcher were not able to see each other. An advantage approach to resolve the ability to see each other was to use software for audio and video, such as Skype, to conduct the interview (Gill & Baillie, 2018).

Data Organization Techniques

This section of the study describes the technique used to organize the data and discusses how to store it securely. Yin (2018) noted the validity and reliability of a qualitative study, and to expose themes and patterns, a researcher uses research noted, research logs, and interview transcriptions. Any audio or video-recorder interview must be transcribed (Sutton & Austin, 2015). The data collected were crucial in the data organization technique process and were characterized by primary sources, such as reflective journals (Chauvette et al., 2019). All data collected were stored on an encrypted storage drive and will be saved for five years and then disposed of after five years. Sutton and Austin (2015) noted that a researcher should maintain field notes to provide important context regarding the participants' impressions, environmental settings, behaviors, and nonverbal actions. I recorded the semistructured interviews using a zoom video conference; Microsoft office applications and Atlas .ti were used to organize the data collected.

According to Merriam and Grenier (2019), qualitative researchers use research logs to note obstacles encountered and ideas emanating from data collected. Meanwhile, Yin (2018) argued that researchers should use notes to document preliminary data interpretations. Atlas .ti was a qualitative data analysis software used for coding and identifying themes in unstructured qualitative data (Friese, 2019). Member checking was used to validate the accuracy of the data collected by the researcher; in return enhanced the credibility of the data provided by the participants (Thomas, 2017). I used a research

log to document emerging themes and patterns, and trends for the data. Research logs were a valuable tool for recording information.

Data Analysis Technique

According to Bengtsson (2016), the purpose of data analysis is to organize and construe meaning from the data collected and extract realistic conclusions. In this study, I provided data analysis to understand the strategies used by IT specialists to implement best practices to protect the USCG network from cybersecurity threats. Qualitative researchers employ software to collect, organize, and examine data from interviews, review documentation, and field notes (Yin, 2018). Raw data were collected through semistructured interviews and using Atlas.ti software. Conversion of the raw data obtained was analyzed to show patterns that were decoded and translated into themes. The researcher's self-reflection is essential for qualitative research to minimize influence bias (Bengtsson, 2016).

Additionally, in a qualitative research study, the researcher generates an in-depth analysis of the data collection better to understand the phenomenon (Watkins, 2017). Yin (2018) suggested that analyzing qualitative data ensures reliability and validity in the data analysis. Davis et al. 2018 stated that triangulation is a strategy used in qualitative research to validate a study by utilizing data from multiple and different sources. There are four types of triangulation: (a) theory triangulation applies to different theories and alternatives theories, (b)methodology triangulation applies to multiple data collection methods, (c) data triangulation is referred to people, time, and space; and (d) investigator triangulation was applied to multiple sets from multiple researchers exploring a

phenomenon (Fusch et al., 2018). To increase validity, enhance credibility, and mitigate bias in this study, I used data triangulation.

The data analysis technique applied in this multiple case study was thematic analysis. Billen et al. (2017) mentioned that thematic analysis assists the researcher in synthesizing qualitative data for the descriptive themes. The data analysis assisted in identifying the patterns in the data collected from the semistructured interviews and organizational documents through thematic analysis. Thoroughly examining the interview transcripts, themes may be identified inductively (Goldstone & Bantjes, 2017). According to Clarke and Braun (2018), thematic analysis is a three-step coding process that involves preparation, organizing, and reporting. The review of each interview and member checking of the transcripts were used to gain a holistic understanding of the data, establishing the research's reliability and dependability during the initial step. Data collected was through semistructured interviews. The software used was Atlas.ti to provide qualitative data analysis to support the sorting, categorizing, browsing, coding, interpreting, and synthesizing of the data (Kalpokaite & Radivojevic, 2020).

Reliability and Validity

The reliability and validity of this study were completed by enforcing the concepts of trustworthiness and consistency. According to Tamul et al. (2020), a study is reliable if the results are repeatable. The creation of data validity refers to the accuracy of the data. According to Yin (2017), the reliability and validity of a case study can be safeguarded with suitable documentation of the research approach and the measures taken by the researcher throughout the research process. A researcher establishing

trustworthiness must use the four dimensions criteria: dependability, credibility, transferability, and confirmability (Forero et al., 2018).

Reliability

In qualitative research, the purpose of reliability is to document detailed procedures as a repeatable measure of a phenomenon (Aravamudhan & Krishnaveni, 2016). Reliability relates to dependability and can be achieved through triangulation (Renz et al., 2018). The interview protocol was used as a strategy to enhance the reliability of this study. Carminati (2018) noted that reliability considers the consistency and accuracy of data within a study; therefore, the interview processes and strategies used ensured that the reliability was captured.

Validity

Validity in qualitative research is the appropriateness of the tools, processes, and data. Research is a process for acquiring new knowledge in a systemic approach with reliability and validity (Garg, 2016). Teusner (2016) believed that validity is important because it allows the reader to believe that the study results are accurate. Strategies to ensure validity in a qualitative study included member checking, detailed description, and data triangulation (Candela, 2019). The audit trail using the Atlas.ti software was used to establish validity in this study. Wixted et al. (2018) stated that detailing the interview protocol and audit trail steps will further validate the study.

Dependability

Dependability in a qualitative study allows someone outside of the research to audit, critique, and recreate (Bongiovanni et al., 2017). In qualitative research, the

researchers enhance the dependability using the same procedures through member checking, data triangulation, interview protocol, and transcript review (Bongiovanni-Delarozière & Le Goff-Pronost, 2017). Moon et al. (2016) stated that detailed coverage of the methodology and methods guarantees readers that the appropriate research practices were applied. Cypress (2017) mentioned that researchers must ensure the research has reliability. The strategies used to provide reliability and trustworthiness in this study included interview recordings and reflective journaling. Member checking was an essential process for establishing dependability in qualitative research for the researcher. The data collection documented for this study and the researcher's thought process in the reflective journal enhanced dependability.

Credibility

Credibility is operationalized through member checking to confirm that the information obtained during the data collection is an accurate interpretation of the delineated experience for the participant (Creswell & Poth, 2016). Establishing credibility was important because credibility determines how the data and the analysis procedures were executed and the nonrelevant data excluded (Bengtsson, 2016). Hammarberg et al. (2016) noted that the credibility of qualitative research relies on the researcher defending the integrity of the study. The researcher establishes and enhances credibility by gathering rich descriptions, member checking, data triangulation, and data saturation (Marshall & Rossman, 2016). Yin (2018) stated that researchers use two sources for data collection to allow data triangulation to support the data findings and improve the credibility and confirmability of the study. Member checking and data triangulation were

used in this research. According to Lub (2015), member checking and data triangulation work simultaneously to ensure the study's credibility. Another area to ensure credibility was accounted for in the research was bias. A researcher must be aware of any bias injected in a qualitative study (Nair, 2018).

Transferability

Transferability refers to the applicability of findings for the readers to connect the elements of a study to their experiences (Cruz & Tantia, 2017). Weis and Willems (2017) state that the researcher should apply techniques that will allow for the generalization or transferability of results beyond the current study. Marshall and Rossman (2016) noted that transferability obtains dependable research results transferable to other settings by someone other than the original researcher. The detailed reports and documentation could be possible for others to transfer findings. Transferability was promoted by maintaining the collected data from the participants, such as the interview records. Moser and Korstjens (2017) mentioned that transferability is enhanced by ensuring rich, descriptive information about participants' experiences and the detailed and maintained research process. Member checking and the interview protocol were used as well to ensure transferability occurs within this study. I detailed the conceptual account in this study using the open-ended questions, sampling strategy, interview protocol, data collection, and analysis.

Confirmability

Confirmability can be demonstrated by way of describing how conclusions and interpretations were established. Also, the findings are derived directly from the collected

data (Noble & Smith, 2015). All participants were interviewed for this study to enhance confirmability. Abdalla et al. (2018) argued the need to promote triangulation to reduce the researcher's influence. Data triangulation and a reflective journal were used for the data collection and analysis process. Data triangulation and the reflective journal will increase dependability and confirmability (Luctkar-Flude et al., 2018). I achieved confirmability and dependability with data triangulation.

Transition and Summary

In section 2 of this study, the study's primary purpose, the target participants, population and sampling, and the methods and processes were used to collect and analyze the explored research data. The purpose of this qualitative multiple case study explored IT specialists' strategies to secure the USCG network for maritime industries from cyber-related threats. Data triangulation will be applied to confirm the credibility of this qualitative study. Section 3 of the study includes presenting findings, implications for social change, a discussion regarding the applicability to professional practice, recommendations for action and further research, reflections, and the study's conclusion.

Section 3: Application to Professional Practice and Implications for Change

This section contains the overview and presentation of the findings for this study. At the same time, describing the major themes that materialized from the data analysis. Also, in this section, I present the applications to professional practice, implications toward social change, recommendations for actions, recommendations to guide further study, reflections, and the conclusion.

Overview of Study

The purpose of this qualitative multiple case study was to explore the strategies IT specialists use to implement standard practices to secure the USCG network for maritime cybersecurity from cyber-related threats. The study was based on GST as the conceptual framework. The target population consisted of six IT specialists across two different maritime organizations in Virginia and West Virginia. Semistructured interviews were conducted with six participants, and 12 publicly available organizational documents were collected. Thematic analysis was used to discover three major themes: (a) adhering to network compliance, (b) promoting adopting cybersecurity standards and best practices, and (c) enhancing cybersecurity awareness and policies. The results of this research study are associated with the literature review findings.

Presentation of the Findings

The overall research question for this study was: What strategies do IT specialists use to implement standard practices to secure the USCG network for maritime cybersecurity from cyber-related threats? The six interviewed participants were IT specialists with expertise as database administrators, system administrators, and network

administrators. I used a pseudonym for each participant and organization: Participant A, Participant B, Participant C, Participant D, Participant E, Participant F, Organization A, and Organization B. I conducted semistructured interviews and collected 12 publicly available organizational documents to analyze using the Atlas.ti software. O'Connor and Joffe (2020) noted that the development of code framing captures the significant features of data in a qualitative analysis phase. Three significant themes (see Table 3) and eight subthemes were found in this research study; data triangulation was used to evaluate the data collected. The following themes of the study emerged after analyzing the data in Atlas.ti software and are aligned with the conceptual framework, GST: (a) adhering to network compliance, (b) promoting adopting cybersecurity standards and best practices, and (c) enhancing cybersecurity awareness and policies.

Table 3

Themes and Their Respective References

Major themes	Participants	Response (%)	Documents	References
Adhering to network compliance	6	100	10	20
Promoting adopting cybersecurity standards and best practices	6	100	10	32
Enhancing cybersecurity awareness and policies	6	100	8	33

Note. % of response means the proportion of responses by participants for each theme. References mean the frequency by which each subtheme was mentioned or alluded to in the documents.

Theme 1: Adhering to Network Compliance

The first theme, adhering to network compliance, supports the data analysis of the need to adhere to network compliance and aligns with the literature. IT specialists must establish strategies to implement standard practices to secure the USCG network and adhere to network compliance. All participants expressed a standard network policy that each IT specialist should comply with to protect the USCG network from cyber-related threats. According to Kerner (2017), cybersecurity standards and practices have helped decline network vulnerabilities. According to Buchanan (2019), the GST theory interprets and views connected units as a whole system. Three subthemes materialized from the data for the theme adhering to network compliance (see Table 4): (a) security and protection, (b) cybersecurity prevention, and (c) network monitoring. The GST, which served as the conceptual framework, focuses on adhering to network compliance because of one principle: the interrelationship between objects in a network.

Table 4

Subthemes for Adhering to Network Compliance

Subthemes	Participants	Response (%)	Documents	References
Security and protection of the network	6	100	10	25
Cybersecurity prevention	6	100	11	27
Network monitoring	6	100	10	23

Note % of response means the proportion of responses by participants for each subtheme. References mean the frequency by which each subtheme is mentioned or alluded to in the documents.

Subtheme: Security and Protection of the Network

The importance of understanding the security and protection of the network was a subtheme discussed by every participant. According to all study participants, security and protection of the network are vital for IT specialists to ensure their internal and external networks are compliant within their organizations. Participant A stated:

> A few years ago, in 2017, our leadership decided to move all of our different network assets to a more centralized virtual platform. Doing so gave us the ability to better leverage and manage our information systems' integrity, security, and availability.

Participant B presented a similar view about network security by elaborating "that the data center consolidation completed by Organization A established network segments. A network segmentation includes different enclaves and firewall rules for an organization."

The study shows that this approach is a standard practice that allows the USCG to leverage the multitenant environments and enhance network security. In return, this approach provides security and protection for the network. In alignment, Participants A and B explained that when Organization A completed the data center consolidation, the IT specialists managed its integrity, security, and availability for the USCG network to secure it from cyber-related threats. In addition, Participant C stated:

> One of the standard practices that I used to protect the network communication infrastructure that I administer is segregating the network from outside traffic. So I control what comes in and what goes out, and because of the sensitive

> information that we utilize in our network, we know we do not want that to get out. So also network segmentation from OT environment.

Additionally, Participant C explained that Organization B also completed a data center consolidation, resulting in network segments and tokens as a second layer of security as a network administrator. Network administrators can control the flow of traffic between the subnets to protect the organizations' networks.

A few of the participants emphasized the security and protection of the network by providing the standard practices their organizations use. Participants D, E, and F believe complex passwords are strategies for security and network protection. Similarly, Participants B, C, and E advocate that password policies prevent users and IT specialists from selecting weak passwords. Participant D expanded on complex passwords: "My organization has made many changes to the policy for changing passwords, such as ensuring the IT specialist changes system and admin passwords every 60 days. However, for financial systems, it is now 35 days." Emphasizing the effectiveness of security and protection of network, Participant D stated,

> One of the recent things that we have done as an organization was to change the policies on changing passwords for different applications. For example, we set the passwords for service accounts to change every 60 days to a different password.

Participant E added that admins have additional multifactor authentication layers, such as jump host, since the data center consolidation. In comparison, Participants D and E mentioned that passwords are cybersecurity prevention that Organization A and B have incorporated. However, according to Participant D, Organization A changed its policy on

changing passwords for different applications. Participants E and F described the security and protection of the network in their organization, and network security has become the number one priority by improving the strategies used to protect the network. The participants indicated that security and protection of the networks, such as network segmentation, were the best practices for Organizations A and B to secure the USCG network.

Ten of the publicly organizational documents emphasized the significance of the network's subtheme security and protection. The documents conveyed that the proper network segmentation is an effective security mechanism to prevent an intruder from transmitting exploits. The document Securing Network Infrastructure Devices_CISA revealed the virtual segmentation uses the same design principles as physical segmentation. The document also mentioned that existing technologies could prevent an intruder from breaching other internal network segments. Additionally, according to the publicly organizational document, NIST's SP 800-63B Section 5.1.1.2, Memorized Secret Verifiers used during data triangulation, an organization should ensure passwords are at least eight characters long. The NIST's SP 800-63B Section 5.1.1.2, Memorized Secret Verifiers, also mentioned that many organizations have failed to implement password change intelligence guidelines, such as password length and complexity (Grassi et al., 2020).

