2019

Exploring Industry Cybersecurity Strategy in Protecting Critical Infrastructure

Mark Boutwell
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Mark Allen Boutwell

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. Gail Miles, Committee Chairperson, Information Technology Faculty
Dr. Nicholas Harkiolakis, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

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

Walden University
2019

Abstract

Exploring Industry Cybersecurity Strategy in Protecting Critical Infrastructure

by

Mark Allen Boutwell

MS, Walden University, 2017

MS, University of Phoenix, 2009

BS, Hawaii Pacific University, 2003

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December, 2019

Abstract

Successful attacks on critical infrastructure have increased in occurrence and sophistication. Many cybersecurity strategies incorporate conventional best practices but often do not consider organizational circumstances and nonstandard critical infrastructure protection needs. The purpose of this qualitative multiple case study was to explore cybersecurity strategies used by information technology (IT) managers and compliance officers to mitigate cyber threats to critical infrastructure. The population for this study comprised IT managers and compliance officers of 4 case organizations in the Pacific Northwest United States. The routine activity theory developed by criminologist Cohen and Felson in 1979 was used as the conceptual framework. Data collection consisted of interviews with 2 IT managers, 3 compliance officers, and 25 documents related to cybersecurity and associated policy governance. A software tool was used in a thematic analysis approach against the data collected from the interviews and documentation. Data triangulation revealed 4 major themes: a robust workforce training program is crucial, make infrastructure resiliency a priority, importance of security awareness, and importance of organizational leadership support and investment. This study revealed key strategies that may help improve cybersecurity strategies used by IT and compliance professionals, which can mitigate successful attacks against critical infrastructure. The study findings will contribute to positive social change through an exploration and contextual analysis of cybersecurity strategy with situational awareness of IT practices to enhance cyber threat mitigation and inform business processes.

Exploring Industry Cybersecurity Strategy in Protecting Critical Infrastructure

by

Mark Allen Boutwell

MS, Walden University, 2017

MS, University of Phoenix, 2009

BS, Hawaii Pacific University, 2003

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December, 2019

Dedication

I dedicate this work to my wife, Ute, who is my best friend and the love of my life. Thank you for your strength and understanding. Without you, I would only be half the person I am.

Acknowledgments

Thank you to my parents and family for their positive encouragement and laughter. Dr. Gail Miles, my committee chair, was the light at the end of the tunnel that guided me and ensured I remained centered. Thank you! Your mentoring kept hope alive. Dr. Nicholas Harkiolakis and Dr. Steven Case, thank you for keeping me grounded and moving forward through constructive and actionable feedback. And thank you to the Walden University staff who was ever present and supportive to help keep the ride as smooth as possible.

Table of Contents

List of Tables iv

Section 1: Foundation of the Study 1

Background of the Problem 1

Problem Statement 2

Purpose Statement 3

Nature of the Study 3

Research Question 4

Conceptual Framework 5

Operational Definitions 6

Assumptions, Limitations, and Delimitations 6

Assumptions 6

Limitations 7

Delimitations 8

Significance of the Study 9

Contribution to Information Technology Practice 9

Implications for Social Change 10

A Review of the Professional and Academic Literature 11

Routine Activity Theory 13

Supporting Theories 16

Cybersecurity in Critical Infrastructure 21

Cybersecurity Strategy 25

Information Technology and Operations Technology 33
Critical Infrastructure Resiliency 39
Transition and Summary 40
Section 2: The Project 42
Purpose Statement 42
Role of the Researcher 42
Participants 45
Research Method and Design 48
Method 48
Research Design 50
Population and Sampling 54
Ethical Research 57
Data Collection 59
Instruments 59
Data Collection Technique 62
Data Organization Techniques 66
Data Analysis Technique 68
Reliability and Validity 71
Dependability 72
Credibility 73
Transferability 73
Confirmability 74

Transition and Summary 75
Section 3: Application to Professional Practice and Implications for Change 76
Overview of Study 76
Presentation of the Findings 77
Theme 1: A Robust Workforce Training Program is Crucial 80
Theme 2: Make Infrastructure Resiliency a Priority 92
Theme 3 - Importance of Security Awareness 100
Theme 4 - Importance of Organizational Leadership Support and Investment 111
Applications to Professional Practice 121
Implications for Social Change 123
Recommendations for Action 124
Recommendations for Further Study 126
Reflections 128
Summary and Study Conclusions 129
References 130
Appendix A: Interview Protocol 164
Appendix B: Training Certificate from the National Institute of Health Office of Extramural Research 168

List of Tables

Table 1. Sample Keywords and Phrases 12

Table 2. List of Theories Considered with the Applicable Factor(s) 21

Table 3. Distribution of Theme 1 81

Table 4. Distribution of Theme 2 93

Table 5. Distribution of Theme 3 101

Table 6. Distribution of Theme 4 113

Section 1: Foundation of the Study

Nation-state cyber actors like China, North Korea, Russia, and Iran pose a sophisticated threat to cybersecurity of U.S. critical infrastructure (Cilluffo, 2016). The U.S. House Permanent Select Committee on Intelligence (2014) clearly articulated the continued threat to the United States critical infrastructure in testimony to the U.S. House Permanent Select Committee on Intelligence:

> There shouldn't be any doubt in our minds that there are nation-states and groups out there that have the capability to do that, to enter our systems, to enter those industrial control systems, and to shut down, forestall our ability to operate our basic infrastructure, whether it's generating power across this nation, whether it's moving water and fuel, whether it's moving… (p. 13).

Background of the Problem

Advances in technology, convergence of legacy and modern technologies in critical infrastructure, and the "moment in time" nature of today's cybersecurity governance present a dynamic cybersecurity challenge for managers and practitioners that equally challenges the supporting training and compliance programs (Lošonczi, Nečas, & Naď, 2016). Cyber threats are dynamic and persistent requiring timely cybersecurity response to remain viable (McLaughlin et al., 2016).

Malicious attacks that include STUXNET, HAVEX, GRIZZLY STEPPE, and BLACKENERGY demonstrate sophisticated cyber exploitation capability against critical infrastructure in key industries such as banking, retail, and healthcare (Lemay, Calvet, Menet, & Fernandez, 2018; Maitra, 2015; National Cybersecurity & Communications

Integration Center & Federal Bureau of Investigation, 2016; Vermeulen, 2015). In 2015, the SANS Institute conducted a security survey of Industrial Control System (ICS) providers/owners comprising 314 participants who indicated challenges in sustaining reliable and secure operational capability; over 40% of those surveyed were unable to identify the intrusion source, 32% revealed a successful intrusion, 15% indicated more than a month was needed to detect an intrusion, and 34% believed there were multiple breaches in a 12-month time frame (Harp & Gregory-Brown, 2015). Lessons learned and attack analyses have been documented and studied throughout the literature (Alcaraz & Zeadally, 2015) revealing standardization in the context of cybersecurity implementation should remain voluntary and elusive (Shackelford, Sulmeyer, Craig, Buchanan, & Micic, 2017). In the context of IT design, implementation, and support of critical infrastructure; the pursuit of cybersecurity strategies to proactively identify, assess, and understand threats continues to advance (Alcaraz & Zeadally, 2015).

Problem Statement

Critical infrastructure experiences sophisticated cyber-attacks and damages incurred by employee negligence or malicious intent (Karabacak, Yildirim, & Baykal, 2016). Between January, 2017, and April, 2017, the U.S. Department of Health and Human Services Office for Civil Rights reported the breach of sensitive personal identity information of over 1,618,000 individuals reported by private and public healthcare facilities and practitioners (U.S. Department of Health and Human Services Office for Civil Rights, 2017). The general IT problem is that cyber threats often challenge the IT professionals' ability to provide effective cybersecurity to critical infrastructure. The

specific IT problem is that some IT managers and compliance officers lack cybersecurity strategies to mitigate cyber threats to critical infrastructure.

Purpose Statement

The purpose of this qualitative case study was to explore cybersecurity strategies used by IT managers and compliance officers to mitigate cyber threats to critical infrastructure. The population for this study included IT managers and compliance officers of two industrial organizations in the Pacific Northwest United States that have cybersecurity strategies to mitigate cyber threats to critical infrastructure. The completed study influences strategic planning as IT providers learn best practices in critical infrastructure IT compliance strategy to inform threat mitigation solutions. Implications for social change include society's increased confidence in critical infrastructure such as the ability to produce and deliver key power and water utilities as well as protecting the reliability and availability of financial and healthcare services.

Nature of the Study

I considered three research methodologies. I chose a qualitative methodology for this study. Researchers use a qualitative method to explore, define, and understand a phenomena (Petocz & Newbery, 2016). Therefore, I chose the qualitative method to explore and understand the phenomenon of strategies that IT managers and compliance officers use to mitigate cyber threats to critical infrastructure. In a quantitative method, researchers use one or more mathematical techniques to measure the collected data producing numeric and/or statistical models that serve to represent the observations related to the phenomena (McCusker & Gunaydin, 2015). I did not choose a quantitative

method for this research because there were no quantifying of variables and no numeric or statistical modeling based upon the measurement of variables. Mixed methods research integrates qualitative and quantitative methods to provide a more holistic understanding of the research problem (Molina-Azorín, 2016). This study did not include the use of theory to form and test hypotheses, and therefore, a mixed methods approach was not suitable for this study.

In choosing a qualitative methodology, I considered three viable design options: case study, phenomenology, and narrative. The case study approach in qualitative research enables the contextual exploration of a phenomenon through one or more sources (Zainal, 2017). I chose a case study design for in-depth exploration of a complex problem through contextual analysis. A phenomenology approach is used for the analysis of lived experiences to clarify meaning (Giorgi, 1997; Petocz & Newbery, 2016). The use of a phenomenology design was not appropriate because this study did not focus upon shared experiences. Sandelowski (2000) defined a narrative approach as the qualitative summary of lived experiences as articulated by the respective individual. The use of a narrative design was not appropriate for this study because the study did not focus upon exploring life's meaning.

Research Question

RQ: What IT cybersecurity strategies are used by IT managers and compliance officers to mitigate cyber threats to critical infrastructure?

Conceptual Framework

The conceptual theory chosen for this study was routine activity theory (RAT) developed by criminologist L. Cohen and M. Felson in 1979. According to Cohen and Felson, RAT requires three criteria that must exist together for a crime to take place: an offender, a target, and the absence of prevention. Cohen and Felson stated that RAT is based upon the principle that an offender exists and is focused upon a target, prevention or lack thereof, and a location. All three of the RAT criteria must exist together in the same place for a threat to pursue action resulting in an incident, and therefore, if one of those criteria is mitigated or controlled, then it may be possible to influence associated incidents (Cohen & Felson, 1979). The application of the RAT supports the exploration and analysis of IT and operations technology (OT) convergance that forms operational critical infrastructure environments (Reyns, Henson, & Fisher, 2016). Existing research of those critical infrastructure constructs in the context of design and implementation of the IT and OT where there is a lack of viable and sustainable strategy remains a core challenge (Alcaraz & Zeadally, 2015). Organizations performing critical or sensitive operations such as financial, utilities, and communications providers should expect a cybersecurity breach to happen referencing a “kill chain” concept (Denham, 2015, p. 5). I chose RAT because it considers the target from the threat's perspective in the context of routine day-to-day activities. I used this theory to approach cybersecurity in critical infrastructure from a proactive cyber defense point of view to explore the context of the offender, target, and prevention (cybersecurity) criteria in reoccurring, routine tasks and functions.

Operational Definitions

Critical infrastructure: Assets deemed critical to the public's health, welfare, finances, and security (Karabacak et al., 2016).

Operational technologies: Industrial systems that operate building infrastructure, utilities, transport, logistics, manufacturing, autonomous vehicles, ships, drones, robotics, and healthcare equipment (Piggin, 2018).

Cybersecurity in critical infrastructure: Functions performed to protect IT and OT that comprise the critical infrastructure to include access (Luo, 2016).

Cyber-physical systems (CPS): Transformative technologies for managing interconnected systems between its physical assets and computational capabilities (Lee, Bagheri, & Kao, 2015).

Cyber threats: A threat with malicious intent to cause harm or damage in the cyber domain (Cilluffo, 2016).

Data analysis: Action of converting the raw collected data into information (Almalki, Gray, & Sanchez, 2015).

Industrial control systems: Systems comprised of information and communication technologies (ICTs) to control and automate stable operation of industrial processes (McLaughlin et al., 2016).

Assumptions, Limitations, and Delimitations

Assumptions

Gergen (2015) noted that research is informed by the use of applicable assumptions or presuppositions formed from our informed biases such as in prior

experience or through prior research. Berger (2015) stated that shared experiences often form challenges for researchers and participants, sometimes resulting in the creation and misapplication of assumptions. Those assumptions are influenced by the perceptions formed during the relevant experiences and, in turn, may impact the ability to make informed decisions because certain data were set aside based upon the assumptions (Berger, 2015). Certain assumptions have been made in this study. I assumed that each of the organizations identified employed at least one IT or compliance professional with prior experience in critical infrastructure protection. I assumed that all employees are expected to comply with the organization's cybersecurity policies and guidance. Another assumption was that participants in the qualitative research interviews are qualified to be part of the study, and each participant is open and truthful in their responses using their relevant knowledge and experience. I also assumed the chosen qualitative research method and conceptual framework for this study would be successful in facilitating the analysis of the collected data and provide relevant findings to the research question. To help mitigate my assumptions, semistructured interview questions and member checking were used to give interviewees an opportunity to articulate and validate their responses in more depth based upon experience rather than providing a simple yes or no answer.

Limitations

According to Busse, Kach, and Wagner (2016), some researchers use the terms of boundary conditions and limitations interchangeably, and therefore they clarified their definition of limitations as theoretical and methodological deficiencies of a study that do not greatly call into question the validity of the research and are unforeseen influences

that might impact the results. In my research, I studied cybersecurity strategies in critical infrastructure with the implementation varying substantially based upon the business and technology needs of the respective organization. There were four principal limitations related to this study. The varying complexity of critical infrastructure represented a limitation in the large number of possible configurations that might be implemented, represented by the number of combinations such as integration of cyber-physical design, embedded systems (e.g. Internet of Things [IoT] devices), legacy OT, and existing organizational IT architecture components to enable functions such as remote access and monitoring. A second limitation was the unknown diversity and depth of the interviewee's experiences that could limit a holistic representation of the organization's cybersecurity planning and implementation. Similar topics suggested the need for further research if the goal were to determine whether the results might suggest similarities or influences across a larger dataset. Thirdly, aligning a strategy to the organization's strategic objectives may include security of critical infrastructure processes and procedures, introducing the potential that data collection might be limited by operations and physical security policy. Finally, the unique factors of cybersecurity in critical infrastructure limited the consideration of defining and describing standard IT cybersecurity practices as a baseline template or model.

Delimitations

Delimitations are constraints that have been anticipated and used to scope and establish boundaries for the respective research (Mertens & Barbian, 2015). The population sample for this study was taken from a specific geographic area, which was

the Pacific Northwest United States. The interview population comprised IT and compliance professionals with knowledge of or experience in cybersecurity in critical infrastructure in the Pacific Northwest United States. I did not consider participants without the knowledge or experience in critical infrastructure cybersecurity in the Pacific Northwest.

Significance of the Study

Contribution to Information Technology Practice

In 2015, the cyber attack on Ukraine's power grid represented the first successful targeted attack of a national power infrastructure and provided insight to the vulnerabilities of critical infrastructure in the United States (Sullivan & Kamensky, 2017). IT represents the key elements of critical infrastructure such as command and control, and therefore, this study may help IT professionals gain insights into the use of cybersecurity strategy to mitigate cyber threats, as well as gain insight and knowledge leading to customized strategies in training and compliance to further enhance or enable cybersecurity efficiency and effectiveness. The results of this study provided IT professionals insgihts about the key factors of successful cybersecurity strategy and best practices in critical infrastructure to include influences of training and compliance.

There is a significant amount of research, past and present, focused upon cybersecurity concerns and challenges within critical infrastructure that include very detailed information on cyber threats and associated vulnerabilities (Alcaraz & Zeadally, 2015; Harp & Gregory-Brown, 2015). However, most research directions and characterizations of the applicable technologies represent results at a top

architecture/infrastructure level and/or system-of-systems context. In the absence of a guiding foundation to create robust and dynamic strategies, IT managers are often left to form more relevant research and/or analyses to meet their respective needs (Alcaraz & Zeadally, 2015). This study provided new insights and research focal points, and potentially new strategic direction for IT managers, compliance officers, and critical infrastructure stakeholders.

Implications for Social Change

The findings from this study contribute to positive social change by advancing society's confidence in critical infrastructure such as the reliability and stability of key utilities, banking, and healthcare services. Research has documented the increased concerns with meeting the present and future challenges of cybersecurity in critical infrastructure (Luo, 2016), which underpins the concerns in society of industry's ability to provide and sustain the necessary reliable and stable critical infrastructure services during crisis and malicious attack. This study provided exploration and contextual analysis of today's cybersecurity strategy and situational awareness of IT and critical IT and OT management to enable positive social change through innovative and creative IT strategies that proactively address threat mitigation and support informed decision making processes. In addition, society's confidence in those managing the associated resources is strengthened, for example, by identifying the associations between critical infrastructure and CPS (IoT) to personal cybersecurity implications in day-to-day life activities.

A Review of the Professional and Academic Literature

The purpose of this qualitative case study was to explore industry cybersecurity strategies used in defending critical infrastructure. The literature review was guided by the RQ: What IT cybersecurity strategies are used by IT managers and compliance officers to mitigate cyber threats to critical infrastructure? I explored the RAT, cybersecurity strategies in critical infrastructure, and concepts in active and passive cyber defense. The review of literature focused upon four key areas: (1) RAT, (2) cybersecurity strategy, (3) challenges in compliance and training in a cybersecurity context, and (4) enabling and sustaining cybersecurity resiliency. The review of the RAT was focused on identifying and understanding factors relevant to victimization such as motivation, opportunity, and guardianship. The research of cybersecurity strategy included background, best practices, and challenges. The research of compliance and training included the roles in supporting and enabling of cybersecurity. Finally, the research of cybersecurity resiliency involved the consideration and application of active defense as applied to cybersecurity and the supporting programs including compliance and training.

Related topics are present throughout the literature such as how existing cybersecurity strategy is technology focused and often ignores the human factor, how traditional vulnerability based cybersecurity approaches are not sufficiently diverse and dynamic to protect modern critical infrastructure, and how the pursuit of cybersecurity resiliency demands a deep awareness and understanding of the IT and OT infrastructures.

Additional cybersecurity topics consistent throughout the literature were revealed as key support functions of cybersecurity compliance and training.

The literature review consisted of 199 candidate sources related to cybersecurity strategy in critical infrastructure, RAT, IT compliance, and training. I used keyword searches to identify and refine the sources; Table 1 contains keywords and phrase samples. After characterizing the initial sources, 116 were chosen for the literature review. My search strategy primarily focused on sources published in 2015 or later to stay in 5-years of the anticipated date of this doctoral study approval. All sources were checked against the Ulrich database to determine peer-reviewed status. Of the 199 sources reviewed, 94% were peer-reviewed and 93% were published in 5-years of the anticipated approval of my doctoral study. The sources were primarily obtained via Google Scholar and Walden University's Library to identify sources in various databases including IEEE Xplore and ProQuest.

Table 1

Sample Keywords and Phrases

Keyword phrases
critical infrastructure AND *cybersecurity*
routine activity theory OR *general systems theory*
information security AND *cyber-physical systems*
(*qualitative* OR *quantitative*) AND *research methodologies*

Routine Activity Theory

Cohen and Felson introduced the RAT in 1979, which explored the rise in violent and nonviolent physical crime activity following World War II focusing on the influences of routine activity in the enabling of criminal opportunity from the offender's perspective (Cohen & Felson, 1979). RAT was developed from the crime opportunity theory to represent the convergence of an offender and target at a time and location of little or no guardianship (Cohen & Felson, 1979). RAT introduced three factors that must be present for a crime to occur: the offender, a target, and the lack of a guardian. Cohen, Kluegel, and Land introduced an adaptation of RAT in 1981 to focus on the risks that an individual offender would encounter and use in a decision making process to help decide whether an opportunity exists for a crime to occur. Cohen and Felson (1979) assumed the existence of an offender, and therefore, the location, target, and guardianship become the core considerations. Cohen and Felson (1979) examined and debated modification to activity patterns with implications on criminal behavior due to the changes in one or more of the key RAT factors: offender, target, and guardian. A key tenant of RAT is the premise that modification of one or more of the key RAT factors may result in positive implications for criminal activity such as inadequate guardianship like cybersecurity practices (Cohen & Felson, 1979).

Cohen and Felson (1979) introduced RAT in response to increased physical crime in a post World War II society. Many researchers including Leukfeldt and Yar (2016), McNeeley (2015), Reyns and Henson (2016), Vernon-Bido, Padilla, Diallo, Kavak, and Gore (2016) have studied the application of RAT to various types of cybercrime.

Advances in IT evolved the original RAT factors to adapt to the influences of cyber dependencies in daily online activities, for instance an offender, cyber user, and lack of appropriate technical or nontechnical controls (Reyns & Henson, 2016). Existing research into the adaptation of RAT in response to society's expanded use of modern IT encompasses theories such as the rational choice theory and lifestyle- RAT as outlined by Reyns and Henson (2016). This adaptation reflects the needed evolution and maturation of RAT to account for situational conformity by an offender, target, and guardian (Reyns & Henson, 2016; McNeeley, 2015; Vernon-Bido et al., 2016).