The subtheme of security and protection of networks was found in the literature. Marinos et al. (2021) acknowledged that the Office of Management and Budget's federal chief information officer (CIO) launched the Federal Data Center Consolidation Initiative

and the Data Center Optimization Initiative. Network segmentation is an architectural design approach that divides a network into multiple subnets to improve the efficiency and security of the network (Musman & Turner, 2018). Prior researchers, Musman and Turner (2018), noted the network segmentation prevents unauthorized network traffic or attacks from reaching portions of the network to prevent access and make monitoring the network traffic easier. The security and protection of the network is a strategy that reinforces the assets in the network. Participant A's and Participant C's responses align with the organizational documents for the segregated network. The participants added that the segregation of the network uses roles and functionality at their organization.

Recent studies acknowledge that password policy could be enforced with the following requirements: (a) Minimum of 11 characters; (b) upper and lower letters, symbols, and numbers; and (c) different from a username (Nieles et al., 2017). A strong password must contain all the necessary elements involving the combination of letters, numbers, and special characters. Halima et al. (2018) mentioned that passwords are a cyber-security measure users experience and remain challenging to manage. IT specialists' passwords and not a hash algorithm are considered weak cybersecurity (Guo et al., 2019). All public organizational documents and recent literature reviewed were in alignment for the security and protection of the network. The IT specialist responsible for the security and protection of the network should understand the tools and methods used as strategies to enhance the security of the USCG network.

Researchers have identified that change management is vital in maintaining network security using network security assessment. According to de Bruijn and Janssen

(2017), security and the protection of the network are an issue if the change management is not in place. The increase of organizations using computer networks has increased challenges to network security (Mihalos et al., 2019). Nieles et al. (2017) mentioned the network security provides strategic support for other parts of the infrastructure. Network security is the act of protecting the network against any threats that may lead to a compromised network (Amrollahi et al., 2020). Also, in the literature, Abdullahi (2018) acknowledged that security policies and network protection should be enforced with confidentiality, integrity, and availability.

The subtheme, security, and protection of the network align with the GST conceptual framework. In the GST, each phenomenon provides a dynamic framework to understand the interaction patterns in networks of interdependent agents that are bound (Turner & Baker, 2019). According to von Bertalanffy (1968), involving holistic views creates a system as a whole, which cannot be broken down into parts. This study's findings recognized that segmentation networks create smaller network systems that are part of the overall network; more recent literature confirms that network segmentation simplifies information security for each network (Musman & Turner, 2018). In addition, when viewing this phenomenon through the lens of GST, findings from this study indicate that IT specialists have strategies to implement standard practices to secure the USCG network for maritime cybersecurity from cyber-related threats. By utilizing the GST as the conceptual framework for this study, IT specialists can institute more effective strategies for best practices to secure the USCG network from cyber-related threats. Blokland and Reniers (2020) noted that GST is an essential foundation for

security and safety in the literature. Organizations must have strategies for best practices to protect their network.

Subtheme: Network Monitoring

Network monitoring was the second subtheme to emerge from adhering to the network compliance significant theme. To secure the USCG network, the lack of best practices from IT specialists is a significant challenge. Without a standard practice monitoring the USCG network, the infrastructure will not be protected from cyber-related threats. Participant A said, "Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are tools that are to be implemented to monitor real-time network traffic as a standard practice with the USCG." Participants B, C, and E mentioned that IDS monitors their organization's firewall logs. Another aspect of network monitoring is a wireless sniffer tool. To underline the significance of different network monitoring, Participant E mentioned that organization B has a DSL tool that analyzes wireless traffic and decodes the packets sent over the network. Participant C also noted, "To ensure important information will not end up in the wrong hands, organization B strives for the IT specialists to monitor, monitor, and review the logs from the SIEM tool." Participant A and Participant B also mentioned that organizations A and B have Security Information and Event Management (SIEM) tools to monitor the entire infrastructure, such as network, servers, and database.

The subtheme of network monitoring was supported in the literature. Kwon et al. (2020) mentioned that real-time monitoring using a monitoring dashboard would provide a single holistic view for identifying a cyber-related threat. Prior researchers believe IDS

is essential in providing network security and collecting logs by identifying possibly network intruders. Ikram and Cherukuri (2016) argued that IDS are critical for identifying and tracing network interlopers. In addition, IT specialists should log and monitor all significant events on the network to actively respond to cyber-related threats. In the literature, Singh and Kumar (2018) acknowledge that network administrators must keep a log of the network's performance, functionality, and security. SIEM provides a holistic view by collecting data and using matching patterns. The SIEM uses logs collected of events from servers, network devices, firewalls, and intrusion detection and prevention systems. (Sekharan & Kandasamy, 2017). Sekharan and Kandasamy (2017) also mentioned that IDS/IPS focuses on monitoring logs, incidents, and processes attempted to terminate from the network, servers, or database

The subtheme of network monitoring aligns with the GST conceptual framework. In the GST, the holism principle was shown in each function within the subtheme of networking monitoring. The SIEM tools support the overall network objectives of external changes coming into a system and the components of adjusting the environment (Teece, 2018). The subtheme was supported by the literature uncovered during the literature review. Prior researchers, participants, and documentation have identified how IT specialists should use network monitoring using GST as a strategy to implement best practices to protect the USCG network. The data from the participants' responses and publicly organizational documents align with the conceptual framework, GST.

Subtheme: Cybersecurity Prevention

Cybersecurity prevention emerged as the third subtheme. The subtheme cybersecurity prevention exposed the strategies used by the IT specialists to implement standard practices that may need better cybersecurity prevention practices. The participants identified the strategies that have been used but did not protect the network from cyber-related threats. Participant A mentioned, "A method IT specialists used that failed to prevent cyber-related threats was the SolarWinds network appliance. This application allowed backdoor access to numerous federal networks without being detected for some time".

Participant B mentioned that network segregation is called enclaves at organization A. The firewall rules are created at organization A to prevent cyber-related threats and hackers from moving to different environments or enclaves. Participants B, C, and D acknowledge firewalls as standard practices that are least effective in protecting the USCG network. Participant C mentioned that an organization should never allow any machine on the control network to talk directly to a machine on the business network or the internet. Participant D believes passwords are the least effective strategy to protect the network from cyber-related threats when correlating security and network protection with cybersecurity prevention. Participant D noted:

> Before changing our current password policy, we would keep resetting the service account to the same passwords, which was secure, but it was meeting the policy. Now, we are mandated to change the password by five characters, so we do not

> use the same password. Even though my organization changed the policies on passwords, I still believe passwords are the least effective strategy.

The avoidance of compromising confidentiality, integrity, and availability includes security metrics. Participant C mentioned that security metrics are a powerful tool for maritime industries to evaluate the effectiveness of protecting computer networks. One of the publicly organizational documents' Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring supported Participant C's claims that security metrics should be repeatable and reproducible. In 2021, participants C and D stated their organization under DHS created a "red team." Participant D mentioned:

> My organization's red team looks at our system from a holistic IT point of view. They attempt to identify and exploit and potential weaknesses. I thought it was incredible that my organization created a red team because, in 2015, they tried something similar with a Cyber Crisis Action (CAT)/Operation Blue Team.

Biswas and Mukhopadhyay (2018) noted that the evaluation for cybersecurity prevention could forecast vulnerabilities using metrics. Participant F noted the security metrics include the following:

1. Common Vulnerabilities and Exposures on the system and network
2. The mean time between a security patch release and actual implementation
3. Policy violation
4. Number of employees that have completed security training

One of the most reliable concepts proposed by Conteh and Schmick (2016) on

cybersecurity protection is to design layers of defense.

The subtheme of cybersecurity prevention was found in the literature. Cybersecurity prevention can protect the network from various attackers and threats by applying a holistic view (Allodi & Massacci, 2017). IT specialists have strategies that may have failed were implemented for the organization, so cybersecurity prevention materialized from theme one. Al-Mohannadi et al. (2018) acknowledge that maritime cyber-related threats could arise in data patterns via communication exchange. Davis (2021) noted that SolarWinds customers downloaded a software product with a malicious backdoor. In 2020, the Cybersecurity and Infrastructure Security Agency (CISA) released an emergency directive with mitigations factors (Cooper, 2020). Damanpour (2020) mentioned that the CISA issued an emergency directive in December 2020 explaining that an advanced persistent threat actor had compromised the network management software suite by inserting a backdoor. Bodnar and Hanlon (2020) reported that Einstein's intrusion detection system failed to detect the Solarwinds because it analyzes network traffic flowing but not encrypted network traffic. Some researchers believe cyber-related failures are due to cybersecurity best practices not being pondered during the implementation of network security (Tam & Jones, 2019).

Mhaskar et al. (2021) believe firewall policies are based on network segmentation and should be placed in the network for a Defence in Depth (DiD) strategy. On the contrary, Mihalos et al. (2019) propose that firewalls strengthen the network, but organizations should look for more effective approaches. The researchers noticed that organizations should recognize violations in the literature and review the firewall settings

to prevent cyber-related threats (Clarke & Knake, 2019). Another preventive cybersecurity policy mentioned found in the literature is email encryption. Email encryption is a security control that assures that the information sent across the network is safe and secure and obtained only by the authorized individual. Allowing spam emails on the network may cause network congestion. Shapiro et al. (2018) discussed methods for security measures to prevent weak authentication in a network. A cyber-related organizational document mentioned that organization A reported a spoofing attack that impersonated the organizations' email addresses and malicious files. The malicious file caused the network to be compromised and resulted in additional spoofed emails.

Herring et al. (2019) described recent literature and how the 2019 Ryuk ransomware affected the IT network for Maritime Transportation Security Act (MTSA) facility operations. The Ryuk ransomware was successful by embedding the malicious link through email. A user with the USCG clicked the licked, and the ransomware virus could corrupt the enterprise IT network files. The virus also disrupted the industrial control systems that monitored and controlled the process operations. Lykou et al. (2019) noted that preventive cybersecurity protocol would allow users who had received malignant emails to report the attacks voluntarily.

Additionally, Tsokkis and Stavrou (2018) mentioned that a false sense of security could occur when users and administrators adhere to password policies in an insecure way. The public organizational documents support the cybersecurity prevention for networks subtheme. Out of the 12 documents reviewed, nine of them validated that cybersecurity prevention is critical for an organization, and cybersecurity policies should

be implemented to avoid compromising confidentiality, integrity, and availability. Through the scholarly literature, vulnerability patching is a significant effort to ensure cybersecurity prevention is in place. Biswas and Mukhopadhyay (2018) mentioned that organizations need to mitigate cyber-related threats by identifying and patching vulnerabilities regularly through accurate techniques and investing in standard strategies. All the participants agreed that patching vulnerabilities are a safety measure for cybersecurity prevention. IT specialists need to stay on top of the latest and greatest patches for vulnerabilities on the network.

On the contrary, the Office of Inspector General reported in 2019 that the DHS has failed to apply security patches for the last ten consecutive years properly. Heckman (2021) noted that the USCG transformed the cyber-CAT blue team into a cyber operational branch and formed a red team. The red team will work with the IT specialists at each location to provide the following:

1. Identify misconfiguration and gaps in existing security products
2. Strengthen network security
3. Elevate awareness among staff
4. Evolve the organization's security strategy
5. Identify unique weaknesses and vulnerabilities within the system and network

The participants' responses and the publicly organizational documents support updating the network systems are critical in adhering to network compliance and having cybersecurity prevention.

The subtheme of cybersecurity prevention aligns with the GST conceptual framework. According to Kosiński et al. (2019), GST aligned with the network's security to propose better cybersecurity prevention strategies and implement best practices. The holistic system approach should be applied when applying cybersecurity prevention. The GST framework was relevant in evaluating cybersecurity prevention as it highlighted the strategies used to secure the USCG network. The data from the participants' responses and supporting literature align with the conceptual framework, GST.

Theme 2: Promote Adopting Cybersecurity Standards and Best Practices

The second theme that emerged during data analysis was the need to adopt cybersecurity standards and best practices. Adopting cybersecurity standards and best practices as a means for effective communication and interactions to improve cybersecurity is necessary to prevent cyber-related threats (Choi, 2016). As standard practice, most organizations adhere to a set of security practices and processes to ensure the network always remains safe (Benaroch, 2018). In recent literature, Syafrizal et al. (2020) defined cybersecurity standards as a set of technical rules to protect cyber environments and users in organizations with internet connections. In 2019, the DHS reported that cybersecurity threats to critical infrastructure are among the most significant strategic risks for the United States. DHS (2019) promoted the adoption of standard cybersecurity policies and best practices that are risk-based and responsive to the ever-changing cyber threat environment.

Adopting and enforcing security policies was a theme all six participants discussed and noted was crucial. Four publicly organizational documents referred to the

theme of promoting the adoption of cybersecurity standards and best practices. Participants B, C, and E mentioned, senior leadership focuses on automated tools to manage network security. Also, according to Sohrabi Safa et al. (2016), senior leadership manages information security by using technological approaches. The subthemes highlighted in Table 5 materialized from data triangulation were (a) management support and leadership, (b) strategic planning for cyber-related threats, (c) technology control and accessibility.

Table 5

Subthemes for Promote Adopting Cybersecurity Standards and Best Practices

Subthemes	Participants	Response (%)	Documents	References
Management support and leadership	6	100	10	25
Strategic planning for cyber-related threats	6	100	11	27
Technology control and accessibility	6	100	10	23

Note. % of response means the proportion of responses by participants for each subtheme. References mean the frequency by which each subtheme is mentioned or alluded to in the documents.

Subtheme: Management Support and Leadership

The subtheme management support and leadership materialized to ensure cybersecurity awareness and best practices are at the forefront of the organization. Participant E stated, “Management support and leadership is senior leadership not understanding security regarding the security standards.” Participants B, C, and D noted

that having management support would better prepare them to secure their organizations' networks from cyber-related threats. Participant C mentioned:

> If we knew about the security protocols and were provided updates by the senior leadership, we would know which standards and best practices to use when there is a cybersecurity breach. It is not easy to protect the network when trying to figure out the best practices rather than the documented practices.

Participant B indicated that "in an organization, senior leadership should be familiar with the NIST risk management framework to improve security within the organization." Three participants believe the lack of committed senior leadership and the unattainable critical cyber-related prevention tools could circumvent network security. Participants B, E, and F believe that they did not receive adequate support from their top management regarding funding for the hardware and software required to protect the network from cyber-related threats and training. Participant E mentioned, "Senior leadership needs to communicate with us and approve cybersecurity policies, risk management registry, and vulnerability remediation plans. We are not able to align our processes with our organizations' policies and processes."

Several participants mentioned various ways that senior leadership can communicate with IT specialists and the workforce. Four out of six participants emphasized that senior leadership should do an annual review of the tools and strategies to ensure they are valid and collaborate to adopt cybersecurity standards and best practices.

The subtheme of management support and leadership was found in the literature. Prior researchers indicated that senior leadership's support is needed to correct human errors, negligence of security practices, lack of awareness programs, and lack of training (Palinkas et al., 2015). According to Garcia et al. (2017), management support should include: assigning responsibilities, setting timelines, allocating resources, and establishing accountability mechanisms. In addition, senior leadership is responsible for taking a holistic approach to cybersecurity that includes both technology and policy (Soomro et al., 2016). Kalhoro et al. (2021) mentioned that IT specialists are not sufficiently skilled, which causes organizations to outsource cybersecurity protection to a third party. If the network security is outsourced, senior leadership cannot manage the security management, and there would be a lack of effective management for the network security. The ability to develop standard practices and provide the capability to audit those standard practices through the security controls is the responsibility of senior leadership. Soomro et al. (2016) mentioned that senior leadership owns the decisions for accepting the implications of strategic decision-making with implementing the cybersecurity standards. As Soomro et al. (2016) suggested, senior leadership should leverage existing security policies to support the IT specialists. The organization's culture on security awareness and cybersecurity policies is based on the guidance and actions of senior leadership.