Technology has evolved significantly since Cohen and Felson (1979) first introduced RAT, and therefore, advances in IT have expanded the possibilities in applying the theory in research and analysis of malicious activity in physical and virtual environments (Fischer, 2016; Leukfeldt & Yar, 2016; Soomro, Shah, & Ahmed, 2016). According to Leukfeldt and Yar (2016) and Wang, Gupta, and Rao (2015), RAT identified four principal properties composing the acronym VIVA (value, inertia, visibility, and accessibility) that when present hold the potential for a target. Choosing a target may vary based upon the motivation(s) and goal(s) of the attacker, and therefore, the four VIVA properties would be measured accordingly to best identify and define a target from the offender's perspective of the VIVA properties. According to Fischer (2016), risk management is a basic factor of IT cybersecurity strategy, but one with substantial value and the associated risk assessment process helps to prioritize the possible threat vectors and infrastructure areas based on criticality of function. An efficient risk management program is in theory a proactive strategic measure used to

mitigate or eliminate organizational cybersecurity risks using RAT to help focus attention upon the principal factors of threat (offender), vulnerability (target), and implication (guardian; Fischer, 2016). My study used the principal factors of offender, target, and guardianship of RAT in a cybersecurity context. Risk management has been seen throughout the literature review noting how important it is for IT cybersecurity professionals to acquire and maintain an awareness and understanding of cyber threat capabilities as well as their own infrastructure to best visualize their perception of normal cybersecurity and threat environments.

The use of IT is common and anticipated in modern society, which exposes citizens to cyber threats in the context of routine daily activities. Leukfeldt and Yar (2016) support Cohen and Felson's (1979) work by reporting an offender might be one or multiple actors, a target could be the data or IT system, and a guardian can take the form of a technical or nontechnical control such as access authentication and system administrator. Fischer (2016) supports Cohen and Felson's work by describing cybersecurity risks comprising three principal elements: threat (who = offender), vulnerability (what = target), and implication (attack vector = lack of guardianship). Fischer (2016), Leukfeldt and Yar (2016), and Reyns et al. (2015) promoted guardianship as a leading factor in information security (cybersecurity). Guardianship is a crucial point of consideration in this study. IT managers and cybersecurity strategy are some examples of guardianship. RAT exists throughout the literature in studying criminal activity to explore a diverse range of possibilities when applied in a cyber context, thus

enabling a holistic cybersecurity focus that includes an expanded awareness and understanding of the daily operating environment.

I chose RAT for the conceptual framework of this study to better understand and explore cybersecurity strategies used by IT managers and compliance officers in critical infrastructure to mitigate cyber threats. RAT defines succinct threat factors, which include an offender, target, and lack of effective guardianship, as well as the four properties represented by VIVA (Cohen & Felson, 1979; Leukfeldt & Yar, 2016). A strength of RAT is in providing a framework for use in analysis to predict activity patterns (Levi, 2017; Williams, 2015). The RAT factors and properties serve as a foundation to assess and analyze offender, target, and/or guardianship indicators in cyber activity providing the opportunity to analyze a probable target through a threat lens, which would include technology and human factors (Busse et al., 2016; Fischer, 2016). They concluded that a guardian inherits a stakeholder role through responsibility for others who may be directly or indirectly engaged in the associated activity or situation such as the relationship of a user and cybersecurity manager.

Supporting Theories

Von Bertalanffy is noted as the father of general systems theory (GST), which he introduced circa 1955, as well as for establishing the skill community for the research and application of GST (Rousseau, 2015; Von Bertalanffy & Sutherland, 1974). Skyttner (1996) stated the role of GST is to be systemic rather than focused upon a singular system with using GST as the comparative lens to analyze and articulate differences between multiple systems at the same or varying levels within the infrastructure. Systems theory

is used to help outline and understand the complexities of infrastructures comprising dynamic systems and/or components, and therefore, the analysis of integrated systems, or components that might become integrated, in critical infrastructure may not be suited to using GST (Katina, 2015). Rousseau (2015) postulated that GST has lacked sufficient detail resulting in roughly 12 distinct interpretations of von Bertalanffy's original theory work calling into question its application to systemic and complex problems. Although there is strength in GST using a qualitative system descriptive approach (Twining, Heller, Nussbaum, & Tsai, 2017), the challenges presented by the dynamic and robust system behaviors of today's complex cybersecurity in critical infrastructures including ambiguous patterns in the associated data (Bochkov, Lesnykh, Zhigirev, & Lavrukhin, 2015; Rousseau, 2015; Sapaty, 2016) introduces a divergence from using GST to study those same cybersecurity challenges in critical infrastructure. GST remains focused upon the use of comparative analysis of multiple systems in consideration of environmental influences (Skyttner, 1996; Valentinov & Chatalova, 2016). If labeled as a system, it is typical to believe that construct to comprise components that deliver reliable and stable functionality (Rousseau, 2015; Skyttner, 1996). GST is a powerful resource for comparative analysis of multiple systems, with a primary focus upon the differences between systems rather than activity to, from, and about the infrastructure in a cybersecurity context, and therefore, it was rejected as the underlying theory for this study.

Becker introduced rational choice theory (RCT) in 1968 as an economic approach to crime. RCT is an economic theory that provides insight to user behaviors assuming

the use of a cost-benefit decision approach with a key consideration of humans not being purely rational when making decisions (Becker, 1968; McCarthy, 2002; Paternoster, Jaynes, & Wilson, 2017; Vernon-Bido et al., 2016). RCT has been a popular theory to study hackers because it provides insight to behaviors used in making decisions (Vernon-Bido et al., 2016), placing emphasis on the individual's propensity to make informed decisions (McCarthy, 2002). Choi and Lee (2017) contrasted cyber lifestyle choices to better understand offender and victimization occurrences, further supporting existing research that shows cyber lifestyle choices influence identification as a target. A researcher applying RCT places an individual's decision-making process on the cognitive behavior (Leukfeldt & Yar, 2016) and attempts to analyze the offender's choices through a cognitive behavior lens (Fusch & Ness, 2015; Vernon-Bido et al., 2016). For this study, I did not choose RCT because it emphasizes individual behaviors in personal decision-making processes.

Kuutti introduced activity theory (AT) in 1991. AT is also focused on an individual's cognitive behavior, but in the context of focusing upon the human-computer interaction over the cybersecurity context of technology and human factors (Karanasios, Allen, & Finnegan, 2015). The analysis of advanced attacks involving critical infrastructure has been associated with technical and human elements, going beyond the boundaries that might encompass an individual's behavior and interactions with the technology. AT lends itself to analysis of integrating differing technologies like IT and OT and the patterns formed in using the related systems (Karanasios et al., 2015). AT was conceived for use in information systems research, noting that the human-computer

interaction in the context of an information system should be the object of analysis (Kuutti, 1991; Mursu, Luukkonen, Toivanen, & Korpela, 2007). AT focuses upon an individual's behavior as a result of tasks performed in using an information system without specifically analyzing the technological implications of the human-computer activity in a cybersecurity context (Kuutti, 1991; Mursu et al., 2007). This study considers human and technology factors in cybersecurity strategy, and therefore, I did ot choose AT because it reduces human behavior considering the tasks and activities but only loosely considers the factors represented by the technology.

Brantingham and Brantingham introduced crime pattern theory (CPT) in 1981, which focused on the offender to determine how targets are identified and chosen. An individual's behavioral patterns formed during the course of their day-to-day activities are studied to help understand how target opportunities are chosen (Brantingham & Brantingham, 1993; Weisburd, 2015; Welsh, Zimmerman, & Zane, 2018). The use of CPT reveals patterns of behaviors in a diversity of location, time, and environment for analysis to determine how those factors might explain the offender's choices (Brantingham & Brantingham, 1993; Weisburd, 2015; Welsh et al., 2018). CPT promotes the main elements of nodes, paths, and edges, and in contrast to RAT, the CPT elements are similar with the nodes and paths roughly equating to the offender identifying target opportunities (Weisburd, 2015). CPT uses an offender's choice of target opportunity to provide insight to how those opportunities might be chosen (Welsh et al., 2018). CPT has been used to focus upon prevention (Welsh et al., 2018), but it does not offer the

same approach through analysis of the offender, target, and guardianship factors as offered by RAT, so I did not choose CPT for this study.

Table 2 is a list of the theories considered to include the principal factor for each theory relevant to this study.

Table 2

List of Theories Considered with the Applicable Factor(s)

Theory	Factors
Routine activity theory	Motivated offender with a chosen target based upon stated properties to include the lack of effective guardianship.
Rational choice theory	Cognitive behavior - decision-making process.
General systems theory	System concept - qualitative and descriptive.
Activity theory	Cognitive behavior - human-computer interaction.
Crime pattern theory	Environmental behavior - daily activities.

Note. Adapted from Vernon-Bido et al. (2016).

Cybersecurity in Critical Infrastructure

The complexity of the critical infrastructure cyber threat landscape continues to evolve resulting in the challenges faced by IT managers and compliance professionals. According to Shoemaker, Davidson, and Conklin (2017) cybersecurity remains an enduring challenge for the IT discipline. Cybersecurity entails a co-existence with supportive programs to include compliance and training that serve principal roles in social change (Shoemaker, Davidson, & Conklin, 2017). Society has become intimately dependent upon information, operations, and communication technologies, and therefore, critical infrastructure threat landscapes have surfaced with target rich environments that offer attractive rewards for those with the motivation and opportunity to attack (Liu, Dong, Ota, Yang, & Liu, 2016; Payette, Anegbe, Caceres, & Muegge, 2015). Traditional IT architectures have become an extension of the respective critical infrastructures as a

result of incorporating IT functionalities such as Internet connectivity with operations and communication technologies (Shackelford et al., 2017). The evolution of cybersecurity strategy continues to depend upon the maturation of supporting IT programs that include compliance and training (Adams & Makramalla, 2015; Pham, Pham, Brennan, & Richardson, 2017). A convergence of IT and OT in critical infrastructure is representative of the inherent cybersecurity challenges, and in turn, highlights the interdependencies between the respective technology disciplines (Shackelford et al., 2017). Modern critical infrastructure is often formed through the converngence of IT, OT, and existing network architectures to provide the necessary functionality to meet operational needs. This convergence surfaces unforeseen cybersecurity challenges for operations and the related support disciplines like compliance and training.

The formation of critical infrastructure introduces unique technical challenges, which bring together IT and OT disciplines as well as the underpinning disciplines to include compliance and training. There is a cross-industry responsibility for cybersecurity strategy that spans information, operations, and communication disciplines to address the challenges of intersecting disciplines to form critical infrastructure that also includes enabling programs like compliance and training (Genge, Kiss, & Haller, 2015). A common thread is the need for collaboration of strategic and tactical level strategic planning, and implementation, for cybersecurity in critical infrastructure (Borum, Felker, Kern, Dennesen, & Feyes, 2015). The existence of cybersecurity gaps, revealed by the integration or convergence of dynamic IT environments with static OT environments continues to pose substantial challenges (Jacobs, von Solms, & Grobler, 2016). IT

environments are often protected by a singular approach of passive defense such as system patches, hardware and software version upgrades, and life-cycle replacement to ensure incorporate of modern components and configuration options (Soomro et al., 2016). OT environments are often comprised of legacy capabilities protected by legacy cyber defense features (Fischer, 2016). Long-term challenges exist in cybersecurity such as focus upon indigenous IT cybersecurity design to get out in front of cyber threats and maintaining a high state of awareness, and understanding, of the cyber threat environment (Fischer, 2016; Nazir, Patel, & Patel, 2017). For IT design and environment factors to benefit cybersecurity strategic planning and implementation there is a need to stay in tune with IT technology advances to be aware of, and understand, threat implications to best anticipate cybersecurity preparedness (Fischer, 2016). My study emphasized the need to obtain and maintain an intimate awareness and understanding of the cyber threat landscape and associated cyber tradecraft to influence and enable cybersecurity strategies. These studies revealed the topic of IT and OT convergence while emphasizing the needs of cybersecurity strategy to ensure operational stability and resiliency while including the supporting programs.

IT and OT skill communities are principal disciplines found throughout the literature most relevant to critical infrastructure. Modern IT professionals embrace the principals of confidentiality, integrity, and availability to bridge the gaps between IT and operational environments (Cabrera, 2016; Popescul, & Radu, 2016). Threats to critical infrastructure is not limited to cybersecurity vulnerabilities, so holistic defense must include the supporting programs (Cabrera, 2016). As such, IT professionals are subject

matter and highly qualified experts on the relevant IT tradecraft and subsequent cybersecurity tradecraft, and therefore, that expertise does not necessarily extend to a familiarity of OT architectures and capabilities (Shafqat & Masood, 2016). Stability, safety, and reliability are main concepts embraced by OT professionals in operating critical infrastructures, which have remained static since implementation (Wolf & Serpanos, 2017). The integration of IT is necessary to provide OT environments with the functionality required to enable cybersecurity (Alcaraz & Zeadally, 2015). Functionality required by critical infrastructure to establish and sustain operational environments has been a common topic throughout this literature.

Challenges faced by IT managers and cybersecurity professionals are often linked to interdependencies between IT and OT. Today's IT architectures benefit from modern hardware, software, and network capabilities incorporating the best cybersecurity features with succinct interoperability and compatibility (Shackelford et al., 2017). In contrast, OT architectures have limited interoperability and compatibility using legacy hardware, software, and networking capabilities such as proprietary protocols, and limited cybersecurity features (Fischer, 2016). In a modern cybersecurity and cyber threat context, defense of an OT environment is unique and does not respond to traditional IT cybersecurity tradecraft (Payette et al., 2015). IT and OT disciplines are not interchangeable; however, the key to designing and implementing an effective and sustainable cybersecurity strategy in critical infrastructure demands collaboration (Baldi, 2016; Popescul & Radu, 2016). IT and OT cybersecurity, compliance, and training must be interleaved to enable and sustain a critical infrastructure environment (Baldi, 2016).

Cybersecurity strategy and implementation must be adjusted to accommodate an IT and OT culture where key resources form a collaborative production environment to unify the best of both in meeting unique technology challenges (Baldi, 2016). For example, improving employee awareness to, and understanding of, the threats of cyber attacks, as well as an intimate knowledge of the organization's technological landscape (Knowles, Prince, Hutchison, Disso, & Jones, 2015). IT managers and compliance officers must be able to design and integrate cyber compliance and training programs into cybersecurity strategy to mitigate cyber threats to critical infrastructure (Chaves, Rice, Dunlap, & Pecarina, 2017; Kim & Kim, 2017). The above research spotlights the need to incorporate cyber compliance and training programs to assist in mitigating cyber threats to critical infrastructure by recognizing the unique variables introduced by IT and OT convergence.

Cybersecurity Strategy

Cyber environments are very dynamic with critical infrastructure environments introducing added dynamics, which presumes to include the associated cyber threat landscape. Wang et al. (2015) identified and focused upon the four properties of value, inertia, visibility, and accessibility in the context of protective measures such as establishing passive or active cyber defenses. The focus was on the user and system behaviors in the context of a threat (offender), vulnerability (target), and response (guardianship). Holt, Burruss, and Bossler (2016) analyzed malicious software propagation through the automation of attack processes while emphasizing the necessity of hardening potential targets by focusing on cybersecurity passive and active defense

tradecraft. Mitigation of cyber threats begins with knowing the threat landscape and the infrastructure being defended. They concluded with the identification of a relationship between increased cyber threat incidents and the presence of advanced infrastructure. Mitigating cyber threat represents the identification and description of dynamic and robust concerns and challenges to cybersecurity strategy in critical infrastructure (Leukfeldt & Yar, 2016). Topics seen through a cybersecurity lens, relevant to threat mitigation, begin to appear in the literature to include the convergence of IT and OT, general workforce IT cybersecurity awareness, and the applicability of cybersecurity focused compliance and training programs.

The approach to designing and implementing cybersecurity within a physical environment may not be suitable for application within a cyber environment; however, IT modernization has begun to level the playing field. Rather than being anticipated, cyber threat opportunities are expected in today's IT invested society, in turn presenting the opportunity for innovative exploration of cyber defense tradecraft (Stratton, Powell, & Cameron, 2017). The convergence of modern IT and legacy OT produces a diverse range of physical and cyber threat environments within critical infrastructure (Holt, Burruss, & Bossler, 2016; Pursiainen, 2017). The offender's opportunity to identify or exploit a target is no longer solely dependent upon physical proximity to a target or the cybersecurity measures protecting a potential target. (Fischer, 2016; Leukfeldt & Yar, 2016; Reyns & Henson, 2016). The identification, assessment, and analysis of potential offenders in a physical environment are complex, and therefore, application within a cyber environment offers specific challenges (Leukfeldt & Yar, 2016). A potential target

in a physical environment is observable such as the geospatial location of the offender in comparison to the target as well as offender and target interaction (Fischer, 2016; Reyns et al., 2015). In a cyber environment the offender is not observable as in the physical environment, and therefore, with the advances in IT the offender's process for choosing a target in a cyber environment is not publically visible and introduces a significant challenge to identifying the offender's behavior, motivations, access, and identity (Leukfeldt & Yar, 2016; McLaughlin et al., 2016). However, IT modernization provides the necessary advances for the observation of an offender and target in a cyber environment, made possible through the evolution of cybersecurity tradecraft (tools, techniques, and methodologies; Fischer, 2016; Nazir et al., 2017). For example, geospatial information can be obtained by using techniques against the Internet Protocol data, which would also provide information regarding the interaction of the offender and target (Fischer, 2016; Nazir et al., 2017). Whether in the physical or cyber environment, the choice of passive or active cybersecurity protective measures remains an analytic challenge and the ability to understand the offender's decision making process leading to target choice. Focus should remain upon the indications that might reveal patterns and behaviors to help predict attacks on critical infrastructure to include revealing the association between the offender, target, and cybersecurity protection measures (guardianship).

Challenges in protecting critical infrastructure have been compounded by the introduction of modern IT and the increased dependency upon services provided in today's modern society. The convergence of technologies that comprise critical

infrastructure also includes Internet and remote network connectivity which calls for proactive strategies (Weinberg, Milne, Andonova, & Hajjat, 2015). In addition to updating current governance (e.g. policy, legislation) to at least reflect today's cybersecurity challenges and cyber threats, the addition of threat intelligence represents a modern response in updating or planning a cybersecurity program (Lošonczi et al., 2016). The complexity and sophistication of attacks against critical infrastructure requires proactive response instead of a vulnerability based defensive posture (McLaughlin et al., 2016). In summary, adapting and evolving traditional cybersecurity practices is necessary to meet the demands of protecting the new micro and macro cyber environments created through the application of IT and OT to form new, hybrid, configurations.

To ensure key cybersecurity enabling and supporting programs keep pace, a holistic risk and knowledge gap assessment should be incorporated into strategic planning (Knowles et al., 2015). A cybersecurity culture that has become routine may also suffer from stagnation, and therefore, there may be implications and similar challenges within an organization to the compliance and training programs supporting the cybersecurity strategy (Li, Yu, Deng, Luo, Ming, & Yan, 2017). The focus upon modernizing the cybersecurity strategy should also address supporting programs such as compliance and training to achieve balance (Knowles et al., 2015). Cybersecurity strategy must be reviewed frequently and consistently to ensure implementation of the workflows and tasks comprise the latest considerations for the organization's technical and operations environments in the context of the cyber threats and production landscape

(Ahlmeyer & Chircu, 2016). Changes in cyber threat tradecraft are a daily occurrence, but cybersecurity is often not programmed with the necessary resources to keep pace (Auffret et al., 2017). Cyber compliance and training programs represent a mitigation approach to assist in countering cyber threats and to strengthen the cybersecurity strategy.

Looking beyond the cyber vulnerabilities is a topic that has gained traction in the literature. Research of cybersecurity strategy in critical infrastructure has mostly focused upon cyber vulnerabilities and the creation of associated checklists or 'best practices', in an attempt to address the maturation of cyber threats against critical infrastructure (Quigley, Burns, & Stallard, 2015). Some researchers introduced and highlighted active defense measures such as the use of threat analysis focused upon gaining an intimate understanding of the target infrastructure and an equal understanding of prior attack tradecraft (Adams & Makramalla, 2015). However, cybersecurity incidents continue to increase with an evolution of sophisticated tradecraft resulting in a dynamic and robust cyber threat while policy and research fall further behind (Adams & Makramalla, 2015). There have been several increasingly sophisticated cyber attacks that targeted ICS comprised in critical infrastructure with some causing physical damage (Massacci, Ruprai, Collinson, & Williams, 2016). IT managers and compliance officers have a significant amount of available research as reference to help guide their respective cybersecurity strategy efforts. The resulting data and analysis presented by the cited research in this study explores cybersecurity strategies in the pursuit of mitigating cybersecurity challenges and also reveals considerations in compliance and training strategy.

A sense of urgency exists for establishing and sustaining cybersecurity in critical infrastructure. The IoT phenomenon is a representation of an order of magnitude increase in Internet connected devices (Ahlmeyer & Chircu, 2016; Ebersold & Glass, 2015). A focus upon critical infrastructure in the context of IoT security considerations, revealed IoT as a possible access vector to critical infrastructure (Ebersold & Glass, 2015; Weinberg, Milne, Andonova, & Hajjat, 2015). Three major gaps were surfaced, which are a lack of security design, lack of security guidelines and standards, and a lack of associated governance (Ahlmeyer & Chircu, 2016; Lee & Lee, 2015). Most stakeholders seem to lack a necessary awareness and understanding of the cyber threats and the extent of the cyber threat posed to their respective infrastructures (Ahlmeyer & Chircu, 2016; Auffret et al., 2017; Weinberg et al., 2015). Cybersecurity principles must be designed in the system and component development processes (Genge, Graur, & Haller, 2015). Convenience often overshadows IT cybersecurity in pursuit of cost and productivity savings; the literature revealed a survey of IT professionals with 70% agreeing that existing frameworks may not adequately address technological advances in critical infrastructure (Lee & Lee, 2015; Weber, 2015; Weinberg, Milne, Andonova, & Hajjat, 2015). The rapid pace of technological advances challenge legislation and governance of cybersecurity in critical infrastructure forcing cybersecurity into a mostly self-regulation state with a wide range of strategic implementation approaches resulting in significant gaps amongst stakeholders (Fischerkeller & Harknett, 2017; Garcia, Forscey, & Blute, 2017; Li, Tryfonas, & Li, 2016). Traditional IT cybersecurity, focused solely upon vulnerability based mitigation, remains a challenge of its own (Esteves,

Ramalho, & De Haro, 2017). A common thread with IT cybersecurity is the lack of awareness and understanding amongst management and cybersecurity practitioner skill communities of the breadth and depth of cyber threats, in particular, the lack of identifying and defining the threat landscape, which belongs to their own infrastructures.