The subtheme management support and leadership align with the GST conceptual framework. The approach supports the conceptual framework, GST, by ensuring that a protection measure is in case IT specialists perceive a cyber-related threat. Mishra et al.

(2019)) highlighted the need for senior leaders in an organization to support strategies that can identify and secure all networks from cyber-related threats. The senior leadership should emphasize security awareness education and training.

Subtheme: Strategic Planning for Cyber-Related Threats

Strategic planning for cyber-related threats emerged as a subtheme. Strategic planning for cyber-related threats is a way for organizations to assess the level of threats they may face. All the participants agreed that the USCG should have a strategic plan for cyber-related threats. Cyber-related threats such as external and internal attacks, hacking, password theft, malware, and data mishandling are critical components organizations should use for strategic planning. Participant C noted that Organization B's network administrators are expected to use the same overall adopted USCG cyber strategy as other organizations within the USCG. Also, participant C mentioned:

> Applying the same strategies for a platform as a service (PaaS) versus software as a service (SaaS) is challenging. There are several entities that the IT specialists administer within the organization, and it would be challenging to have a one size fit all strategic plan.

Organizational security policies must specify how employees and users of information resources need to behave to prevent, detect, and respond to security incidents (Cram et al. (, 2017). Participant F states, "Our strategic plans and policies will assist senior leaders and IT specialists on how to deal with cyber-related threats." The National Guard Bureau has established the Cyber Mission Assurance Team (CMAT) program to protect critical infrastructure connected to military installations (Healey & Korn, 2019).

The subtheme of strategic planning for cyber-related threats was supported in the literature. In prior literature, Yang et al. (2016) noted that effective and consistent IT strategic planning is a model of the organizational culture. In recent literature, San Nicolas-Rocca and Burkhard (2019) define strategic planning for cybersecurity policy as a document identifying rules and procedures that guide how the organization's IT resources and assets are accessed. The CISA works with federal agencies to promote standard policies and best practices to respond to cyber-related threats effectively. In the literature, Verma et al. (2018) believe an organization should align an organization's strategic plan with the people, processes, and technology to mitigate risks from cyber-related threats. Therefore, a strategic plan emphasizes the need to establish standard practices and policies for IT specialists. The standard practices and policies should be guided by its senior leadership and employees' organizational security awareness.

The subtheme, strategic planning for cyber-related threats, aligns with the GST conceptual framework. Von Bertalanffy's concept for GST recognizes that an organization needs to interact with its external environment. Viewing the theme of information security planning through the lens of GST, the USCG with adequate strategic plans will holistically contribute to a secured network environment. In alignment with the holism concept of GST, Barca (2017) stressed that any information security system that fails to function entirely results in a breakdown of its defenses.

Subtheme: Technology Control and Accessibility

Technology control and accessibility were a standard subtheme to secure the USCG network from cyber-related threats. For example, participants A, B, and D

mentioned the technical controls that organization A employs: two-factor authentication, intrusion detection software, vulnerability scans, and audit logging to secure the USCG network from maritime cyber-related threats. Participants A and B and recent literature also noted that technical controls protect unauthorized access, supporting security requirements for network devices, applications, and data (Aldawood & Skinner, 2019). Participant D noted:

> I believe firewalls and privilege access for administrators are necessary to have as a tool. Both of them allow protection, and privileged access improves the security controls on the network. We have to log in with multi-factor authentication and then again with our tokens to become an admin on the network.

Participants from all cases shared that using technical controls is a means of protecting the USCG network. Participant E mentioned:

> We have audit logging as a tool. We use it to capture the events, actions, and activities on the network. We have hundreds of servers that we manage, so we have to review a volume of audit logs. When the audit logs are configured correctly, they are beneficial.

All the participants noted, their organization uses technical security control tools, but a few mentioned that not all IT specialists may have access to those tools.

The subtheme of technology control and accessibility was supported in the literature. In the literature, Mihalos et al. (2019) added that technology control is one of the most well-known network security mechanisms for protecting the network. In recent literature, Butavicius et al. (2020) inferred that technical controls could reduce

vulnerabilities, but no technology provides absolute protection from cyber-related threats. The analysis of organizational documents and my review of the participants' responses indicated that technical controls are critical solutions to address cyber-related threats and lead to a more secure network. The literature supported the usage of technical security controls. While also highlighting audit logs to be reviewed for unusual activity, user accounts creation, control lists access, two-factor authentication, and intrusion detection software. In recent literature, Liu et al. (2021) supported the need for technical controls by describing networks having cyber-related threats because of passwords. The technical security controls in place are IDS, audit logs, and standard configuration and security reinforcement. Skilled IT specialists should maintain the accessibility to those tools to regularly analyze the logs to detect abnormalities (Liu et al., 2021).

Additionally, Nieles et al. (2017) mentioned that technical controls should be prescribed to protect the system's confidentiality, availability, integrity, and information. The technical security controls improve the authentication mechanism on the network between internal and external components. Adopting technical security controls should reduce cyber-related attacks, and the analysis of the logs will ensure that the internal and external components of the network are secure. The participant's responses and the organizational documents supported technical controls and access to protect the USCG network. Soomro et al. (2016) indicated in the literature that organizations should have technical security controls to protect the network and prevent the increase of cyber-related attacks. Participants in this study indicated that using technical control and having accessibility to use a tool for implementation for network security.

The subtheme technology control and accessibility align with the GST conceptual framework. The GST conceptual framework was valuable to this study because it demonstrates the value of IT security technical controls. GST is a system that looks at the interaction of related instruments that influences the cooperation of all parts. Aligning the GST as the conceptual framework for this study, the IT specialists establish a more effective strategy by depending on the entire Cybersecurity policies have financial costs that evolve as new technologies for managing cyber-related threats (Blum, 2020). For organization A as relies on the documents, it uses Domain-based Message Authentication Reporting and Conformance (DMARC) as the authentication method for their official organizations' emails.

Theme 3: Enhancing Cybersecurity Awareness and Policies

The final theme to emerge during the data analysis phase of the study was cybersecurity awareness and policies. The concept behind cybersecurity awareness and policies is vital in protecting the network from cyber-related threats. The subthemes under this theme include certification requirements and training and security awareness. The literature characterized cybersecurity awareness as contextualized due to the behavior of humans to protect information processed by the organization through compliance and security policies (Burns et al., 2017). Table 6 highlights the subthemes under the enhancing cybersecurity awareness and policies theme.

Table 6

Subthemes for Enhancing Cybersecurity Awareness and Policies

Subthemes	Participants	Response (%)	Documents	References
Certification requirements and training	6	100	10	25
Security awareness	6	100	11	27

Note. % of response means the proportion of responses by participants for each subtheme. References mean the frequency by which each subtheme is mentioned or alluded to in the documents.

Subtheme: Certification Requirements and Training

Certification requirements and training emerged as a subtheme of enhancing cybersecurity awareness and policies. The importance of certification and training requirements entails details for IT specialists managing the USCG network. All the participants confirmed that their organizations require information assurance certifications from the DoD 8570 policy. Participant E stated:

> The IA certifications must be renewed every three years, but some five years. It depends on the certifications. However, it would be good if my organization provided on-the-job training for IT specialists based on the job role. The certifications are on theory only, but each organization is different, so we need training based on the policies set by CIO.

The participants defined continued professional education (CPE) for certification renewal as a way for IT specialists to keep their knowledge and skills current. Participant B said:

> It is hard to receive cybersecurity training when we are acting in multiple roles. My organization is short in skilled federal staff, and they add government

> contractors. However, there are specific jobs contractors cannot hold in the federal government, so, therefore, we have to have multiple roles.

Due to IT specialists not having the correct certifications and training, the system will not function efficiently. Cybersecurity constantly evolves, which shifts the perspective of threats, vulnerabilities, and countermeasures. In return, IT specialists with federal organizations should engage in continuous education to remain current in their skill set.

The subtheme cybersecurity requirements and training were supported in the literature. In the early 2000s, DoD established the Cyber Workforce Management policy called DoD 8570. This policy requires IT specialists to train and obtain an information assurance certification to perform their job requirements on the network (Leenen & van Vuuren, 2019). One of the organizational documents indicated that cybersecurity workforce functions must be identified and managed and that the personnel is performing cybersecurity functions (DoD Directive, 2020). He and Zhang (2019) believe an employee should receive adequate cybersecurity training to ensure productivity increases for the organization. In recent literature, Li et al. (2019) support the need to communicate between IT specialists and external teams to bring awareness for cyber-related threats to support and maintain efficiency. The GAO believes the federal government should have a better understanding of the desires of the cybersecurity workforce. Providing training and bonus pay for additional certifications benefits recruiting and retaining IT specialists (Marinos et al., 2021). However, Knapp et al. (2017) noted that professional and vendor certifications do not replace experience or education.

The subtheme certification requirements and training are closely associated with the conceptual framework, GST. The GST conceptual framework requires a system to be functioning at its highest efficiency when all parts of the system are working correctly (von Bertalannffy, 1972). Additionally, cybersecurity issues continue to evolve, so no standard base of knowledge or technical skills will allow one IT specialist to handle all cyber-related threats unless continuous training is completed. The certification requirements and training support the GST conceptual framework by ensuring IT specialists understand human behavior under IT threats. The IT specialists are a complex subsystem of the USCG network. Bertanlaffy (1972) described GST as a system with inputs and outputs. The certification requirements and training will be the inputs through a GST conceptual framework lens, and the IT specialist's performance should be considered the output.

Subtheme: Security Awareness

Security awareness is a concept that emerged as a subtheme of cybersecurity awareness and policies. The subtheme security awareness supports cybersecurity operations in cyber defense (Lagouvardou, 2018). Education and training are critical to ensure employees know the risk and responsibilities of protecting information technology assets (Dawson, 2018). Participant D stated, "Security awareness and training programs to be used as an effective strategy to implement cybersecurity policies by an organization." Participants A, C, and D noted that communicating security policies should go further than employees and vendors. The participants also suggested that the IT specialist should be educated on security policies and procedures, but the users, since

everyone plays a role in securing their data. According to Mishra et al., security lapses within their organizations resulted from a lack of security awareness. According to Yang et al. (2018), successful security awareness training should be adaptive and interactive, such as providing on-the-job training or mentoring program. Halibozek and Kovacich (2017) noted that cybersecurity awareness could decrease human error, identity threat, internet fraud, and misuse of digital assets. Participant D mentioned, “Security awareness should be explained to the IT specialists to understand the exact cybersecurity policy to develop standard practices. If we were informed better, we would be able to handle the cybersecurity threats for our organization better.”Participants E and F proposed that the cybersecurity policy would improve the overall standard practices if the organization identified the key elements to protect the USCG network using security awareness.

The subtheme, security awareness, was supported in the literature. In prior literature, Li et al. (2016) noted that humans play a role in ensuring the defenses are in place, detecting cybersecurity attacks immediately, and taking security measures as soon as the attacks are known. In the literature, researchers mentioned that the lack of security awareness and the erroneous classification of cyber-related threats presents cybersecurity risks (Tam & Jones, 2019). Dubosson et al. (2019) stated that security awareness ensures that employees thoroughly understand the consequences of failing to protect the organization from outside attackers. Security awareness is an effective strategy for creating a security culture and ensuring the IT specialists and the users understand the organizational processes and policies. All six participants and seven of the twelve

documents collected revealed that cybersecurity awareness training is crucial to cybersecurity and network compliance success.

The subtheme of security awareness aligns with the GST conceptual framework. Security awareness is a concept closely associated with GST. GST consists of the system working together. Security awareness training is considered an input and interaction mechanism with a system. According to Kim and Kim (2017), security awareness attains compliance behavior using a cybersecurity mechanism through materials and support infrastructure. Security awareness relies on the IT specialists, users, and senior leadership's understanding of the respective technologies and the awareness's potential cause and possible effects. The perspective between IT specialists and the security awareness programs must be aligned to ensure the organization adopts proper awareness training.

Applications to Professional Practice

The specific IT problem was the perceived assumption that IT specialists lack strategies to implement the standard practices needed to secure the USCG network. The findings in the study resulted in critical themes and subthemes that IT specialists could use as strategies to implement standard practices. The findings were compelling and supported current literature on network compliance and cyber-related threats, and organizational documents. Findings from this study are crucial to IT specialists, network compliance, and cybersecurity standards and practices in maritime industries. The findings are relevant to IT specialists and senior leaders who can use the strategies revealed in the study to mitigate the cyber-related threats to the USCG network. The IT

strategies found in the literature and confirmed by the participants are (a) network and security protection, (b) technical controls, (c) buy-in from senior leaders, (d) certification requirements and training.

The study revealed three themes: adhering to network compliance, promoting cybersecurity standards and best practices, and enhancing cybersecurity awareness and policies. Based on the evidence in the study, the critical factors with renewed insight io improving cybersecurity strategy to include new ideas on network compliance and security awareness training programs with buy-in from senior leaders. The essential cybersecurity factors revealed in this study provide an advantage to the IT specialist's and senior leaders' awareness and understanding to impact the workforce and enhance existing strategies.

The study identified the three themes as essential to network compliance and best practices on the network. IT specialists may use this knowledge to implement strategies for cyber-related threats on the USCG network. Security policies and strategies are constantly updated to reflect the evolving cyber-related changes (Nieles et al., 2017). The key factors were identified and discussed for each theme that encourages the detection of improved best practices. The critical strategies from this study may improve standard practices to facilitate adapting the current tools, technical controls, and security awareness.

Implications for Social Change

The study findings indicate there could be some improvements to strategies used by IT specialists to implement standard practices to secure the USCG network for

maritime cybersecurity from cyber-related threats. By utilizing strategies discovered in this research study, social implications will assist IT specialists in standardizing best practices. Improvements in the protection of the USCG network may reduce the unauthorized exposure to maritime industry operations and privacy protections by the community and society. The implication for social change may include the need for USCG to develop tools that will detect cyber-related threats, monitor the USCG network, and prevent adverse effects for the maritime industries. Implementing best practices might affect how the IT specialists secure the USCG network by providing efficient strategies that every IT specialist could use to obstruct cyber-related attacks further.

Another social implication is the inherent issue with IT specialists in cybersecurity positions. During the one-on-one semistructured interviews with the participants, it was discovered that there was a shortage of qualified IT specialists. In recent literature, Kam et al. (2020) reported that the (ISC)2 Cyber Security Workforce study materialized a shortage of over a million cyber security professionals globally. In this doctoral study, it became apparent that there is a lack of IT specialists that could protect the USCG network. This study aimed to explore the strategies that IT specialists use to implement the USCG standard practices needed to secure the USCG network for maritime cybersecurity from cyber-related threats. Using strategies such as network compliance policies, network segmentation, the complexity of passwords, and the adoption of cybersecurity standards would assist with lessening the shortage of IT specialists.

This qualitative multiple case research identifies strategies that could promote positive social change to secure the network, reduce unauthorized exposure to maritime industry operations while improving cybersecurity awareness to better cyber-related practices, and protect the targeted population.