Advanced cyber attacks on targets in government and industry continues to be highlighted in today's media, revealing the topic of management engagement in the sphere of cybersecurity. The cybersecurity management challenge has been described as a choice between convenience and cybersecurity (information confidentiality and integrity) (Weinberg, Milne, Andonova, & Hajjat, 2015) coupled with the consideration that cybersecurity in critical infrastructure continues to lack the anticipated sense of urgency considering the consequences of successful compromise (Mangelsdorf, 2017). When IT modernization results in the enhancement of OT, the threat landscape related to both become intertwined, and therefore, the creation of new and hybrid vulnerabilities highlight the potential for new threats (Urquhart & McAuley, 2018; Weinberg, Milne, Andonova, & Hajjat, 2015). The research identified a management factor, revealing insights to the need for consideration of the role and possible challenges introduced by management in cybersecurity strategy. The management role must be equally considered along with the technical and human factors pointing to a direction of inquiry for my study.

Two principal factors must be considered in cybersecurity strategy, which are technical and human. Most of the cybersecurity challenges seen in the literature reflects upon one of those factors (Cong, Dang, Brennan, & Richardson, 2017; Cook, Janicke,

Smith, & Maglaras, 2017; Gartzke & Lindsay, 2015; Gyunka & Christiana, 2017; Han, Kim, & Kim, 2017). Cybersecurity strategy is key to resolving the management challenge of designing a sustainable program to protect and defend the subject critical infrastructure (Weinberg, Milne, Andonova, & Hajjat, 2015). Technical and human factors must be built into the design for achieving a holistic cybersecurity program (Weinberg, Milne, Andonova, & Hajjat, 2015; Wirtz & Weyerer, 2017). The inclusion of expertise spanning the technical and human factors are covered throughout the literature, but remain one of the leading challenges in management implementation of cybersecurity strategy.

Converging multiple technologies often spotlights potential opportunities to cyber threats due to the likelihood that existing cybersecurity strategy is not flexible enough to quickly adapt to the changes that result. Future challenges in critical infrastructure cybersecurity includes the avoidance or mitigation of second and third order of effects related to the convergence of IT with OT to modernize what has historically been standalone architectures (Borum, et al., 2015; Elkhannoubi & Belaissaoui, 2016; Jacobs, von Solms, & Grobler, 2016). Borum, et al. (2015), Elkhannoubi and Belaissaoui (2016), and Jacobs, von Solms, and Grobler (2016) found citical infrastructure often representing an integration of legacy OT with modern IT to form one or more complex systems necessary to achieve the required infrastructure. The threat landscape becomes rich with likely targets because the current cybersecurity strategy lacks flexibility underpinned by supporting programs like IT compliance and training to help with capturing and acting upon the early indication and warning signs.

Sharing information and cyber intelligence in the critical infrastructure community is a topic revealed throughout the literature. Critical infrastructure are unique in their own configurations, components, and implementations, thus creating a greater dependency upon sharing cybersecurity knowledge and lessons learned (Chaves, Rice, Dunlap, & Pecarina, 2017; Fraga-Lamas, Fernández-Caramés, Suárez-Albela, Castedo, & González-López, 2016). A dynamic and robust cybersecurity strategy for critical infrastructure first depends upon the organization securing its' information and architectures using a deep awareness and understanding the existing information, operations, and communication technologies that form the combined, or integrated, environment (Lee & Lim, 2016). Depending strictly upon cyber vulnerability alerts and post incident lessons learned is reactive, and therefore, provides the threat to the technology and people a substantial advantage (Esteves, Ramalho, & De Haro, 2017). The core approach includes a deep knowledge of the infrastructure from the defender and attacker's perspectives that also includes consideration of the intelligence harvested from detailed analyses of the threat tools, techniques, methods, and prior attacks (Lemay et al., 2018). Obtaining a greater breadth and depth of knowledge and understanding of the infrastructure help maximize the focus upon the unique demands and strategic surprises that are often anticipated in protecting critical infrastructure, and also to highlight the role of key support programs to include compliance and training.

Information Technology and Operations Technology

In today's society, IT plays a pivotal role in day-to-day activities, and therefore, has resulted in creating dedicated users of its computing, storage, and communication

offerings. The convergence of IT and OT is necessary to meet the functional requirements for a critical infrastructure such as on-demand and mobile remote connectivity in near real-time, quickly and seamlessly (Baldi, 2016; Ponomarev & Atkison, 2016). The creation of unique configurations in the formation of critical infrastructures has provided insight to weaknesses not previously anticipated, which results in new cyber threat opportunities (Fitzgerald, 2015). The application of traditional IT information security practices has revealed complex challenges to cybersecurity strategy as a result of integrating IT protocols with legacy OT protocols, a need for diverse simulation and testbedding environments, and the reliability and scalability of end-to-end encryption of sensor data and network communications (Mclaughlin et al., 2016; Qassim et al., 2017). The research has revealed a focus upon modernization of human-machine interface and the pursuit of increased mobility as a result of the expanding role of the IoT, training and response readiness, and the need for communications infrastructure that enables crucial data transport functionality (Sajid, Abbas, & Saleem, 2016; Sicari et al., 2015; Yoon, Dunlap, Butts, Rice, & Ramsey, 2016; Zhu, He, Xiang, Zhang, & Pattavina, 2016). The research points to the creation of a rich cyber threat landscape that is created through what is considered a creative integration of IT and OT with existing communication technology.

Traditional IT considerations often become complex challenges in critical infrastructure operations. Critical infrastructure providers are faced with the daily challenges in protecting the operations environment and traditional IT data, and systems, from cyber threats in a newly formed construct (McLaughlin et al., 2016). Critical

infrastructure is composed of legacy and modern technologies with Internet connectivity, and therefore, providers are faced with the added challenges of cyber threats against their internal and extended IT architectures (Alcaraz & Zeadally, 2015; McLaughlin et al., 2016;). To protect the related data and systems the cybersecurity professional must understand the protocols that directly or indirectly relate to the data and systems, which goes beyond focusing upon the vulnerabilities alone (Candell, Zimmerman, & Stouffer, 2015; Cintuglu, Mohammed, Akkaya, & Uluagac, 2017; Wang, Du, Yang, Zhu, Shen, & Zhang, 2016). The research summarizes the importance of knowing the capabilities of the cyber threat in the context of the infrastructure to be protected. Without an adequate awareness and understanding of the 2nd and 3rd order of effects caused by the convergence and/or integration of modern IT and legacy OT capabilities, viable courses of action may not be properly considered resulting in weak implementation.

The convergence of traditional and modern technologies introduces a new cyber threat landscape for IT managers and cybersecurity professionals, and practitioners and IT managers in supporting disciplines to include compliance and training. Critical infrastructure has become a societal dependency lurking in the background, which was interleaved with the adoption and use of IT introducing the capacity for public consumption in the form of the Internet of Things (Farooq, Waseem, Mazhar, Khairi, & Kamal, 2015). ITcomprises systems used in critical infrastructure for computing and communication functions along with OT creating a convergence of the components to manage, monitor, and control physical processes such as with electric transformers, water-filter sensing, and gas pipe valves (Thames & Schaefer, 2016). In the context of

this study, critical infrastructure is a broad category of systems to include CPS, IoT, and ICS, such as Supervisory Control and Data Acquisition (SCADA), as a convergence of information, operations, and communications technologies to form an infrastructure, which is not geographically or geospatially bounded. Management must support cybersecurity from the top down and ensure all applicable programs incorporate the same level of flexibility to guide its effectiveness to remain relevant in directly or indirectly supporting cybersecurity (Knowles et al., 2015; Li et al., 2017). The review of this cybersecurity literature in association with critical infrastructure has revealed specific topics and challenges faced by IT managers. Unique environments created by the convergence and/or integration of IT and OT continues to guide cybersecurity research along with the supporting cyber programs such as compliance and training.

Innovation and creativity is a common pursuit in IT; however, OT has not garnered the same consideration. Cybersecurity applied as a function in the field of IT to protect critical infrastructure is an enduring strategic challenge (Labaka, Hernantes, & Sarriegi, 2016). The practice of converging or integrating modern IT and legacy OT in attempts to enhance critical infrastructure with required functionality such as mobile connectivity has created peer-architecture on the same level of cybersecurity urgency as the OT itself (Pursiainen, 2017). Critical Information Infrastructure Protection (CIIP) was introduced as a new area of research to spotlight the influence of modern IT in critical infrastructure in providing the functionality for control and automation, while creating a new threat landscape in converging IT and OT (Alcaraz & Zeadally, 2015; Bou-Harb et al., 2017). The design and implementation of physical and virtualized

capabilities in critical infrastructure inherently includes the potential for introducing one or more vulnerabilities (Ferdinand, 2015). Many of the vulnerabilities would be known such as a zero-day revealed during testing and evaluation resulting in a software or firmware update, and therefore, as integration progresses, anticipated vulnerabilities are documented to create a knowledge base as a result of integrating a component with a remediated zero-day and another component (i.e. software, hardware) to enable the required functionality (Ferdinand, 2015; Robert, Morabito, Cloutier, & Hémond, 2015). The overarching message in the literature in such situations is that cybersecurity should identify known, suspected, and causational vulnerabilities in order to anticipate threat vectors and implications to the goal of baselining what is normal patterns of component behavior.

The research has introduced the robust and dynamic challenges that begin to surface at the architecture level when different technologies are applied to achieve the necessary functionality to support critical infrastructure demands. Protecting IT assets is a significant challenge to protecting OT and communications (e.g. network and data transport) in critical infrastructure (Labaka, Hernantes, & Sarriegi, 2016). An example of the new cyber threat landscape as a result of IT and OT forming required infrastructure is the introduction of cloud computing to centralize data storage and access (Ali, Khan, & Vasilakos, 2015). Another key challenge is protecting data at rest and in transit as with sensor command and control, and the reliability of internal and external database interactions (de Fuentes, González-Manzano, Tapiador, & Peris-Lopez, 2017). In summary, the need to incorporate modern IT functionality in critical infrastructure like

remote access and encrypted network communications has become a leading concern of whether the pursuit of vulnerability focused cyber threat mitigation is creating more unpredicted vulnerability.

With the convergence, or integration, of IT with OT the new functionality and configurations contribute to the formation of a unique communication infrastructure that must be protected without degrading the critical services. This connectivity introduces unique cybersecurity weaknesses revealing an enduring public facing threat landscape and the inherent vulnerabilities associated with the individual IT components with the unforeseen vulnerabilities created as a result of the integration itself (Alcaraz & Zeadally, 2015; Cedergren, Johansson, & Hassel, 2017; Ferdinand, 2015; Labaka, Hernantes, & Sarriegi, 2016; Robert, Morabito, Cloutier, & Hémond, 2015). The principal weakness revealed by the research exists at the architecture integration level causing a need to pause and reassess how cybersecurity strategy might be viewed other than from a vulnerability lens.

A common topic revealed in the literature is research focused upon vulnerabilities and the resulting creation of checklists and descriptions related specific vulnerabilities, often forgetting to analyze the cyber threat. To help manage, track, and learn from threat incidents there are a number of public databases available to include Computer Emergency Response Teams (CERT), ICS-CERT, and Testbed Framework to Exercise Critical Infrastructure Protection (Alcaraz & Zeadally, 2015). According to ICS-CERT (2016), there are six prevalent weaknesses associated to ICS cybersecurity; (1) boundary protection, (2) increased access opportunities (internal and external), (3) compromised

accounts - user and system-administrators, (4) physical security, (5) auditing to include process and log analyses, and (6) clear text password communication and lack of detection and response for malicious use of a trusted account. It is not a leap in logic when discussing modern critical infrastructure to presume to consider IT and OT as one construct, and therefore, the application of cybersecurity strategy typical for IT does not fit seamlessly into a critical infrastructure environment (Fischer, 2016). Approaching cybersecurity strategy from a resiliency perspective and active cyber defense point of view offers a new point of inquiry for my study.

Critical Infrastructure Resiliency

Services like utilities and power are typically considered in the scope of critical infrastructure and modernized everyday activities have become dependent upon timely delivery of those services. The literature has revealed the topic, which is the fast evolving desire to achieve critical infrastructure resilience over the traditional pursuit of protection afforded through a cybersecurity program (Ferdinand, 2015; Labaka, Hernantes, & Sarriegi, 2016; Pursiainen, 2017). Dunn, Kaufmann, & Søby Kristensen (2015) discussed the critical need for focusing upon resiliency noting the principal catalyst as time-sensitive nature of the supported services. The convergence of IT and OT has become a core design consideration in forming critical infrastructure to meet documented requirements (Ferdinand, 2015; Pursiainen, 2017). Protecting the infrastructure from all possible cyber threats is not realistic while sustaining the necessary capabilities; instead, pursuit of infrastructure resilience is advanced over protection to include enhancing the role of cybersecurity, so the conceptual and strategic approach of

resiliency is based upon securing vital functions over the protection of component infrastructures underpinning those functions (Ferdinand, 2015; Pursiainen, 2017). Protection is viewed as a defensive posture that reacts to cyber attack instead of establishing a resilience posture that is proactive to address a broad range of threats (Ferdinand, 2015; Pursiainen, 2017). Traditional cybersecurity focused upon protecting or defending the cyber assets must adapt and evolve to achieve resiliency (Robert, Morabito, Cloutier, & Hémond, 2015). There is a low probability of success when trying to zero mitigate cyber threats in today's advanced IT and OT environments, so instead, resiliency has surfaced as a likely way ahead.

Transition and Summary

This section explored cybersecurity strategies used by IT managers and compliance officers to mitigate cyber threats to critical infrastructure. The research approach is outlined in the context of the study's stated problem and purpose through a review of the related literature. I chose to use a qualitative method to explore and understand the phenomenon associated to the challenges facing IT managers and compliance officers in mitigating cyber threats to critical infrastructure. A case study design and the RAT as the conceptual theory were chosen for this study for in-depth exploration of a complex problem through contextual analysis. The literature focused upon cybersecurity topics revealing challenges to critical infrastructure to include strategy, compliance, training, vulnerability and resiliency, IT, and the human factor.

Section 2 provided added detail on the selected research methodology. In addition, Section 2 described the role of the researcher, established guidelines for

participants, research method and design, population and sampling, ethical research considerations, data collection and analysis, and factors related to reliability and validity. Section 3 represents the analytic findings of the study, revealing themes associated with cybersecurity strategy in critical infrastructure.

Section 2: The Project

With this study I intended to provide an exploration of cybersecurity strategies used by IT managers and compliance officers to mitigate cyber threats to critical infrastructure. In this section of the study, I define and explain details on the role of the researcher, selection of participants, research methodology and design, population and sampling, ethical research, data collection techniques and related instruments, data organization techniques, data analysis, and reliability and validity.

Purpose Statement

The purpose of this qualitative case study was to explore cybersecurity strategies used to mitigate cyber threats to critical infrastructure. Cyber attacks targeting critical infrastructure have steadily increased in occurrence and sophistication, revealing challenges for IT and compliance professionals. IT managers and/or compliance officers of two industrial organizations in the Pacific Northwest United States composed the population for this study. Modern society has become reliant upon critical infrastructure, which represents a convergence of modern and legacy information, operations, and technologies. Strategic planning is an anticipated beneficiary of the completed study as IT and compliance professionals learn from successful cybersecurity practices in critical infrastructure. Implications for social change may include society's increased confidence as the breadth and depth of the reliance upon critical infrastructure is expanded.

Role of the Researcher

I was the primary data collection instrument for this qualitative study. My relationship to the subject area spans 35 years of intelligence and technical analysis

experience, along with associated experience in related compliance and training disciplines. Incorporating and adhering to robust data collection is a key factor to influencing the value and strength of the study results (Kallio, Pietila, Johnson, & Kangasniemi, 2016). Fusch and Ness (2015) and Kallio et al. (2016) discussed the importance of data collection and portrayed the role of the researcher as a principal intermediary. Young, Lopez, Rice, Ramsey, & McTasney, (2018) examined the broad use of interview techniques in research that encompass a wide span of population densities, revealing the inherent personal bias of the researcher(s) and the advantage of using a semistructured approach to help limit personal bias by taking advantage of equal influence on the direction of the interview by the researcher and participant. The semistructured interview approach includes the use of an interview protocol and presenting the questions in the published research (Kallio et al., 2016). Conducting an interview requires a balanced combination of several elements, for instance the relevant questions, proper tools, and the environment (Grenier & Dudzinska-Przesmitzki, 2015). In contrast to my analytic, compliance, and instructor experience, I am not an expert in critical infrastructure or in the design and implementation of cybersecurity strategy. An interview is a powerful technique to gain an awareness and understanding of participant experiences and insights, while serving as a strengthening element to the study design such as the identification of additional topics and association of themes trending in the literature and interviews (Kallio et al., 2016). Interviewing cybersecurity and compliance practitioners in the critical infrastructure industry provided direct insight to their experiences with the related challenges and successes.

I used the principles outlined in *The Belmont Report* (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979) to help guide the study and to safeguard ethical principals. I designed the semistructured interview protocol (Appendix A) and created the interview questions along with the eligibility criteria for determining participant qualification, which I used to assess and select the participants from those who chose to volunteer. I closely followed the design elements identified by Kallio et al. (2016), which included the study's research question as an anchor, developing semistructured questions based in part on the literature review, performing follow-up inquiry to clarify participant responses, and ordering the questions to help build upon the collected information. A letter of cooperation was used to contact candidate organizations and to document their approval to participate. I considered the suggestions of Grenier and Dudzinska-Przesmitzki (2015), Teusner (2016), and Young et al. (2018) on designing and conducting the interviews in an environment that promoted a sense of comfort and security, engagement, and professionalism with an air of flexibility to adhere to the standards described in *The Belmont Report* (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979) of respect for persons, beneficence, and justice. I successfully finished the training provided by the National Institute of Health Office of Extramural Research for protecting human research participants (Appendix B).

A common consideration in qualitative research is how to account, assess, and mitigate personal bias. Young et al. (2016) presented bias in qualitative research as a dominant challenge. Minimizing personal bias remains a vital goal of the researcher in

data collection and analysis (Butler, Hall, & Copnell, 2016). Testing the interview guide and the interview questions through mock interviews was suggested by Kallio et al. (2016) pointing out the advantages to the study in the form of uncovering potential bias and possible concerns with interpreting the guideline itself. In general, an interview is a common technique used in qualitative research methods resulting in providing essential advantages including but not limited to flexibility and breadth and depth of data analysis (Young et al., 2018). I created the interview protocol (Appendix A) as a mechanism to help mitigate personal bias through techniques such as literal transcription of audio recordings, notes taken during the interview, obtaining post interview feedback from the participants, and data triangulation.

Participants

I chose IT professionals with support and compliance experience as the target interview population for this study to obtain extant, present-day, data on experience and expertise in cybersecurity in critical infrastructure operational and/or support environments. The targeted IT and compliance professionals represented the managers and practitioners planning, enabling, implementing, and sustaining the cybersecurity strategies in critical infrastructure. Their insights in day-to-day performance of functions and correlated experiences typify the realities of cybersecurity applied in critical infrastructure.

IT and compliance professionals from the Pacific Northwest constituted the population for this study. The potential participants were volunteers in the study and were treated as autonomous agents. All data and analytic results are kept confidential

and securely stored. Potential participants were identified based upon the eligibility criteria. They were selected from a pool of candidates with current or prior experience in managing or supporting cybersecurity in a critical infrastructure owner/operator or support oriented organization. Contacting organizations engaged in critical infrastructure planning and implementation, and IT support companies to introduce the research details is a consideration when attempting to identify possible participant candidates (Hoyland, Hollund, & Olsen, 2015). The eligibility criteria used to identify potential candidates were (a) IT or compliance professional with responsibilities associated with critical infrastructure services/functions, (b) 2 or more years of cybersecurity experience as a manager or practitioner, and (c) prior or current knowledge of cybersecurity strategy/implementation in critical infrastructure. Participants represented experience in cybersecurity of critical infrastructure environments as managers and/or practitioners whose daily activities entail functions of compliance, training, auditing, and technical and nontechnical controls. To be selected, the candidate met the three eligibility criteria. Participants were identified using the predetermined eligibility criteria and then the proper contact path was selected, For example, if the candidate worked for a local electric utility company, the published contact information for the company was used in coordinating my request to contact individual employees for interview participation. Interview candidates may be identified using personal and professional networks and by working through available contacts to outline the purpose and details of the study focused upon advancing the pursuit of interview participants (Peticca-Harris, deGama, & Elias, 2016). Upon receiving IRB approval, I began a systematic approach to identify and gain

access to potential interview candidates and provided each interview participant an invitation letter to participant using e-mail or postal mail.

At the initial contact with each candidate I summarized the purpose and scope of the interview with emphasis on the problem statement and research question, as well as addressed questions from the candidate. If the candidate agreed to participate, the interview logistics were discussed with each candidate by e-mail to include date, time, location, and other preferences to best accommodate the participant's needs, which were included in the consent form provided to the participants. In addition, I outlined the interview workflow to prevent confusion or surprises in preparing for and starting the interview, for example, clearly articulating the points of expectation to record the interview using audio and/or video capabilities and manual note taking during the interview.

Slight alteration of the interview questions may serve to illicit deeper response by the participant (Turley, Monro, & King, 2016), and therefore, I connected with the participants through informal conversation using e-mail focused upon introduction, familiarization, and orientation to the study and interview protocol to better understand their backgrounds and thoughts regarding the interview. I built upon this connection by providing the study's consent form and interview protocol in advance for the participant's review and opportunity to form questions for clarification, if needed.

I anticipated the compiled data analysis product from participant interviews would contribute a condensed dataset that would bring to light success factors in cybersecurity strategy and themes traversing the existing literature through data triangulation.

Research Method and Design

In this section I present a description of the research method and design, and the justification for its use in the context of researching the applied IT problem statement. I also give details on the chosen research method, affiliated design, other methods and designs that were considered to amplify the discussion in Section 1.