Recommendations for Action

The findings of this study could benefit IT specialists and senior leaders by providing them with strategies they could use to implement standard practices to secure the USCG network from maritime cyber-related threats. The first recommendation is for senior leaders to provide a strategic plan that aligns the cyber-related standards practices within their Area of Responsibilities (AOR). The study findings show that IT specialists perform some strategies, but this study provides insight for senior leaders to be more proactive with cyber-related threats.

The second recommendation is to incorporate network segmentation. Network compliance is an essential facet of the cybersecurity standards and best practices for the organization. Ensuring the USCG network is secure by segregating the network in different segments to control the traffic and monitor the external and internal connections. By not segmenting the network, the IT specialists would not prevent unauthorized network traffic from reaching portions of the USCG network that could cause cyber-related threats. Senior leaders should ensure best practices and security awareness training are available and build a culture for the USCG to secure the network against cyber-related threats is a priority for adopting cybersecurity and best practices.

The study results lead to senior leadership establishing and promoting the cybersecurity standards and best practices adopted.

The third recommendation focuses on reviewing the strategies that have been applied to prevent cyber-related threats and adopting those strategies as best practices. Security controls should be set in place to ensure the technical controls and tools effectively prevent cyber-related threats. The senior leadership should do an annual review of the tools and strategies to ensure they are valid and collaborate to adopt cybersecurity standards and best practices. Additionally, the senior leaders would execute a strategic plan for cyber-related threats by identifying the current strategies. The strategic plan includes policies and standard practices to protect the USCG network. The strategic plan should include the following as a minimum:

1. Multifactor authentication mechanism and password policies for IT specialists and users;
2. The network should have IDS installed for network monitoring, firewall rules, along with an established schedule for vulnerability patch remediation;
3. The established security awareness training for the IT specialists and users will assist the organizational guidelines.

This study benefits IT specialists, senior leadership, and users within the USCG organization and the strategies uncovered to be used to implement best practices. I may circulate the study findings through presentations at professional conferences and workshops. This study identified strategies that could be used to secure the USCG network for maritime industries.

Recommendations for Further Study

The findings of this study revealed some strategies IT specialists use to implement standard practice to protect the USCG network. The focus was on the organizations in Virginia and West Virginia within USCG that have strategies for cyber-related threats on the USCG network. Recommendations for further study include similar research in other parts of the USCG, considering using a different design methodology and conceptual framework for research diversity. The study was limited to strategies that IT specialists in Virginia and West Virginia use to prevent cyber-related threats from the USCG network for maritime industries. However, there is a possibility that including more IT specialists from different parts of the USCG and geographic areas may reveal other strategies that were not uncovered in this study and could contribute further to the current literature.

Another recommendation is for future researchers to use quantitative research methodology to provide another perspective for implementing standard practices to protect the USCG network from cyber-related threats. This qualitative multiple case study could assist the impact of standard practices and the number of cyber-related threats that impact the USCG network. This study has contributed to the literature; however, additional research is merited as reported in this study's findings.

Reflections

My experience while exploring the strategies used during the doctoral study revealed a couple of reflections. First, I recognized the complexity of protecting and securing the USCG network when the technology continues to change. As an IT specialist, early in my career, I have been involved with the remediation of cyber-related

threats. However, being involved with this research provided me with an appreciation for IT specialists in the current state and what they must endure. My journey in this study took a holistic turn because I focused on the strategies and best practices when I first started this doctoral study. Nevertheless, the doctoral study assisted in identifying the cybersecurity strategies and best practices that must be seen through a holistic view.

Second, the themes and subthemes that evolved during the data collection and analysis highlighted that IT specialists have evolved since I was an IT specialist. Interacting with the IT specialists responsible for cybersecurity gave the researcher a new appreciation for its work to secure a network. This study was challenging, but it aligned with my personal and professional aspirations as a deputy chief. I learned through this qualitative research to have patience because there were many roadblocks, such as IRB approval. However, I have better understood the strategies used to implement standard practices to secure the USCG network.

Summary and Study Conclusions

This qualitative multiple case study aimed to explore the strategies IT specialists used to protect the USCG network. The multiple case organizations in the study represented the USCG network for the maritime industries in Virginia and West Virginia. Data triangulation was performed using the interview and member checking data and the publicly organizational documents to help answer the study's research question. The data analysis phase of the study revealed three principal themes related to the strategies the IT specialists use to implement standard practices to secure the USCG network for maritime cybersecurity from cyber-related threats, which were (a) adhering to network compliance,

(b) promoting adopting cybersecurity standards and best practices, (c) enhancing cybersecurity awareness and policies. IT specialists could use these findings to formulate strategies that could help to implement standard practices to secure the USCG network.

References

Abbass, W., Bakraouy, Z., Baina, A., & Bellafkih, M. (2019). Intelligent risk management framework. *IAES International Journal of Artificial Intelligence*, *8*(3), 278. https://doi.org/10.11591/ijai.v8.i3.pp278-285

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulations as a methodological alternative. *Administração: Ensino e Pesquisa*, *19*(1), 66–98. https://doi.org/10.13058/raep.2018.v19n1.57

Abdullahi, S. (2018). Examining the network & security infrastructure of skype mobile application. *International Journal of Computer Networks and Communications Security, 6*(12), 264–269. https://www.ijcncs.org/published/volume6/issue12/2Vol6No12.pdf

Aggarwal, N., Gupta, R., & Saxena, P. (2019). Comparative study of OSI & TCP/IP reference model. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*. https://www.ijraset.com/fileserve.php?FID=1124

Ahearne, S., O'Mahony, N., Boujnah, N., Ghafoor, S., Davy, A., Guerrero, L. G., & Renaud, C. (2019). Integrating THz wireless communication links in a data centre network. https://doi.org/10.1109/5gwf.2019.8911705

Ahokas, J., Kiiski, T., Malmsten, J., & Ojala, L. (2017). Cybersecurity in ports: A conceptual approach. In *Proceedings of the Hamburg International Conference of Logistics* (pp. 343–359). https://doi.org/10.15480/882.1448

Aiken, M., McMahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2016). A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, *11*(4), 373–39. https://doi.org/10.1080/21582041.2015.1117648

Akinrolabu, O., Nurse, J., Martin, A., & New, S. (2019). Cyber risk assessment in cloud provider environments: Current models and future needs. *Computers & Security, 87,* 101600. https://doi.org/10.1016/j.cose.2019.101600

Alabady, S. A., Al-Turjman, F., & Din, S. (2020). A novel security model for cooperative virtual networks in the IoT era. *International Journal of Parallel Programming*, *48*(2), 280–295. https://doi.org/10.1007/s10766-018-0580-z

Albahar, M. (2017). Cyber-attacks and terrorism: A twenty-first-century conundrum. *Science and Engineering Ethics*, 1–14. https://doi.org/10.1007/s11948-016-9864-0

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future internet*, *11*(3). https://doi.org/10.3390/fi11030073

Alexander, R. (2017). Using the analytical hierarchy process model in the prioritization of information assurance defense in-depth measures—A quantitative study. *Journal of Information Security*, *8*(03), 166. https://doi.org/10.4236/jis.2017.83011

Alhmeidiyeen, M. S. (2019). Change management and organizational development: A critical conceptual study. *Global Journal of Management and Business Research*.

https://www.journalofbusiness.org/index.php/GJMBR/article/view/2847

Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors*, *18*(3), 817. https://doi.org/10.3390/s18030817

Allodi, L., & Massacci, F. (2017). Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis*, *37*(8), 1606–1627. https://doi.org/10.1111/risa.12864

Almalki, S. (2016). Integrating quantitative and qualitative data in mixed methods research – Challenges and benefits. *Journal of Education and Learning, 5*(3), 288–296. https://doi.org/10.4135/9781483348919.n9

Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M., & Musa, A. (2018, August). Understanding awareness of cybersecurity threat among it employees. In *2018 6th International Conference on Future Internet of Things and Cloud Workshops* (pp. 188–192). IEEE. https://doi.org/10.1109/w-ficloud.2018.0003

Alves, T., & Morris, T. (2018). Hardware-based cyber threats. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 259–266. https://doi.org/10.5220/0006577202590266

Al-Yaseen, W. L., Othman, Z. A., & Ahmad Nazri, M. Z. (2016). Real-time intrusion detection system using multi-agent system. *IAENG International Journal of Computer Science, 43*(1), 80–90. http://www.iaeng.org/IJCS/issues_v43/issue_1/IJCS_43_1_10.pdf

Amiri, I., Wang, L., Levy, Y., & Hur, I. (2018). An Empirical Study on the Factors Contributing to Disclosing Personal Information Online: Insecurity in the Digital

Age. https://aisel.aisnet.org/amcis2018/Security/Presentations/2/

Amrollahi, M., Hadayeghparast, S., Karimipour, H., Derakhshan, F., & Srivastava, G. (2020). Enhancing network security via machine learning: opportunities and challenges. *Handbook of big data privacy*, 165-189. https://doi.org/10.1007/978-3-030-38557-6_8

Anderson, N. (2020). Actions Needed to Evaluate the Effectiveness of Organizational Changes and Determine Workforce Needs. https://www.gao.gov/assets/710/704873.pdf

Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32-74. https://doi.org/10.1080/23742917.2016.1252211

Anttila, J., & Jussila, K. (2017, December). Challenges for the comprehensive and integrated information security management. In *2017 13th International Conference on Computational Intelligence and Security (CIS)* (pp. 586-589). IEEE. https://doi.org/10.1109/cis.2017.00136

Apuke, O. D. (2017). Quantitative research methods: A synopsis approach. *Kuwait Chapter of Arabian Journal of Business and Management Review*, *33*(5471), 1-8. https://doi.org/10.12816/0040336

Aravamudhan, N. R., & Krishnaveni, R. (2016). Establishing content validity for new performance management capacity building scale. *IUP Journal of Management Research*, 15, 20-43. https://www.iupindia.in/Management_Research.asp

Arief, B., Adzmi, M. A. B., & Gross, T. (2015). Understanding cybercrime from its

stakeholders' perspectives: Part 1--attackers. *IEEE Security & Privacy*, *13*(1), 71-76. https://doi.org/10.1109/msp.2015.19

Arifin, S. R. M. (2018). Ethical considerations in qualitative study. *International Journal of Care Scholars*, *1*(2), 30-33.https://doi.org/10.1109/msp.2015.19

Arnold, R. D., & Wade, J. P. (2017). A complete set of systems thinking skills. *Insight*, *20*(3), 9-17. https://doi.org/10.1002/inst.12159

Arsel, Z. (2017). Asking questions with reflexive focus: A tutorial on designing and conducting interviews. *Journal of Consumer Research*, *44*(4), 939-948. https://doi.org/10.1093/jcr/ucx096

Asgarkhani, M., Correia, E., & Sarkar, A. (2017, February). An overview of information security governance. In *2017 International Conference on Algorithms, Methodology, Models, and Applications in Emerging Technologies (ICAMMAET)* (pp. 1-4). IEEE. https://doi.org/10.1109/icammaet.2017.8186666

Asghari, H., van Eeten, M. J., & Bauer, J. M. (2015). Economics of fighting botnets: Lessons from a decade of mitigation. *IEEE Security & Privacy*, 13(5), 16-23. https://doi.org/10.1109/msp.2015.110

Azungah, T. (2018). Qualitative research: Deductive and inductive approaches to data analysis. *Qualitative Research Journal, 18*(4), 383-400. https://doi.org/10.1108/qrj-d-18-00035

Baral, U. N. (2017). 'Research Data' in Social Science Methods. *Journal of Political Science*, *17*, 82-104. https://doi.org/10.3126/jps.v17i0.20515

Barca, D. C. (2017). Information security in digital trunking systems. *Database Systems*

Journal, *8*(1), 40–48. http://www.dbjournal.ro/

Bardarova, S., & Simic, I. (2019). Managers' role in achieving balance between people and organization. *Contemporary economic trends: Technological development and challenges of competitiveness*. https://eprints.ugd.edu.mk/22743/

Barglowski, K. (2018). Where, what and whom to study? Principles, guidelines and empirical examples of case selection and sampling in migration research. In *Qualitative research in European migration studies* (pp. 151-168). Springer, Cham. https://doi.org/10.1007/978-3-319-76861-8_9

Baškarada, S. (2014). Qualitative Case Study Guidelines. *Qualitative Report*, *19*(40), 1–25. https://nsuworks.nova.edu/tqr/vol19/iss40/3/

Benaroch, M. (2018). Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. *Information Systems Research*, *29*(2), 315-340. https://doi.org/10.1287/isre.2017.0714

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, *2*, 8-14. https://doi.org/10.1016/j.npls.2016.01.001

Billen, A., Madrigal, J. A., Scior, K., Shaw, B. E., & Strydom, A. (2017). Donation of peripheral blood stem cells to unrelated strangers: A thematic analysis. *PloS one*, *12*(10). https://doi.org/10.1371/journal.pone.0186438

Bird, R. C., & Davis-Nozemack, K. (2018). Tax Avoidance as a Sustainability Problem. *Journal of Business Ethics*, 151, 1009-1025. https://doi.org/10.1007s10551-016-3162-2

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member Checking: A

Tool to Enhance Trustworthiness or Merely a Nod to Validation? *Qualitative Health Research,* 26(13), 1802–1811. https://doi.org/10.1177/1049732316654870

Biswas, B., & Mukhopadhyay, A. (2018). G-RAM framework for software risk assessment and mitigation strategies in organizations. *Journal of Enterprise Information Management, 31*(2), 276-299. https://doi.org/10.1108/jeim-05-2017-0069

Blaikie, N. (2018). Confounding issues related to determining sample size in qualitative research. *International Journal of Social Research Methodology*, 21(5), 1-7. https://doi.org/10.1080/13645579.2018.1454644

Blokland, P., & Reniers, G. (2020). Safety Science, a Systems Thinking Perspective: From Events to Mental Models and Sustainable Safety. *Sustainability*, *12*(12), 5164. https://doi.org/10.3390/su12125164

Bloomberg, L. D., & Volpe, M. (2018). *Completing your qualitative dissertation: A road map from beginning to end*. Sage Publications. https://doi.10.4135/9781452226613

Blum, D. (2020). Manage Risk in the Language of Business. In *Rational Cybersecurity for Business* (pp. 123-156). Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5952-8_5

Bodnar, J., & Hanlon, B. (2020). "Three Takeaways for Defending Against Foreign Interference from the SolarWinds Hacks," Alliance for Securing Democracy, December 22, 2020; For more, see Appendix A, Section II: Private Sector, Cybersecurity, and Technology Companies; Appendix A, Section I: Public Sector,

Executive Branch. https://securingdemocracy.gmfus.org/three-takeaways-for-defending-against-foreign-interference-from-the-solarwinds-hacks/

Bongiovanni, I., Leo, E., Ritrovato, M., Santoro, A., & Derrico, P. (2017). Implementation of best practices for emergency response and recovery at a large hospital: A fire emergency case study. *Safety Science*, *96*, 121-131. https://doi.org/10.1016/j.ssci.2017.03.016

Bongiovanni-Delarozière, I., & Le Goff-Pronost, M. (2017). Economic evaluation methods applied to telemedicine: From a literature review to a standardized framework. *European Research in Telemedicine/La Recherche Européenne en Télémédecine*, *6*(3-4), 117-135. https://doi.org/10.1016/j.eurtel.2017.08.002

Bourke, B. (2014). Positionality: Reflecting on the research process. *Qualitative Report*, *19*(33). https://nsuworks.nova.edu/tqr/vol19/iss33/3

Brink, H. I. L. (1993). Validity and Reliability in Qualitative Research. *Curationis*, 16(2), 35–38. https://doi.org/10.4102/curationis.v16i2.1396

Bronk, R., & Dewitte, P. (2020, January). Maritime Cybersecurity: Meeting Threats to Globalization's Great Conveyor. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2020.240

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

Buchanan, R. (2019). Systems Thinking and Design Thinking: The Search for Principles in the World We Are Making. *She Ji: The Journal of Design, Economics, and*

Innovation, *5*(2), 85-104. https://doi.org/10.1016/j.sheji.2019.04.001

Budke, C. A., & Ferguson, J. A. (2017). Data Integration and e-Commerce Threats Challenging Providers. *Missouri medicine*, *114*(6), 419. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6139979/

Buetow, S. (2019). Apophenia, unconscious bias and reflexivity in nursing qualitative research. *International Journal of Nursing Studies*, 89, 8–13. https://doi.org/10.1016/j.ijnurstu.2018.09.013

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. https://doi.org/10.1016/j.chb.2016.11.018

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., & Pattinson, M. (2020). When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. *Computers & Security, 98*, 1-11. http://dx.doi.org/10.1016/j.cose.2020.102020

Candela, A. G. (2019). Exploring the function of member checking. *The Qualitative Report*, 24(3), 619-628. https://nsuworks.nova.edu/tqr/vol24/iss3/14

Caretta, M. A. (2016). Member checking: A feminist participatory analysis of the use of preliminary results pamphlets in cross-cultural, cross-language research. *Qualitative Research*, *16*(3), 305-318. https://doi.org/10.1177/1468794115606495

Carminati, L. (2018). Generalizability in qualitative research: a tale of two traditions. *Qualitative health research*, *28*(13), 2094-2101.

https://doi.org/10.1177/1049732318788379

Cassidy, W. (2017). China-based cyberattack hits logistics operators, shippers. *Outsource*, *5*(6), 1-8. https://doi.org/10.3390/ijerph14080888

Chandler, J., Rycroft-Malone, J., Hawkes, C., & Noyes, J. (2016). Application of simplified Complexity Theory concepts for healthcare social systems to explain the implementation of evidence into practice. *Journal of advanced nursing*, *72*(2), 461-480. https://doi.org/10.1111/jan.12815

Chatterjee, S., & Thekdi, S. (2020). An iterative learning and inference approach to managing dynamic cyber vulnerabilities of complex systems. *Reliability Engineering & System Safety*, *193*, 106664. https://doi.org/10.1016/j.ress.2019.106664

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

Chierici, L., Fiorini, G., Rovere, S., & Vestrucci, P. (2016). The evolution of defense in depth approach: A cross-sectorial analysis. *Open Journal of Safety Science and Technology, 06*(02), 35-54. https://doi.org/10.4236/ojsst.2016.62004

Chikere, C. C., & Nwoka, J. (2015). The systems theory of management in modern day organizations-A study of Aldgate congress resort limited Port Harcourt. *International Journal of Scientific and Research Publications*, *5*(9), 1-7. https://pdfs.semanticscholar.org/d1e4/03a4a017d00b081122c2a0abd1d7317f14fe.pdf

Chile, P. (2018). Some of the disadvantages of using the diffusion theory. https://bizfluent.com/info-8633492-disadvantages-using-diffusion-theory.html

Chitchyan, R., Groher, I., & Noppen, J. (2017). Uncovering sustainability concerns in software product lines. *Journal of Software: Evolution and Process*, *29*(2), e1853. https://doi.org/10.1002/smr.1853

Chiumento, A., Khan, M. N., Rahman, A., & Frith, L. (2016). Managing Ethical Challenges to Mental Health Research in Post-Conflict Settings. *Developing world bioethics*, *16*(1), 15-28. https://doi.org/10.1111/dewb.12076

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability*, 8(7), 638. https://doi.org/10.3390/su8070638

Chu, A. M. Y., & So, M. K. P. (2020). Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective. *Sustainability, 12*(8), 3163. https://doi.org/10.3390/su12083163

Ciocănel, A., Lazăr, F., Munch, S., Harmon, C., Rentea, G.-C., Gaba, D., & Mihai, A. (2018). Helping, mediating, and gaining recognition: The everyday identity work of Romanian health social workers. *Social Work in Health Care*, 57(3), 206–219. https://doi.org/10.1080/00981389.2018.1426674

Clark, K. R., & Vealé, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology*, *89*(5), 482CT-485CT. https://www.ncbi.nlm.nih.gov/pubmed/29793921

Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press. http://www.radiologictechnology.org/content/89/5/482CT.extract

Clarke, V., & Braun, V. (2018). Using thematic analysis in counseling and psychotherapy research: A critical reflection. *Counseling and Psychotherapy Research*, *18*(2), 107-110. https://doi.org/10.1002/capr.12165

Congress, U. S. (2006). Security and accountability for every port act. *Public Law*, 109-347. https://www.congress.gov/109/plaws/publ347/PLAW-109publ347.pdf

Constantinou, C. S., Georgiou, M., & Perdikogianni, M. (2017). A comparative method for themes saturation (CoMeTS) in qualitative interviews. *Qualitative Research*, *17*(5), 571–588. https://doi.org/10.1177/1468794116686650

Conteh, N. Y., & Schmick, P. J. (2016). 'Cybersecurity: risks, vulnerabilities, and countermeasures to prevent social engineering attacks', *International Journal of Advanced Computer Research,* 6(23), pp. 31–38. https://doi:10.19101/ijacr.2016.623006

Cooper, H. (2020). Meta-Analysis and Research Synthesis. In P. Atkinson, S. Delamont, A. Cernat, J.W. Sakshaug, & R.A. Williams (Eds.), *SAGE Research Methods Foundations.* https://doi.org/10.4135/9781526421036849598

Cooper, M. J., & Schaffer, K. B. (2019). *Security Requirements for Cryptographic Modules* (No. Federal Inf. Process. Stds. (NIST FIPS)-140-3). https://doi.org/10.6028/nist.fips.140-3

Corner, P. D. (2002). An integrative model for teaching quantitative research design.

Journal of Management Education, 26, 671-692. https://doi.org/10.1177/1052562902238324

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems,* 26(6), 605-641. https:10.1057/s41303-017-0059-9

Creswell, J. W., & Poth, C. N. (2016). Qualitative inquiry and research design: Choosing among five approaches. Sage publications. https://doi.org/10.13187/rjs.2017.1.30

Crick, J. M. (2020). Qualitative research in marketing: what can academics do better? *Journal of Strategic Marketing*, 1-40. https://doi.org/10.1080/0965254x.2020.1743738

Cruz, R. F., & Tantia, J. F. (2017). Reading and understanding qualitative research. *American Journal of Dance Therapy*, 39(1), 79-92. https://doi.org/10.1007/s10465-016-9219-z

Cumyn, A., Ouellet, K., Côté, A.-M., Francoeur, C., & St-Onge, C. (2018). Role of researchers in the ethical conduct of research: A discourse analysis from different stakeholder perspectives. *Ethics & Behavior*. https://doi.org/10.1080/10508422.2018/1539671

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

Damanpour, F. (2020). *Organizational Innovation: Theory, Research, and Direction*.

Edward Elgar Publishing. https://doi.org/10.4337/9781788117449

Daum, O. (2019). Cyber Security in The Maritime Sector. *Journal of Maritime Law & Commerce*, 50(1), 1–19. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlc50&div=7&id=&page=

Davis, J. B. (2017). Sraffa on the Open vs.' Closed Systems' Distinction and Causality. *Closed Systems' Distinction and Causality (July 18, 2017). Forthcoming in Research in the History of Economic Thought and Methodology*. https://doi.org/10.1108/s0743-41542017000035b007

Davis, P. (2021). SolarWinds Hack Was the Largest and Most Sophisticated Attack Ever. *Journal of Counterterrorism & Homeland Security International*, *26*(3), 12–15.

Davis, S. M., Davidov, D., Kristjansson, A. L., Zullig, K., Baus, A., & Fisher, M. (2018). Qualitative case study of needle exchange programs in the Central Appalachian region of the United States. *PLoS One*, *13*(10). https://doi.org/10.1371/journal.pone.0205466

Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review*, 35(2), 60–67. https://doi.org/10.1177/0266382118773624

Dearing, J. W., & Cox, J. G. (2018). Diffusion of innovations theory, principles, and practice. *Health Affairs, 37*(2), 183-190. https://doi.org/10.1377/hlthaff.2017.1104

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-

7. https://doi.org/10.1016/j.giq.2017.02.007

Dedeke, A. (2017). Cybersecurity framework adoption: Using capability levels for implementation tiers and profiles. *IEEE Security & Privacy*, (5), 47-54. https://doi.org/10.1109/MSP.2017.368106

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: a balance of relationship and rigor. *Family Medicine and Community Health*, 7(2), e000057. https://doi.org/10.1136/fmch-2018-000057

Denzin, N. K., & Lincoln, Y. S. (2008). *The landscape of qualitative research* (Vol. 1). Sage. https://www.bookdepository.com/book/9781412957588

De Oliveira Albuquerque, R., Garcia Villalba, L. J., Sandoval Orozco, A. L., De Sousa Junior, R. T., & Kim, T. (2016). Leveraging information security and computational trust for cybersecurity. *The Journal of Supercomputing*, 72, 3729–3763. https://doi.org/10.1007/s11227-015-1543-4

Department of Defense Directive 8140.01. (2020). Cyberspace workforce management. https://fas.org/irp/doddir/dod/d8140_01.pdf

Dettori, J. R., & Norvell, D. C. (2018). The anatomy of data. *Global spine journal*, *8*(3), 311-313. https://doi.org/10.1177/2192568217746998

Dhillon, G., & Ward, J. (2002). Chaos theory as a framework for studying information systems. *Information Resources Management Journal*, 15(2), 5-13. https://doi.org/10.4018/irmj.2002040101

Donaldson, S., Siegel, S., Williams, C. K., & Aslam, A. (2015). *Enterprise cybersecurity: how to build a successful cyberdefense program against advanced threats*.

Apress. https://doi.org/10.1007/978-1-4302-6083-7_14

Dubosson, M., Fragniere, E., Junod, N., Meier, S., Varone, S., & Fournier, A. (2019). Integration of a human risk module into a risk management software. *Informatica Economica, 23*(3), 5-15. https://doi.org/10.12948/issn14531305/23.3.2019.01

Du Plessis, A. E. (2018). The Lived Experience of Out-of-field STEM Teachers: a Quandary for Strategising Quality Teaching in STEM?. *Research in Science Education*, 1-35. https://doi.org/10.1007/s11165-018-9740-9

Edgar, T. W., & Manz, D. O. (2017). *Research methods for cybersecurity*. Syngress. https://doi.org/10.1016/b978-0-12-805349-2.00033-9

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, *5*(1), 1-4. https://doi.org/10.11648/j.ajtas.20160501.11

Fagerholm, F., Kuhrmann, M., & Münch, J. (2017). Guidelines for using empirical studies in software engineering education. *PeerJ Computer Science*, *3*, e131. https://doi.org/10.7717/peerj-cs.131

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity Indices and Cybercrime Annual Loss and Economic Impacts. *Journal of Business and Behavioral Sciences*, 32(1), 63-71. http://asbbs.org/files/2020/JBBS_32.1_Spring_2020.pdf#page=63

Fetterman, D. M. (2019). *Ethnography: Step-by-step* (Vol. 17). SAGE Publications, Incorporated. https://us.sagepub.com/en-us/nam/ethnography/book239000

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., McCarthy,

S., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC health services research*, *18*(1), 120. https://doi.org/10.1186/s12913-018-2915-2

Friese, S. (2019). *Qualitative data analysis with ATLAS.ti.* SAGE Publications Limited. https://us.sagepub.com/en-us/nam/qualitative-data-analysis-with-atlasti/book261755?page=1

Fritz, R. L., & Vandermause, R. (2018). Data collection via in-depth email interviewing: Lessons from the field. *Qualitative Health Research*, *28*(10), 1640-1649. https://doi.org/10.1177/1049732316689067

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change*, *10*(1), 2. https://doi.org/10.5590/josc.2018.10.1.02

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national-level strategic approach. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo I komunikacije*, *58*(3), 273-286. https://doi.org/10.1080/00051144.2017.1407022

Garcia, M., Forscey, D., & Blute, T. (2017). Beyond the network: A holistic perspective on state cybersecurity governance. *Neb. L. Rev.*, *96*, 252. https://digitalcommons.unl.edu/nlr/vol96/iss2/3

Garg, R. (2016). Methodology for research I. *Indian journal of anesthesia*, 60(9), 640. https://doi.org/10.4103/0019-5049.190619

Gill, P., & Baillie, J. (2018). Interviews and focus groups in qualitative research: An

update for the digital age. *British Dental Journal, 225*(7), 668-672. https://doi.org/10.1038/sj.bdj.2018.815

Goldstone, D., & Bantjes, J. (2017). Mental health care providers' perceptions of the barriers to suicide prevention amongst people with substance use disorders in South Africa: a qualitative study. *International journal of mental health systems*, *11*(1), 1-11. https://doi.org/10.1186/s13033-017-0153-3

Gopaldas, A. (2016). A front-to-back guide to writing a qualitative research article. Qualitative Market Research: *An International Journal*, 19(1), 115-121. https://doi.org/10.1108/qmr-08-2015-0074

Gorzeń-Mitka, I., & Okręglicka, M. (2014). Improving decision making in complexity environment. *Procedia Economics and Finance*, *16*, 402-409. https://doi.org/10.1016/s2212-5671(14)00819-3

Goss, D. (2017). Operationalizing Cybersecurity — Framing Efforts to Secure U.S. Information Systems. *The Cyber Defense Review*, 2(2), 91-110. https://www.jstor.org/stable/26267345

Goulielmos, A. M. (2019). Management by Chaos Theory with a Case-Study from Shipping Industry. *Modern Economy*, 10, 2004-2029. https://doi.org/10.4236/me.2019.108127

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, N. B., Lefkovitz, J. M., Danker, Y. Y., Choong, K. K., Greene, K., & Theofanos, M. F. (2020). Digital identity guidelines: Authentication and lifecycle management. https://doi.org/10.6028/NIST.SP.800-63b

Greener, S. (2018). Research limitations: the need for honesty and common sense. *Interactive Learning Environments*, *26*(5), 567-568. https://doi.org/10.1080/10494820.2018.1486785

Greiman, V. (2019). Navigating the Cyber Sea: Dangerous Atolls Ahead. *Proceedings of the International Conference on Cyber Warfare & Security*, 87–93. https://www.jinfowar.com/journal/volume-19-issue-3/defending-cyber-sea-legal-challenges-ahead

Guo, Y., Zhang, Z., & Guo, Y. (2019). Optiwords: A new password policy for creating memorable and strong passwords. *Computers & Security*, *85*, 423-435. https://doi.org/10.1016/j.cose.2019.05.015

Gupta, K. P., Bhaskar, P., & Singh, S. (2017). Prioritization of factors influencing employee adoption of e-government using the analytic hierarchy process. *Journal of Systems and Information Technology*, *19*(1/2), 116-137. https://doi.org/10.1108/JSIT-04-2017-0028

Halibozek, E., & Kovacich, G. L. (2017). *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Butterworth-Heinemann.