Method

I chose a qualitative approach using a mutliple-case study design to explore cybersecurity strategies used by IT and compliance professionals to mitigate cyber threats in critical infrastructure. Mitigation approaches to cybersecurity challenges in critical infrastructure continue to concentrate upon internal cyber vulnerability instead of a holistic, interconnected, strategic view of an organization's resources and assets (Horne, Maynard, & Ahmad, 2017). Hussein (2015) described research methodologies as qualitative, quantitative, and mixed-methods going on to define mixed-methods in his research as the use of qualitative and quantitative methods to study the same phenomenon.

The qualitative approach is known for its strength in analysis of complex phenomena (Fagerholm, Kuhrmann, & Münch, 2017), which was used in this study as a purposive exploration of cybersecurity strategy in critical infrastructure to discover relevant themes. The qualitative method enabled attribution to cybersecurity strategy in critical infrastructure. The exploration and analysis of the collected data such as participant interviews result in robust data triangulation for associations found in the case context (Castillo-Montoya, 2016). Qualitative methods have the advantage of performing

concurrent data analysis and data collection, supporting the use of various approaches to include member checking and data triangulation (Ranney et al., 2015). I chose a qualitative approach for its strengths in collecting and analyzing numerical and non-numerical data in seeking a thorough exploration of the phenomena to discover and analyze relevant themes, and seek answers to the research question(s).

I considered the application of quantitative methods in this study. Quantitative research characterizes data with descriptive variables and measurements taken to create focused numeric data to explain dependency and interaction relevant to the phenomena (McCusker & Gunaydin, 2015). Mathematical models are created to help explain what is observed in the data (McCusker & Gunaydin, 2015). Quantitative methods are therefore typically chosen to represent numerical data in addressing a research question to provide answers in the form of how many or how much, testing of a hypothesis, or producing a statistical explanation of an action or condition (Molina-Azorín, 2016; Twining et al., 2017). To further emphasize, quantitative methods are suited to explore a problem in depth, to easily develop a hypothesis, to study a complex problem, or to explore a problem to gaining awareness and understanding of an activity (McCusker & Gunaydin, 2015; Molina-Azorín, 2016). Zainal (2017) stated that a weakness of quantitative methods is the limitation in exploring social and behavioral problems through a user's lens. A quantitative method was not appropriate for my study because it would not provide a holistic, in-depth, exploration of the case used to study the stated problem.

I considered options in using a mixed-method approach. Qualitative research views numeric or non-numeric data analytically in the same context, which is in the

pursuit of answers to one or more research question (Twining et al., 2017). The mixing of numeric and non-numeric data does not define a mixed-method research approach; the researcher's purpose for the respective data is the driving force in leveraging pieces, or in whole, one or more qualitative or quantitative methodologies to meet the research needs (McCusker & Gunaydin, 2015; Molina-Azorín, 2016; Twining et al., 2017). Applying qualitative and quantitative methods in the same research study presents a complementary approach using the strengths of both such as triangulation while introducing the weaknesses and issues (Twining et al., 2017). I decided that a mixed method approach did not meet the research needs of my study due to the demand on available resources and the identification of variables required to explore the phenomenon.

Research Design

I chose a multiple case study design to conduct my research. Zainal (2017) described the strength of a case study as the ability to explore and understand complex problems through contextual analysis; the case may be bounded to represent a geographic area or population sample, which may be focused in size and scope from small to large. In a case study, the target of the in-depth study is the phenomena and not the subject that comprises the datasets (Zainal, 2017). This study includes the exploration of cybersecurity strategies in critical infrastructure through the relevant literature and conducting interviews to obtain a current awareness and understanding of real-world experiences and challenges. Twining et al. (2017) highlighted the advantage of using a case study as the flexibility in collecting the needed volume and variety of data to ensure

in-depth analysis and to enable data triangulation. The interviews are focused upon gathering current knowledge and understanding of the participant's experiences, and therefore, the purposive semi-structured approach leverages questions to support how or why details of a phenomena in the context of cybersecurity strategy in critical infrastructure (Twining et al., 2017; Zainal, 2017). A multiple case study design is appropriate for my study to provide a method to collect data from different organizations using current and relevant literature and interviews for an in-depth analysis and exploration of the problem in a past and present frame of reference.

Three types of case study designs were considered for this study. Pearson, Albon, and Hubball (2015) identified and described the three case study designs based upon the study purpose, which are exploratory, explanatory, and descriptive. An exploratory case study can facilitate a deep dive into the subject phenomena to help answer the research question, and inform subsequent research (Melewar, Foroudi, Dinnie, & Nguyen, 2017). The explanatory case study can be used to identify and characterize interactions and relationships between the case factors (Pearson et al., 2015). A descriptive case study facilitates an in-depth contextual description of the case phenomena (Kaba, Baumann, Kolotylo, & Akhtar-Danesh, 2017). Gentles, Charles, Ploeg, and McKibbon (2015) recommended the use of single case study under the condition that between four and 15 cases were intended for study. Harrell (2017) and Weishäupl et al. (2018) referenced the approach to cases as single and multiple loop learning events, choosing single loop learning for a timely response to attack incidents. A multiple case study is comprised of several independently defined cases and the results from each are compared to one

another to derive a comparative analysis result to help draw conclusions (Gentles et al., 2017). A multiple case study design helps to define and understand the phenomena in a real-world environment using document analysis and interviews for an increased awareness and understanding of the stated problem to address the research question in a bounded context (Gentles et al., 2015). The use of a single case study did not support the purpose of my study, so I chose a multiple case study to gain an in-depth description and understanding of cybersecurity strategies in critical infrastructure.

The alternate qualitative approaches that were considered, but not chosen, included phenomenology and narrative. A phenomenology approach explores the meaning of an individual's experience by analyzing the results of an interview using open-ended questions (Petocz & Newbery, 2016). The analysis of the phenomenology result set produces a description of the experience using the story obtained from the interview as a reference baseline with an overarching goal to determine the meaning or basis of the individual's experience (Bowden & Galindo-Gonzalez, 2015). A qualitative researcher following a phenomenology design would represent the participant's point of view of the phenomena as an experience and how the experiences may have contrasted (Lewis, 2015). I did not choose to use a phenomenology approach because my study is not focused upon the meaning of individual perspectives regarding the phenomena.

Narrative research is used to approach the problem through the description or explanation of past experiences using a story to describe the information (Hege et al., 2018). Lewis (2015) noted that narratives help in describing a lived experience as informally represented by the individual. Narrative has been identified as a key enabler

for an individual to reflect upon a life experience (Esposito & Freda, 2016). My study is focused upon obtaining data through interviewing participants to collect their experiences relevant to cybersecurity in critical infrastructure. A narrative approach focuses upon an individual's life story and would not provide the required data to address the study's research question. The narrative approach was not chosen because my study is an exploration of cybersecurity strategy in critical infrastructure and not reflecting upon the life stories of the respective individuals.

Data saturation is a crucial part of this research. Gentles et al., (2015) described data saturation as the point in research where data becomes redundant because further data collection does not yield new information, and indicates the point of ending collection. According to Fusch and Ness (2015) a standardized approach to achieve data saturation has not been established, and therefore, identified criteria for indicating data saturation which are no new information, themes, or coding. These criteria are achieved through in-depth data collection represented by the quality and veracity instead of the strict measurement by volume of data collected (Fusch & Ness, 2015). To achieve data saturation, I conducted interviews of a diverse, purposive, sampling of the target population comprised of IT and compliance professionals. Using an interview approach to ensure the interviews were not limited to scientists and engineers is necessary to prevent highly technical data overshadowing the problem (Fusch & Ness, 2015; Hennink, Kaiser, & Marconi, 2017). As the researcher and data collection instrument, I strived to ensure the participants drive the research context. Fusch and Ness (2015) highlighted the association between data triangulation and saturation. I used the research data sources to

triangulate the results to help identify and fill information gaps, which supported data saturation.

Population and Sampling

The population for this study is IT and compliance professionals within industrial organizations operating or supporting critical infrastructure within the U.S. Pacific Northwest. I contacted the chosen organizations to get a decision on whether each would participate. Researchers need to understand the study's target population and describe it in sufficient detail (Asiamah, Mensah, & Oteng-Abayie, 2017). The study population was IT and compliance professionals within the organizations who are part of the study. Rahi (2017) stated that qualitative study is the pursuit of in-depth understanding of a phenomenon with the assumption that a single individual can represent a population. I used eligibility criteria to guide the selection of interview participants for this study by first identifying candidates within the participating organizations. Sarstedt, Bengart, Shaltoni, and Lehmann (2017) emphasized the need for well-defined protocols in a case study design approach. I collected and analyzed data using a homogeneous purposive sample. Following the participant eligibility criteria outlined in the interview protocol (Appendix A), the interview participants selected for this study were IT and compliance professionals with knowledge of cybersecurity strategy.

There are many techniques that comprise probability and non-probability sampling methods with three non-probability techniques having greater popularity, which are purposive/judgmental, quota, and convenience sampling (Sarstedt et al., 2017). Researchers have been plagued with sampling size issues and understanding the

population assists in determining the necessary sampling to support the study (Rahi, 2017). Clearly describing the study population remains a subtle flaw in qualitative research with an implication toward reader confusion and misinterpretation of the study population (Asiamah, Mensah, & Oteng-Abayie, 2017). Purposive sampling allows the researcher to focus upon the practitioners directly engaged in the topic, or area, of study; hence, the selection of participants is not random with a focus on answering the research question (Sarstedt et al., 2017). The population for the study embodies IT and compliance professionals with knowledge of cybersecurity strategy in critical infrastructure. Homogeneous sampling is used against a candidate population that shares related traits to include, but not limited to, skill community, work role, and job position (Sarstedt et al., 2017). The adoption of advanced IT, to include data storage and networking, has continued to increase within private, public, and government organizations prompting a closer look at IT and compliance staffing levels (Williams, Asi, Raffenaud, Bagwell, & Zeini, 2016). IT and compliance staffing levels often fall short in keeping pace with the rate of IT transformation such as with the introduction of the Health Information Technology of Economic and Clinical Health Act in 2009 by President Barack Obama (Singh & Hess, 2017; Williams et al., 2016). Two case organizations were identified within the U.S. Pacific Northwest and I anticipated there were four eligible IT and compliance professionals. I chose to use homogeneous purposive sampling to select interview candidates for this study.

I offered each participant a choice of virtual or physical interview preferences based upon their geographic location. Holland et al. (2016) emphasized the importance

in obtaining participant preferences regarding the interview settings, which may include holding a small group (researcher plus a neutral participant) and choice of using email, audio only, or video chat to conduct the interview. When discussing preferences it is helpful to provide options for the participant (Ali & Johnson, 2017). Therefore, I coordinated in advance with each participant to ensure the interview environment, whether virtual or physical, met the participant's expectations and needs. I provided options for conducting the interview that addressed the participant's feedback. There are many preference options that could be identified by an interview participant to include the type of language, and therefore, it is important for the researcher to clearly frame the inquiry to the participant regarding preferences (Kung et al., 2016). I articulated my inquiry regarding preferences by identifying the conditions of the interview that I can control to help make it a comfortable and pleasant experience.