Halima, I. K., Islam, S., & Mohammad, A. R. (2018). An integrated cybersecurity risk management approach for a cyber-physical system. Applied Sciences, 8(6). https://doi.org/10.3390/app8060898

Hall, J., & Martin, B. R. (2019). Towards a taxonomy of research misconduct: The case of business school research. *Research Policy, 48*, 414-427.

https://doi.org/10.1016/j.respol.2018.03.006

Hallinan, Z. P., Forrest, A., Uhlenbrauck, G., Young, S., & McKinney Jr, R. (2016). Barriers to change in the informed consent process: A systematic literature. *IRB*, *38*(3). 1-10. https://www.jstor.org/journal/irbethihumarese

Hamilton, A. B., & Finley, E. P. (2019). Qualitative methods in implementation research: An introduction. *Psychiatry Research*, 280, N.PAG. https://doi.org/10.1016/j.psychres.2019.112629

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: when to use them and how to judge them. *Human reproduction*, *31*(3), 498-501. https://doi.org/10.1093/humrep/dev334

Hancock, D. R., & Algozzine, B. (2017). *Doing case study research: A practical guide for beginning researchers*. Teachers College Press. http://www.tcrecord.org

Hanson, J., Balmer, D., & Giardino, A. (2011). Qualitative research methods for medical educators. *Academic Pediatrics*, 11, 375-386. https://doi.org/10.1016/j.acap.2011.05.001

Harrison, A., Burress, R., Velasquez, S., & Schreiner, L. (2017). Social media use in academic libraries: A phenomenological study. *The journal of academic librarianship*, *43*(3), 248-256. https://doi.org/10.1016/j.acalib.2017.02.014

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

Harvey, M. (2016). The rise of the LP: the politics of diffusion innovation in the

recording industry. *Business History*, *58*(7), 1095-1117. https://doi.org/10.1080/00076791.2016.1156673

Hayes, B., Bonner, A., & Douglas, C. (2013). An introduction to mixed methods research for nephrology nurses. *Renal Society of Australasia Journal*, *9*(1), 8-14. http://www.renalsociety.org/RSAJ/index_nl.html

Hayles, N. K. (2018). *Chaos bound: Orderly disorder in contemporary literature and science*. Cornell University Press. http://nkhayles.com/assets/Chaos_Bound.pdf

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. Journal of Organizational Computing and Electronic Commerce, 1-9. https://doi:10.1080/10919392.2019.1611528

Heale, R., & Twycross, A. (2018). What is a case study? Evidence-Based Nursing,21, 7–8. https://doi.org/10.1136/eb-2017-102845

Healey, J., & Korn, E. B. (2019). Defense Support to the Private Sector: New Concepts for the DoD's National Cyber Defense Mission. *Cyber Defense Review*, 227.

Heckman, J. (2021). Coast Guard to stand up first cyber 'red team' as it creates Cyber Operational Assessments Branch. Coast Guard to stand up first cyber 'red team' as it creates Cyber Operational Assessments Branch | Federal News Network

Herring, D., Maennel, O. M., & Venables, A. N. (2019). Shortcomings in cybersecurity education for seafarers. In *5th International Conference on Maritime Technology and Engineering, Lisbon, Portugal*. https://doi.org/10.1201/9781003216582-06

Holtrop, J. S., Rabin, B. A., & Glasgow, R. E. (2018). Qualitative approaches to use of the RE-AIM framework: rationale and methods. *BMC health services research*,

18(1), 177. https://doi.org/10.1186/s12913-018-2938-8

Hopcraft, R., & Martin, K. M. (2018). Effective maritime cybersecurity regulation–the case for a cyber code. *Journal of the Indian Ocean Region*, *14*(3), 354-366. https://doi.org/10.1080/19480881.2018.1519056

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

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

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attacks business: A survey. *ACM Computing Surveys*, *51*, 1–36. https://doi.org/10.1145/3199674

Hubbard, T., Weber, G., & Steinhoff, J. (2017). Protecting data assets in a perilous cyber world. *The Journal of Government Financial Management, 66*(3), 26-31. https://www.questia.com/library/journal/1P4-2101246514/protecting-data-assets-in-a-perilous-cyber-world

Iivari, N. (2018). Using member checking in interpretive research practice. *Information*

Technology & People, *31*(1), 111–133. https://doi.org/10.1108/ITP-07-2016-0168

Ikram, S. T., & Cherukuri, A. K. (2016). Improving accuracy of intrusion detection model using PCA and optimized SVM. Journal of Computing & Information Technology, 24(2), 133-148. https://doi.org/10.20532/cit.2016.1002701

ISACA. (2016, January). *2016 cybersecurity skills gap. Cybersecurity nexus*. https://imagestore/slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg

Jacobs, M. (2019, June). Applying a Systems and Complexity Framework to Transformative Learning. In *Proceedings of the 63rd Annual Meeting of the ISSS-2019 Corvallis, OR, USA*. https://doi.org.10.1016/S1353-4858

Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., & Simonin, J. (2018, October). Detecting and hunting cyberthreats in a maritime environment: Specification and experimentation of a maritime cybersecurity operations centre. In *2018 2nd Cyber Security in Networking Conference (CSNet)* (pp. 1-8). IEEE.1. https://doi.org/10.1109/csnet.2018.8602669

James, L. (2018). Making cyber-security a strategic business priority. *Network Security*, *2018*, 6-8. https://doi.org/10.1016/S1353-4858(18)30042-4

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, 82, 85–105. https://doi.org/10.1509/jm.16.0124

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*, 973-993.

https://doi.org/10.1016/j.jcss.2014.02.005

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. https://doi.org/10.1007/978-3-319-52878-6

Johansen, J. H. (2018). *Paradox Management: Contradictions and Tensions in Complex Organizations*. Springer. https://doi.org/10.1108/IJEM-04-2020-0181

Johnson, B. (2018, April). Towards a theory of engineered complex adaptive systems of systems. In *2018 Annual IEEE International Systems Conference (SysCon)* (pp. 1-5). IEEE. https://doi.org/10.1109/syscon.2018.8369514

Johnson, B. (2020). USCG: Ransomware Attack Crippled Network, Access Control at Maritime Facility. https://www.hstoday.us/subject-matter-areas/transportation/uscg-ransomware-attack-crippled-network-access-control-at-maritime-facility/

Johnson, J. L., Adkins, D., & Chauvin, S. (2019). Quality indicators of rigor in qualitative research. *American Journal of Pharmaceutical Education*, 1-22. https://www.ajpe.org/doi/abs/10.5688/ajpe7120

Joseph, R. P., Keller, C., & Ainsworth, B. E. (2016). Recruiting Participants into Pilot Trials: Techniques for Researchers with Shoestring Budgets. *Californian Journal of health promotion*, *14*(2), 81–89. https://doi.org/10.32398/cjhp.v14i2.1878

Jouini, M., & Rabai, L. B. A. (2017). Security problems in cloud computing environments: A deep analysis and a secure framework. In *Apps Management and E-Commerce Transactions in Real-Time* (pp. 70-103). IGI Global.

https://doi.org/10.4018/978-1-5225-5634-3.ch046

Ju-Long, D. (1982). Control problems of grey systems. *Systems & control letters*, *1*(5), 288-294. https://doi.org/10.1016/s0167-6911(82)80025-x

Kabir, S. M. S. (2016). Basic guidelines for research: An introductory approach for all disciplines. *Book Zone Publication, Chittagong*-4203, Bangladesh

Kalhoro, S., Rehman, M., & Shaikh, F. (2021). Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3097144

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/jan.13031

Kalloniatis, C., Kavroudakis, D., Polidoropoulou, A., & Gritzalis, S. (2019). Designing Privacy-Aware Intelligent Transport Systems: A roadmap for identifying the major privacy concepts. *International Journal of Applied Geospatial Research (IJAGR)*, *10*(1), 73-91. https://doi.org/10.4018/ijagr.2019010104

Kalloniatis, C., Pattakou, A., Kavakli, E., & Gritzalis, S. (2017). Designing Secure and Privacy-Aware Information Systems. *International Journal of Secure Software Engineering (IJSSE)*, *8*(2), 1-25. https://doi.org/10.4018/ijsse.2017040101

Kalpokaite, N., & Radivojevic, I. (2020). "I wish I knew what I know now": Exploring psychology undergraduate students' experiences when learning about qualitative research and CAQDAS. *The Qualitative Report, 25*(7), 1817-1840.

https://nsuworks.nova.edu/tqr/vol25/iss7/6

Kam, H. J., Menard, P., Ormond, D., & Crossler, R. E. (2020). Cultivating cybersecurity learning: An integration of self-determination and flow. *Computers & Security*, 101875. https://doi:10.1016/j.cose.2020.101875

Karchefsky, S., & Rao, H. R. (2017). Toward a safer tomorrow: Cybersecurity and critical infrastructure. In *The Palgrave Handbook of Managing Continuous Business Transformation* (pp. 335-352). Palgrave Macmillan, London. https://doi.org/10.1057/978-1-137-60228-2_15

Kast, F., & Rosenzweig, J. (1972). General systems theory: Application for organization and management. *Academy of Management Journal*, 15(4), 447–464. https://doi.org/10.5465/255141

Kaušpadienė, L., Ramanauskaitė, S., & Čenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy*, *25*(5), 979-997. https://doi.org/10.3846/tede.2019.10298

Kay, L. (2019). Guardians of research: negotiating the strata of gatekeepers in research with vulnerable participants. *PRACTICE*, 1-16. https://doi.org/10.1080/25783858.2019.1589988

Kerner, B. S. (2017). Breakdown in Traffic Networks. Springer Berlin-New York. https://doi:10.1007/978-3-662-54473-0

Kessler, G. C., Craiger, J. P., & Haass, J. C. (2018). A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification

System. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 12(3), 429, https://doi.org/10.12716/1001.12.03.01

Kiliańska-Przybyło, G. (2018). Litosseliti, L.(ed.).(2018). Research Methods in Linguistics. London: Bloomsbury Academic-review by Grażyna Kiliańska-Przybyło. *Theory and Practice of Second Language Acquisition*, *5*(2), 123-127. https://doi.org/10.31261/tapsla.7638

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

Kim, S. S., & Kim, Y. J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management*, *21*(4), 986–1010. https://doi.org/10.1108/jkm-08-2016-0353

Kivak, R. (2017). Complexity theory and organizations. Hackensack, NJ: Salem Press Encyclopedia.

Klaic, A. (2016). A METHOD FOR THE DEVELOPMENT OF CYBER SECURITY STRATEGIES. *Information & Security*, 34(1), 37-55. https://doi.org/10.11610/isij.3403

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. *Journal of Information Systems Education*, *28*(2), 101. https://aisel.aisnet.org/jise/vol28/iss2/4

Komodromos, M., Halkias, D., & Harkiolakis, N. (2019). Managers' perceptions of trust in the workplace in times of strategic change. *EuroMed Journal of Business*. https://doi.org/10.1108/emjb-03-2018-0018

Koopmans, M. (2017). Perspectives on Complexity, Its Definition, and Applications in the Field. *Complicity: An International Journal of Complexity and Education*, 14(1), 16-35. https://doi.org/10.29173/cmplct27611

Kosiński, J., Košla, R., & Gontarz, T. (2019). Cybersecurity and the handling of cyber incidents. *Internal Security*, 10(2), 107-128. https://doi.org/10.5604/01.3001.0013.4219

Kozleski, E. B. (2017). The uses of qualitative research: Powerful methods to inform evidence-based practice in education. *Research and Practice for Persons with Severe Disabilities*, *42*(1), 19-32. https://doi.org/10.1177/1540796916683710

Kozlowski, S. W. (2018). Enhancing the effectiveness of workgroups and teams: a reflection. *Perspectives on Psychological Science*, *13*(2), 205-212. https://doi.org/10.1177/1745691617697078

Kuhn, K. (2018). Cyber Risk Management in the Maritime Transportation System. https://www.hstoday.us/channels/us-coast-guard/cyber-risk-management-maritime-transportation-system/

Kwon, T., Shin, I., Kim, K., Song, J., & Lee, J. (2020, September). Integrated Visual Analytics Approach against Multivariate Cybersecurity Attack. In *Proceedings of the International Conference on Advanced Visual Interfaces* (pp. 1-3).

Lagouvardou, S. (2018). Maritime Cyber Security: concepts, problems and models.

Kongens Lyngby, Copenhagen. https://dx.doi.org/10.26240/heal.ntua.16388

Langner, R., & Pederson, P. (2013). Bound to fail: Why cybersecurity risk cannot be "managed" away. Paper, The Brookings Institution, Washington, D.C. https://www.brookings.edu/wp-content/uploads/2016/06/cybersecurity_langner_pederson_0225.pdf

Laracy, J. R., & Marlowe, T. (2018). Systems Theory and Information Security: Foundations for a New Educational Approach. https://10.6025/isej/2018/5/2/35-48

Leake, M. L. (2019). A study of the diffusion of innovations and hurricane-response communication in the U.S. coast guard (Order No. 22618341). https://digitalcommons.odu.edu/communication_etds/8

Lee, A., & Wogan, H. (2018). "All at Sea: The Modern Seascape of Cybersecurity Threats of the Maritime Industry," *Oceans 2018 MTS/IEE Charleston*, Charleston, SC, pp. 1-8. https://doi.org/10.1109/OCEANS.2018.8604554

Leenen, L., & van Vuuren, J. J. (2019, February). Framework for the cultivation of a military cybersecurity culture. In *Proceedings of the International Conference on Cyber Warfare & Security* (pp. 212-216). https://www.researchgate.net/profile/Louise-Leenen/publication/336605506_Framework_for_the_Cultivation_of_a_Military_Cybersecurity_Culture/links/5db08613299bf111d4c016cb/Framework-for-the-Cultivation-of-a-Military-Cybersecurity-Culture.pdf

Li, A., Hu, Q., Liu, J., & Pan, Y. (2016). Resistance and security index of networks:

Structural information perspective of network security. *Scientific Reports* (Nature Publisher Group), 6, 26810. https://doi.org/10.1038/srep26810

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. https://doi:10.1016/j.ijinfomgt.2018.10.017

Liu, C., Alrowaili, Y., Saxena, N., & Konstantinou, C. (2021). Cyber Risks to Critical Smart Grid Assets of Industrial Control Systems. *Energies*, *14*(17), 5501. https://doi.org/10.3390/en14175501

Liu, S., Yang, Y., Xie, N., & Forrest, J. (2016). New progress of grey system theory in the new millennium. *Grey Systems: Theory and Application.* https://doi.org/10.1108/gs-09-2015-0054

Lub, V. (2015). Validity in qualitative evaluation: Linking purposes, paradigms, and perspectives. *International Journal of Qualitative Methods,* 14(5), 1-8. https://doi.org/10.1177/1609406915621406

Luctkar-Flude, M., Tyerman, J., & Groll, D. (2018). Exploring the use of neurofeedback by cancer survivors: Results of interviews with neurofeedback providers and clients. *Asia-Pacific Journal of Oncology Nursing*. https://doi.org/https://doi.org/10.4103/apjon.apjon_34_18

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2019). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors*, *19*(1), 19. https://doi.org/10.3390/s19010019

Madill, A., & Sullivan, P. (2018). Mirrors, portraits, and member checking: Managing difficult moments of knowledge exchange in the social sciences. *Qualitative Psychology, 5*(3), 321–339. https://doi.org/10.1037/qup0000089

Malecic, A. (2017). Footprints of General Systems Theory. *Systems Research & Behavioral Science*, 34(5), 631–636. https://doi.org/10.1002/sres.2484

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies. *Qualitative Health Research*, *26*(13), 1753-1760. https://doi.org/10.1177/1049732315617444

Malyuk, A., & Miloslavskaya, N. (2016, July). Cybersecurity culture as an element of IT professional training. In *2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)* (pp. 205-210). IEEE. https://doi.org/10.1109/dipdmwc.2016.7529390

Mania-Singer, J. (2017). A Systems Theory Approach to the District Central Office's Role in School-Level Improvement. *Administrative Issues Journal: Connecting Education, Practice, and Research*, *7*(1), 70-83. https://doi.org/10.5929/2017.7.1.6

Marinos, N., D'Souza, V. A., & Franks, J. R. (2021). HIGH-RISK SERIES: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges. *GAO Reports*, 1–93.

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

Masli, A., Richardson, V. J., Watson, M. W., & Zmud, R. W. (2016). Senior Executives IT Management Responsibilities: Serious IT-Related Deficiencies and CEO/CFO Turnover, *MIS Quarterly*, 40, 687-708. https://doi.org/10.25300/MISQ/2016/40.3.08

Mason, R. B., & Staude, G. (2009). An exploration of marketing tactics for turbulent environments. *Industrial Management & Data Systems*. https://doi.org/10.1108/02635570910930082

Masys, A. J. (2015). Applications of systems thinking and soft operations research in managing complexity. *Boston. USA*, 321. https://doi.org/10.1007/978-3-319-21106-0

Matthews, J. R. (2017). Understanding indigenous innovation in rural west Africa: Challenges to diffusion of innovations theory and current social innovation practice. *Journal of Human Development and Capabilities*, *18*(2), 223-238. https://doi.org/10.1080/19452829.2016.1270917

Mayer, N., & Aubert, J. (2020). A risk management framework for security and integrity of networks and services. *Journal of Risk Research*, 1-12. https://doi.org/10.1080/13669877.2020.1779786

Mbengue, P., Ondracek, J., Saeed, M., & Bertsch, A. (2018). Management and Chaos Theory, Complexity Theory, and Self-organizing Systems Theory. *Asia Pacific Journal of Research in Business Management*, *9*(3). https://www.academia.edu/download/57324173/APJ1March18-4775.pdf.

McFadyen, J., & Rankin, J. (2016). The role of gatekeepers in research: learning from

reflexivity and reflection. *GSTF Journal of Nursing and Health Care*, *4*(1), 82-88. http://dl6.globalstf.org/index.php/jnhc/article/view/1745

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2019). Twelve tips for conducting qualitative research interviews. Medical teacher, 41(9), 1002-1006. https://doi.org/10.1080/0142159X.2018.1497149

McKusker, K., & Gunaydin, S. (2014). Research using qualitative, quantitative, or mixed methods and choices based on the research. *Perfusion*, *30*(7), 537-542. https://doi.org/10.1177/0267659114559116

Meng, F., Liu, Y., Liu, L., Li, Y., & Wang, F. (2017). Studies on mathematical models of wet adhesion and lifetime prediction of organic coating/steel by grey system theory. *Materials, 10,* 715. https://doi.org/10.3390/ma10070715

Merriam, S. B., & Grenier, R. S. (Eds.). (2019). Qualitative research in practice: Examples for discussion and analysis. John Wiley & Sons.

Mhaskar, N., Alabbad, M., & Khedri, R. (2021). A formal approach to network segmentation. *Computers & Security*, 103, 102162. https://doi.org/10.1016/j.cose.2020.102162

Micó, J. C., Caselles, A., Soler, D., & Romero, P. D. (2016). Formalism for discrete multidimensional dynamic systems. *Kybernetes*, *45*(10), 1555-1575. https://doi.org/10.1108/K-01-2015-0024

Mihalos, M. G., Nalmpantis, S. I., & Ovaliadis, K. (2019). Design and Implementation of Firewall Security Policies using Linux Iptables. *Journal of Engineering Science & Technology Review*, *12*(1), 80–86. https://doi-

org.proxy.cecybrary.com/10.25103/jestr.121.09

Mishra, B. K., Rolland, E., Satpathy, A., & Moore, M. (2019). A framework for enterprise risk identification and management: The resource-based view. *Managerial Auditing Journal*. https://doi.org/10.1108/MAJ-12-2017-1751

Mohammadi, M. M., Poursaberi, R., & Salahshoor, M. R. (2018). Evaluating the adoption of evidence-based practice using Rogers's diffusion of innovation theory: a model testing study. *Health promotion perspectives*, *8*(1), 25. https://doi.org/10.15171/hpp.2018.03

Moon, K., Brewer, T., Januchowski-Hartley, S., Adams, V., & Blackman, D. (2016). A guideline to improve qualitative social science publishing in ecology and conservation journals. *Ecology and Society, 21*(3). www.jstor.org/stable/26269983

Moser, A., & Korstjens, I. (2017). Series: Practical guidance to qualitative research. Part 1: Introduction. *European Journal of General Practice*, *23*(1), 271–273. https://doi.org/10.1080/13814788.2017.1375093

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection, and analysis. *European Journal of General Practice*, *24*(1), 9-18. https://doi.org/10.1080/13814788.2017.1375092

Moskal, S., Yang, S. J., & Kuhl, M. E. (2018). Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach. *The Journal of Defense Modeling and Simulation*, 15(1), 13–29. https://doi.org/10.1177/1548512917725408

Musman, S., & Turner, A. (2018). A game-theoretic approach to cybersecurity risk management. *The Journal of Defense Modeling and Simulation*, 15(2), 127–146. https://doi.org/10.1177/1548512917699724

Nair, L. B. (2018). Conference report: Scientific Integrity in Qualitative Research (SCIQUAL), seminar 2017. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 19, No. 1, p. 8). DEU. https://dx.doi.org/10.17169/fqs-19.1.2964

National Institute of Standards and Technology. (2017). *Minimum security requirements for federal information and information systems*. US Department of Commerce, National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/nistir/8170/archive/2017-05-12

Nelson, I. A., London, R. A., & Strobel, K. R. (2015). Reinventing the role of the university researcher. *Educational Researcher*, 44, 17–26. https://doi.org/10.3102/0013189X15570387

Neubauer, B. E., Witkop, C. T., & Varpio, L. (2019). How phenomenology can help us learn from the experiences of others. *Perspectives on Medical Education*, *8*(2), 90-97. https://doi.org/10.1007/s40037-019-0509-2

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An Introduction to Information Security. *NIST Special Publication*, *800*, 12. https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final

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

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

O'Har, J. P., Senesi, C. W., & Molenaar, K. R. (2017). Development of a Risk Register Spreadsheet Tool for Enterprise- and Program-Level Risk Management. *Transportation Research Record*, 2604(1), 19–27. https://doi.org/10.3141/2604-03

Oltsik, J., Alexander, C., & CISM, C. (2017). The life and times of cybersecurity professionals. *ESG and ISSA: Research Report*. 2017-ESG-ISSA-full-report.pdf

Onwuegbuzie, A. J., & Collins, K. M. T. (2017). The role of sampling in mixed methods-research. Kölner Zeitschrift Für Soziologie Und Sozialpsychologie, 69, 133-156.

Otero, A. R. (2019). Optimization Methodology for Change Management Controls Using Grey Systems Theory. *International Journal of Business and Applied Social Science*, *5*(6). https://doi.org/10.33642/jbass.v5n6p4

Öztürk, Z., & Kızılkaya, S. (2017). Chaos-complexity theory at management. *International Online Journal of Education and Teaching*, *4*, 259-264. https://core.ac.uk/download/pdf/276292883.pdf

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

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in

Mixed Method Implementation Research. *Administration and policy in mental health*, *42*(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Park, S., Kim, Y., & Chang, H. (2016). An empirical study on security expert ecosystem in the future IoT service environment. *Computers & Electrical Engineering*, 2016(52). 199-207. https://doi.org/10.1016/j.compeleceng.2016.04.001

Pathak, A., & Intratat, C. (2016). Use of semi-structured interviews to investigate teacher perceptions of student collaboration. *Malaysian Journal of ELT Research*, *8*(1), 10. https://journals.melta.org.my/index.php/majer/article/view/149

Peters, K., & Halcomb, E. (2015). Interviews in qualitative research. *Nurse Researcher, 22*(4), 6-7. https://doi.org/10.7748/nr.22.4.6.s2

Pillitteri, V. (2019). *The Next Generation Risk Management Framework (RMF 2.0): A Holistic Methodology to Manage Information Security, Privacy and Supply Chain Risk* (No. ITL Bulletin February 2019). National Institute of Standards and Technology. https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2019-02.pdf

Polit, D., & Beck, C. (2020). *Essentials of Nursing Research: Appraising Evidence for Nursing Practice*. Lippincott Williams & Wilkins.

Pouvreau, D. (2014). On the history of Ludwig von Bertalanffy's "general systemology," and on its relationship to cybernetics - part II: Contexts and developments of the system logical hermeneutics instigated by von Bertalanffy. International Journal of General Systems, 43(2), 172-245.

https://doi.org/10.1080/03081079.2014.883743

Quigley, K., Burns, C., & Stallard, K. (2015). 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, *32*(2), 108-117. https://doi.org/10.1016/j.giq.2015.02.001

Rajamäki, J., Tikanmäki, I., & Räsänen, J. (2019). CISE as a tool for sharing sensitive cyber infor-mation in maritime domain. *Information & Security*, 43(1), 215-235. https://doi.org/10.11610/isij.4317

Ramage, M., & Shipp, K. (2020). Ludwig von Bertalanffy. In Systems Thinkers. (pp. 53-62). Springer, London. https://doi.org/10.1007/978-1-4471-7475-2_6

Rand, W., Rust, R. T., & Kim, M. (2018). Complex systems: marketing's new frontier. *AMS Review*, *8*(3-4), 111-127. https://doi.org/10.1007/s13162-018-0122-2

Rashid, Y., Rashid, A., Warraich, M. A., Sabir, S. S., & Waseem, A. (2019). Case Study Method: A Step-by-Step Guide for Business Researchers. *International Journal of Qualitative Methods*, *18*, 1609406919862424. https://doi.org/10.1177/1609406919862424

Renz, S. M., Carrington, J. M., & Badger, T. A. (2018). Two strategies for qualitative content analysis: An intramethod approach to triangulation. *Qualitative Health Research*, 28, 824–831. https://doi.org/10.1177/1049732317753586

Resler, L. M. (2016). Edward N Lorenz's 1963 paper, "Deterministic nonperiodic flow", in Journal of the Atmospheric Sciences, Vol 20, pages 130–141: Its history and relevance to physical geography. *Progress in Physical Geography: Earth and*

Environment, *40*(1), 175–180. https://doi.org/10.1177/0309133315623099

Rick Van der, K., Geert, K., & Heather, Y. (2017). Computer security incident response team effectiveness: A needs assessment. *Frontiers In Psychology, 8*(2017). https://doi.org/10.3389/fpsyg.2017.02179/full

Roache, B., & Kelly, J. (2018). A research method to explore midwives' views of national maternity service reforms. *Women and Birth*, *31*(3), e216-e221. https://doi.org/10.1016/j.wombi.2017.09.014

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative research in psychology*, *11*(1), 25-41. https://doi.org/10.1080/14780887.2013.801543

Rogers, E. M. (2003). *Diffusion of Innovations, Fifth Edition*. New York, NY: The Free Press

Rogers, E. M. (2010). *Diffusion of innovations*. Simon and Schuster.

Rondelez, R. (2018). Governing cybersecurity through networks: An analysis of cybersecurity coordination in Belgium. *International Journal of Cyber Criminology*, 12(1), 300-315. https://doi.org/10.5281/zenodo.1467929

Roulston, K. (2018). Qualitative interviewing and epistemics. *Qualitative Research, 18*(3), 322-341. https://doi.org/10.1177/1468794117721738

Rousseau, D. (2017). Strategies for Discovering Scientific Systems Principles. *Systems Research & Behavioral Science*, *34*(5), 527–536. https://doi-org.proxy.cecybrary.com/10.1002/sres.2488

Ruelle, D. (1991). *Chance and chaos*. Princeton, NJ: Princeton University Press.

https://doi.org/10.1515/9780691213958

San Nicolas-Rocca, T., & Burkhard, R. J. (2019). Information Security in Libraries. *Information Technology and Libraries*, *38*(2), 58-71. https://doi.org/10.6017/ital.v38i2.10973

Sarstedt, M., Bengart, P., Shaltoni, A. M., & Lehmann, S. (2018). The use of sampling methods in advertising research: A gap between theory and practice. *International Journal of Advertising,* 37(4), 650-663. https://doi.org/10.1080/02650487.2017.1348329

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity*, 52(4), 1893-1907. https://doi.org/10.1007/s11135-017-0574-8

Savalkar, V. A. (2018, January). Link prediction for identifying link failure using cross layer approach. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 1120-1129). IEEE. https://doi.org/10.1109/icisc.2018.8398978

Sayin, H. U. (2016). A Short Introduction to System Theory: Indispensable Postulate Systems and Basic Structures of the Systems in Quantum Physics, Biology, and Neuroscience. NeuroQuantology, 14(1), 126–142. https://doi.org/10.14704/nq.2016.14.1.855

Scarlat, E., & Delcea, C. (2016). An Overview on the Hybrid Intelligent Systems from the Grey Systems Theory and Knowledge Perspective. *Journal of Grey System*,

28(2), 13–26. https://go.gale.com/A469850597

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

Schneider, D., & Trapp, M. (2018). B-space: Dynamic management and assurance of open systems of systems. *Journal of Internet Services and Applications, 9*(1), 1-16. https://doi.org/10.1186/s13174-018-0084-5

Schober, M. M., Gerrish, K., & McDonnell, A. (2016). Development of a conceptual policy framework for advanced practice nursing: An ethnographic study. *Journal of Advanced Nursing,* 72(6), 1313–1324. https://doi.org/10.1111/jan.12915

Schoonenboom, J., & Johnson, R. B. (2017). How to construct a mixed methods research design. *KZfSS Kölner Zeitschrift für Soziologie und Sozialpsychologie*, *69*(2), 107-131. https://doi.org/10.1007/s11577-017-0454-1

Scott, P. (2019). General System Theory and the Use of Process Mining to Improve Care Pathways. *Applied Interdisciplinary Theory in Health Informatics: A Knowledge Base for Practitioners*, *263*(11). https://doi.org/10.3233/SHTI190124

Sekharan, S. S., & Kandasamy, K. (2017, March). Profiling SIEM tools and correlation engines for security analytics. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 717-721). IEEE. https://doi.org/ 10.1109/WiSPNET.2017.8299855

Shapiro, L. R., Maras, M. H., Velotti, L., Pickman, S., Wei, H. L., & Till, R. (2018).

Trojan horse risks in the maritime transportation systems sector. *Journal of Transportation Security*, 8, 1–19. https://doi.org/10.1007/s12198-018-0191-3

Shin, J., Son, H., & Heo, G. (2017). Cyber security risk evaluation of a nuclear I&C using BN and ET. *Nuclear Engineering and Technology*, *49*(3), 517-524. https://doi.org/10.1016/j.net.2016.11.004

Shorten, A., & Smith, J. (2017). Mixed methods research: Expanding the evidence base. *Evidence-Based Nursing*, 20(3), 74. https://doi.org/10.1136/eb-2017-102699

Simola, S. (2018). Fostering collective growth and vitality following acts of moral courage: A general system, relational psychodynamic perspective. *Journal of Business Ethics*, *148*(1), 169-182. https://doi.org/10.1007/s10551-016-3014-0

Simpson, A., & Quigley, C. F. (2016). Member checking process with adolescent students: Not just reading a transcript. *Qualitative Report, 21*(2), 377-392. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2386&context=tqr

Singh, R., & Kumar, S. (2018, December). A comparative study of various wireless network monitoring tools. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)* (pp. 379-384). IEEE. https://doi.org/ 10.1109/ICSCCC.2018.8703216

Škrjanc, I., Ozawa, S., Ban, T., & Dovžan, D. (2018). Large-scale cyber-attacks monitoring using Evolving Cauchy Possibilistic Clustering. *Applied Soft Computing*, *62*, 592-601. https://doi.org/10.1016/j.asoc.2017.11.008

Smeets, M. (2018). Integrating offensive cyber capabilities: meaning, dilemmas, and assessment. *Defense Studies*, *18*(4), 395-410.

https://doi.org/10.1080/14702436.2018.1508349

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. https://doi:10.1016/j.ijinfomgt.2015.11.009

Sosin, A. (2018). How to Increase the Information Assurance in the Information Age. *Journal of Defense Resources Management, 9*(1), 45-57. https://www.jodrm.eu/issues/volume9_issue1/05_Sosin.pdf

Stacey, R. D. (2011). *Strategic management and organization dynamics: The challenge of complexity* (6th ed.) Essex, England: Pearson. https://epdf.pub/strategic-management-and-organisational-dynamics-the-challenge-of-complexity-to-.html

Sundler, A. J., Lindberg, E., Nilsson, C., & Palmér, L. (2019). Qualitative thematic analysis based on descriptive phenomenology. *Nursing open*, *6*(3), 733-739. https://doi.org/10.1002/nop2.275

Supriyadi, Y., & Hardani, C. W. (2018, November). Information System Risk Scenario Using COBIT 5 for Risk and NIST SP 800-30 Rev. 1 A Case Study. In *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)* (pp. 287-291). IEEE. https://doi.org/10.1109/icitisee.2018.8721034

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian journal of hospital pharmacy*, 68(3), 226. https://doi.org/10.4212/cjhp.v68i3.1456

Svilicic, B., Kamahara, J., Rooks, M., & Yano, Y. (2019). Maritime cyber risk management: An experimental ship assessment. *The Journal of Navigation*, *72*(5), 1108-1120. https://doi.org/10.1017/S0373463318001157

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security, 12*(3), 417-432.

Taiwo, K. O. (2019). *Organizational Decision-making Through Employee Diversity* (Doctoral dissertation, Walden University). https://scholarworks.waldenu.edu/dissertations/7759/

Tajir, G. (2018). Ethical treatment of participants in public health research. *Journal Of Public Health and Emergency*, 2(1). https://doi.org/10.21037/jphe.2017.12.04

Tam, K., & Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, *18*(1), 129-163. https://doi.org/10.1007/s13437-019-00162-2

Tamul, D., Elson, M., Ivory, J. D., Hotter, J. C., Lanier, M., Wolf, J., & Martinez-Carrillo, N. I. (2020, April 7). Moral Foundations' Methodological Foundations: A Systematic Analysis of Reliability in Research Using the Moral Foundations Questionnaire. https://doi.org/10.31234/osf.io/shcgv

Taylor, M. J., Fornusek, C., Ruys, A. J., Bijak, M., & Bauman, A. E. (2017). The Vienna

FES Interview Protocol–A mixed-methods protocol to elucidate the opinions of various individuals responsible for the provision of FES exercise. *European journal of translational myology*, *27*(3). https://doi.org/10.4081/ejtm.2017.6604

Teece, D. J. (2018). Dynamic capabilities as (workable) management systems theory. *Journal of Management & Organization*, *24*(3), 359-368. https://doi.org/10.1017/jmo.2017.75

Teusner, A. (2016). Insider research, validity issues, and the OHS professional: one person's journey. *International Journal of Social Research Methodology, 19*(1), 85–96. https://doi.org/10.1080/13645579.2015.1019263

Thomas, D. R. (2017). Feedback from research participants: are member checks useful in qualitative research? *Qualitative Research in Psychology*, *14*(1), 23-41. https://doi.org/10.1080/14780887.2016.1219435

Thomas, L., & Briggs, P. (2016). Assessing the value of brief automated biographies. *Personal and Ubiquitous Computing*, 20(1), 37-49. https://doi.org/10.1007/s00779-015-0896-2

Tran, V., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology*, 80, 88-96. https://doi.org/10.1016/j.jclinepi.2016.07.014

Trautman, L. J. (2016). Managing cyberthreat. *Santa Clara Computer & High Tech. LJ*, *33*, 230. https://doi.org/10.2139/ssrn.2534119

Trimble, D., Monken, J., & Sand, A. (2017). A framework for cybersecurity assessments

of critical port infrastructure. *2017 International Conference on Cyber Conflict (CyCon U.S),* Cyber Conflict (CyCon U.S.), 2017 International Conference on, 1. https://doi.org/10.1109/cyconus.2017.8167506

Tsokkis, P., & Stavrou, E. (2018, June). A password generator tool to increase users' awareness on bad password construction strategies. In *2018 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-5). IEEE. https://doi.org/10.1109/ISNCC.2018.8531061

Tuntivivat, S., Jafar, S. F., Seelhammer, C., & Carlson, J. (2018). The Indigenous Youth Engagement in Environmental Sustainability: Native Americans in Coconino County. *The Journal of Behavioral Science*, 13(2), 81-93. https://so06.tci-thaijo.org/index.php/IJBS/article/view/106174

Turner, J. R., & Baker, R. M. (2019). Complexity theory: An overview with potential applications for the social sciences. *Systems*, *7*(1), 4. https://doi.org/10.3390/systems7010004

Tzafestas, S. G. (2017). *Systems, cybernetics, control, and automation*. River Publishers. https://www.bookdepository.com/Systems-Cybernetics-Control-Automation-Spyros-G-Tzafestas/9788793609075

Uprichard, E., & Dawney, L. (2019). Data diffraction: Challenging data integration in mixed methods research. *Journal of Mixed Methods Research, 13*(1), 19-32. https://doi.org/10.1177/1558689816674650

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

US Department of Homeland Security (2012), "CyberSkills task force report", US Department of Homeland Security, Homeland Security Advisory Council. www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf

US Department of Homeland Security [DHS] (2018). https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

U.S. Department of Homeland Security[DHS]. (2019). *Secure Cyberspace and Critical Infrastructure.* https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. https://doi.org/10.5430/jnep.v6n5p100

Van Assche, K., Verschraegen, G., Valentinov, V., & Gruezmacher, M. (2019). The social, the ecological, and the adaptive. Von Bertalanffy's general systems theory and the adaptive governance of social-ecological systems. *Systems Research and Behavioral Science*, *36*(3), 308-321. https://doi.org/10.1002/sres.2587

Van Rijnsoever, F. J. (2017). (I Can't Get No) Saturation: A simulation and guidelines for sample sizes in qualitative research. *PloS one*, 12(7), e0181689. https://doi.org/10.1371/journal.pone.0181689

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.

https://doi.org/10.1145/3170521.3170525

Visner, S. S. (2016). The cybersecurity storm front- forces shaping the cybersecurity landscape: A framework for analysis. *Georgetown Journal of International Affairs, 17*(3), 85-99. https://doi.org/10.1353/gia.2016.0039

Viswambharan, A. P., & Priya, K. R. (2016). Documentary Analysis as a Qualitative Methodology to Explore Disaster Mental Health: Insights from Analyzing a Documentary on Communal Riots. *Qualitative Research*, 16(1) 43–59. https://doi.org/10.1177/1468794114567494

Von Bertalanffy, L. (1950). An outline of general system theory. *British Journal of the Philosophy of Science, 1*, 135–165. https://doi.org/10.1093/bjps/i.2.134

Von Bertalanffy, L. (1968). *General systems theory: Foundations, development, application* (Revised ed.). New York, NY: George Braziller. https://monoskop.org/images/7/77/Von_Bertalanffy_Ludwig_General_System_Theory_1968.pdf

Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal*, *15*(4), 407-426. https://doi.org/10.5465/255139

Wagner, N., Şahin, C. Ş., Winterrose, M., Riordan, J., Hanson, D., Peña, J., & Streilein, W. W. (2017). Quantifying the mission impact of network-level cyber defensive mitigations. *The Journal of Defense Modeling and Simulation*, *14*(3), 201–216. https://doi.org/10.1177/1548512916662924

Waldrop, M. M. (1992). *Complexity*: The emerging science at the edge of order and chaos. New York, NY: Simon & Schuster. https://doi.org/10.1063/1.2809917

Wallis, S. E., & Valentinov, V. (2017). A limit to our thinking and some unanticipated moral consequences: A science of conceptual systems perspective with some potential solutions. *Systemic Practice and Action Research*, 30(2), 103-116. https://doi.org/10.1007/s11213-016-9394-3

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, 17(6), 681-699. https://doi.org/10.1007/s10207-017-0382-0

Warren, G., & Szostek, L. (2017). Small business strategies for sustainability beyond 10 years. *International Journal of Applied Management and Technology*. 16. 111–122. https://doi.org/10.5590/IJAMT.2017.16.1.07

Watkins, D. C. (2017). Rapid and rigorous qualitative data analysis: The "RADaR" technique for applied research. *International Journal of Qualitative Methods*, 16(1), 1-9. https://doi.org/10.1177/1609406917712131

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

Weishapl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation, and learning. *Computers & Security, 77,* 807-823. https://doi-

org.ezp.waldenulibrary.org/10.1016/j.cose/2018.02.001

Whalen, E. A. (2018). Understanding a shifting methodology. *International Journal of Contemporary Hospitality Management, 30*(11), 3423-3441. https://doi.org/10.1108/ijchm-08-2017-0536

Whitehead, D., & Whitehead, L. (2016). Sampling data and data collection in qualitative research. https://ro.ecu.edu.au/ecuworkspost2013/1555/

Wixted, J. T., Mickes, L., & Fisher, R. P. (2018). Rethinking the reliability of eyewitness memory. *Perspectives on Psychological Science, 13*(3), 324-335. https://doi.org/10.1177/1745691617734878

Yang, G., Dai, L., & Wei, Z. (2018). Challenges, threats, security issues and new trends of underwater wireless sensor networks. *Sensors*, *18*(11), 3907. https://doi.org/10.3390/s18113907

Yang, T., Ku, C., & Liu, M. (2016). An integrated system for information security management with the unified framework. *Journal of Risk Research*, 19(1), 21-41. https://doi.org/10.1080/13669877.2014.940593

Yasin, M. M., Czuchry, A. J., & Small, M. H. (2018). Organizational security: A conceptual framework and implementation issues. *Competition Forum*, 16(1), 38-49. https://www.questia.com/library/journal/1P42133361299/organizational-security-a-conceptual-framework

Yeong, M. L., Ismail, R., Ismail, N. H., & Hamzah, M. I. (2018). Interview protocol refinement: Fine-tuning qualitative research interview questions for multi-racial populations in Malaysia. *The Qualitative Report, 23*(11), 2700-2713.

https://nsuworks.nova.edu/tqr/vol23/iss11/7/

Yin, R. K. (2017). Case study research and applications: Design and methods. Sage publications. https://www.bookdepository.com/Case-Study-Research-Applications-Robert-K-Yin/9781506336169

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed). Thousand Oaks, CA: Sage. https://www.bookdepository.com/Case-Study-Research-and-Applications-RobertK-Yin/9781506336169

Young, D., Lopez Jr, J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, 14, 43-57. https://doi.org/10.1016/j.ijcip.2016.04.001

Yurtsevena, M. K., Buchananb, W. W., & Pilantb, M. S. (2016). Introducing Sustainability Concepts into University Curricula Through Systems Thinking. *Sociology*, *6*(9), 583-590. https://doi.org/10.17265/2159-5526/2016.09.004

Zăgan, R., Raicu, G., Hanzu-Pazara, R., & Enache, S. (2018). Realities in the maritime domain regarding cybersecurity concept. In *Advanced Engineering Forum* (Vol. 27, pp. 221-228). Trans Tech Publications. https://doi.org/10.4028/www.scientific.net/aef.27.221

Zhao, J., Bai, J., Zhang, Q., Yang, F., Li, Z., Zhang, X., & Bai, R. (2018, December). The Discussion about Mechanism of Data Transmission in the OSI Model. In *2018 International Conference on Transportation & Logistics, Information & Communication, Smart City (TLICSC 2018)*. Atlantis Press.

https://doi.org/10.2991/tlicsc-18.2018.1

Zhao, X., Yan, H., & Zhang, J. (2017). A critical review of container security operations. *Maritime Policy & Management*, 44(2), 170–186. https://doi.org/10.1080/03088839.2016.1253883

Zukunft, A. (2015). United States Coast Guard Cyber Strategy. *Retrieved on November 27*, 2017. https://www.hsdl.org/?view&did=767212

Appendix A: Projecting Human Research Participants Certificate of Completion

Certificate of Completion

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

Date of completion: 09/12/2015

Certification Number: 1839546

Appendix B: Interview Protocol

Participant Code: _____

Date: _____

1. The interview protocol will begin with introductions: Hello, My Name is
2. Explain to the participant the interview will be recorded and thank the participant for agreeing to participate in the study.
3. Introduce the Type of interview: Qualitative Multiple Case Study
4. Explain the Research Topic: To explore strategies to protect the organization's network
5. Discuss the Research Question: What strategies do IT specialists use to implement standard practices needed to secure the organization's network for maritime cybersecurity from cyber-related threats?
6. Let the participants know the interview will be 30-45 minutes, or until all of the interview questions have been answered.
7. Explain the participant has the right to stop at any time during the interview and that the consent form is to meet human subject requirements.
8. At the end of the interview, I will explain the plan for the follow-up interview for member checking.
9. Once I confirm that all statements and answers are satisfactory to the participant, the interview will end, and I will thank the participant for participating.

Semistructured interview questions

1. What methods and tools have IT specialists used to prevent cyber-related threats from the organization's network for maritime?
2. How would those methods and tools secure the organization's network for maritime security successfully?
3. What methods have IT specialists used that failed to prevent cyber-related threats from the organization's network for maritime?
4. What challenges have IT specialists faced implementing strategies?
5. What metrics do IT specialists use to assess the vulnerabilities or ensure the organization's network is secure for maritime?
6. What type of training or certifications has been identified through cybersecurity awareness policies at your organization?
7. What additional information, processes, or documentation would you like to provide that may help in this research study?
8. As an IT specialist, what is your role if a breach or threat is identified?