To help mitigate bias and support data saturation, I incorporated member checking and data triangulation. According to Morse (2015) and Harvey (2015), the use of member checking is a technique to obtain additional information and support to data saturation by offering each participant the opportunity to verify the researcher's interpretation of the collected data during the interview. In addition to member checking, I performed data triangulation using multiple sources of data such as the participant interviews and organizational documents to help achieve data saturation. Young et al. (2018) described the use of member checking as a valuable tool to increase researcher awareness and understanding of the participant's point of view, pursuit of data saturation, and to strengthen the researcher's rapport with the respective skill community associated

to the study. I conducted telephonic member checking interview(s) with each participant to allow for review and validation of my data analysis.

Ethical Research

Conducting interviews highlights the need to ensure ethical research practices. Lloyd and Hopkins (2015) identified the recruitment of, and access to, candidate participants in a research study as crucial elements for consideration in conducting ethical research. Qualitative research methods bring a different perspective to study where quantitative research may have previously dominated, for instance, the disembodied approach in quantification of information deemed sensitive by the participant (Lloyd & Hopkins, 2015). My research incorporated semi-structured interviews to collect qualitative data using open-ended questions seeking the knowledge and experience of participants who have volunteered their participation. As the researcher, I am responsible for data collection, serving as the collection instrument, and the steward for determining the application of research tradecraft to my study using the design and approach to research the stated problem. I collected and analyzed the relevant data like the interview log and transcripts, and organizational documents to create the study summary that documented corresponding themes.

Information does not exist in isolation and I sought to achieve a level of adequate participant transparency by ensuring informed consent. Elements that represent informed consent may vary by situation, and culture; however, there are common elements like authorization, process familiarization, and a clear description of choices as in being a volunteer with the right to withdraw at any time (Grady, 2015). To ensure

comprehensive communication with the participants, I provided each participant with an informed consent form, description of the study, and detailed information. The participants should be informed regarding how the data is protected, how the results are shared, and the general interview process (Grady, 2015). I provided a pre-interview orientation comprised of a review of the interview protocol, which oriented and familiarized the participant with the interview process to include options for withdrawal or pausing at any time. Each participant was provided a consent form, which articulated the right to withdraw at anytime during the study. If the participant decided to withdraw, all associated data for that participant was destroyed and the participant notified by email.

I informed the participants of the problem statement and purpose of the study to instill a sense of association and investment. No compensation was given as an incentive for participation. The relevance and inclusion in such a study served as the incentive to participate. Participating in research that is directly or indirectly linked to a person's professional and/or personal goals is a strong motivator (Lloyd & Hopkins, 2015). The knowledge and experience the participant gained from participating in this study is presented as the principal incentive, appealing to the chosen participant's sense of engagement and contribution to the IT skill community at large.

Participant's rights to privacy and confidentiality will be ensured by securing digital data using password protection and the use of physical security procedures to store hard copy documentation in a locked file cabinet (Saunders, Kitzinger, & Kitzinger, 2015). I explained how information security was used to protect participant information like password protecting each file and storing all hard copy material in a locked cabinet.

I explained how the audio was recorded during the interviews (if they approved to be recorded) and that no wireless or other communications technology was used to store and/or transmit data during the interview. In addition, I provided the participants an explanation of how a numeric label was used to protect their identity in place of their real name. The data was secured and is retained for five years. Prior to contacting candidate participants, and collecting data, I obtained approval from Walden's Institutional Review Board (IRB). The approval number issued by the IRB is 03-18-19-0630791.

Data Collection

This section identifies the data collection instrument, technique, and the organization of the collected data into information for data analysis.

Instruments

As the researcher, I am the principal data collection instrument in this study. The researcher is engaged in every facet of the study from design and implementation to its conclusion (Barnham, 2015). A semi-structured interview is often used for flexibility in identifying themes and to obtain an in-depth awareness and understanding of the study topic (Yeoh & Popovič, 2016). Morse (2015) described the application of reliability and validity to make the research rigorous. I used a semi-structured interview as the primary data collection instrument in my study. Data collection was comprised of sources to include semi-structured interviews and organizational documents using data collection instruments that include an interview protocol, interview guide, research notes, and the analysis results to help achieve reliability and validity.

By creating and following an interview protocol, I ensured a standard approach to the semi-structured interviews. An interview protocol should provide the necessary rules and procedures to govern the use of an interview (Castillo-Montoya, 2016). Establishing processes and procedures that are reproducible and flexible give power to supporting programs, for instance, like compliance and training to help mitigate insider threats (Mangelsdorf, 2017). Cyber threats have grown to keep pace with, or in advance of, modernization efforts toward the integration of information and communication integration with legacy technology, necessitating compliant protocols to govern processes and procedures to satisfy industrial uses (DiMase, Collier, Heffner, & Linkov, 2015). I used the same questions for each participant, researcher observation, and performed member checking as outlined in the interview protocol (Appendix A). Steps to codify the data to guarantee confidentiality of the participants was enforced by stepping through the interview process with the participant prior to the formal start. I ensured confidentiality of the participant's identity by removing all personally identifiable information from the research material. I used numeric labels for each participant to associate the respective participant with their data throughout the study. I evaluated and minimized all research data to maintain confidentiality by purging personal information when no longer needed for the study. I secured electronic data by encrypting and hard copy information was physically secured in a locked container along with the electronic storage device(s).

An interview guide should be created to help focus the interview process, which would contain at a minimum the interview script and open-ended questions for the interview process (Petocz & Newbery, 2016). I used an interview protocol (Appendix A)

as a working aid to conduct and guide the interview process, which included the interview script, questions, and participant criteria. Guest, Namey, Taylor, Eley, and McKenna (2017) referenced the use of an interview guide in each interview setting to create a standard practice for application in each interview. An interview provides the method to help reveal and capture individual experiences related to the research phenomena (Sorsa, Kiikkala, & Åstedt-Kurki, 2015). The interview protocol consists of the open-ended questions used for each interview along with associated secondary questions, as appropriate, to facilitate an interaction with the participants.

I used member checking in this study. Harvey (2015) described member checking as the process of presenting the results produced from the interview to each participant for their review and feedback, using that feedback to refine and finalize the results. The member checking technique is used to establish credibility (Morse, 2015). The review of the transcribed data and researcher's notes by the participant provides quality control of the content adding to the study's credibility (Perrotta, 2017). I used member checking by providing the transcribed data, notes (perceptions and interpretations), and other general interview findings to each participant during a follow up face-to-face or telephonic interview. To ensure member checking is value added as a validation technique and to contribute to data triangulation, I focused upon each participant's feedback and conducted additional interviews until no new data is collected. I maintained a member checking section for each interview, which documented any indicators and thoughts during the interview that held implications to member checking. In addition, the member checking section of the log contained the feedback from the

original interview I received from each participant. I provided an interview summary for each interview conducted for review and feedback. During the follow up interview used for member checking, I edited the interview summary to reflect the participant's feedback. I conducted a follow up interview with each participant after coordinating how the participant would like to proceed, for example, conducting a face-to-face or telephonic interview. The member checking section of the log contained the notes from the follow up interview. This approach continued for each participant until the interview did not produce new data.

Data Collection Technique

Two principal methods of data collection were used in my study, which are document analysis and interviews. My data collection technique is comprised of identifying organizational documents relevant to the study topic, review and analyze the documents, identify and access interview candidates, select participants and obtain consent, plan the interviews, conduct member-checking, and data triangulation. Conducting interviews is a data collection technique used in my qualitative research study. Applying the interview data collection technique to acquire effective data is crucial, and therefore, the sampling method must support the overall purpose of the study (Yazan, 2015). Prior to conducting data collection, and approaching interview candidates, I obtained IRB approval.

The review and analysis of organizational documents help gain a deeper awareness and understanding of cybersecurity strategy in critical infrastructure (Baxter et al., 2016). A wide range of documents, spanning credible sources, is necessary to acquire

a robust dataset consistent with data analysis and triangulation to include participant interview (Tas, Yetkiner, & Ince, 2017). I collaborated with the respective contacts for each participant organization to identify and access the relevant documentation such as policies, operating procedures, working aids, and strategies. I also asked interview participants for suggestions on documentation and coordinated with the contacts for each participant organization for access to the documents.

I compiled a list of potential sources of interview candidates (businesses, individuals) based upon the study's interview eligibility criteria. Identifying and gaining access to interview candidates is a crucial step to conducting an interview (Peticca-Harris et al., 2016). Prior to identifying and accessing the potential interview candidates there is a necessary step of identifying the key stakeholders and establishing a point of contact (gatekeeper) from among those to help facilitate, negotiate, and champion the interview process (Peticca-Harris et al., 2016). The gatekeeper is a trusted stakeholder, usually someone in management or a co-worker or peer, that assists the researcher in communicating with potential interview candidates, ensuring sustainable access over the course of the research, and help the researcher navigate associated challenges (Rimando et al., 2015). Once interview candidates were identified, I contacted the sources using email or telephone with the goal of identifying a gatekeeper to help facilitate and orchestrate the identification and access of interview candidates from selection through to conclusion.

I spoke with each participant to familiarize and orient the participant to the interview process. I then followed up with each participant by providing physical or

electronic copies (email is preferred) of the interview documentation to include the appropriate instructions in the interview protocol (Appendix A). Obtaining informed consent from the interview participants is often categorized as a simple task by researchers, while at the same time described as a key requirement and causing stress (Peticca-Harris et al., 2016). The use of an interview protocol provides a structure, which is important in mitigating the challenges related to planning for and acquiring informed consent (Wolf, Clayton, & Lawrenz, 2018). Written informed consent is a standard approach used to document the elements of consent such as voluntary action and confidentiality for the participant and researcher in accordance with U.S. federal regulations (Kim & Miller, 2015). Once a participant has consented to participate, I reiterated the voluntary nature of the study and the participant can withdraw at any time resulting in their interview data being destroyed to protect confidentiality.

I used the interview protocol to keep the discussion focused and to stay in the allotted time of 60-minutes for each interview. Planning is a crucial step in preparing to conduct interviews which ensures special accommodations and other logistical needs have been put into place to include date and time of the interview, and location (Brown & Danaher, 2017). Other key elements covered in interview planning are preparations for the selected method of recording/documenting the interview and the contact procedure leading up to the scheduled interview (Vinci, Rijo, de Azevedo Marques, & Alves, 2017). Preparing for, and conducting, an interview encompasses some advantages and disadvantages to include schedules, contact method, and creating a comfortable environment (Brown & Danaher, 2017). A common disadvantage of interviews is the

potential for researcher bias; however, the creation and application of an interview protocol provide a great advantage in limiting bias (Kallio et al., 2016) . Each interview provides the advantage of being a separate collection event of the participant's knowledge and experience (Young et al., 2018). I collaborated with the stakeholder/gatekeeper and participant to accommodate early identification of possible logistic challenges such as scheduling and the choice of location.

I carefully considered the case-by-case conditions for each interview to identify, coordinate, and plan the logistics of conducting the interviews. Choosing a neutral interview location with a favorable environment free from distraction is vital to establishing a setting conducive to data collection (Rimando et al., 2015). There are many considerations in choosing a viable location with each interview case, which may present unique factors related to the researcher, participant, and the goal/objective of the study, for example, the environment impacting data interpretation (Sutton & Austin, 2015). Another environmental example is to ensure the location is free from background noise to prevent negative implications in recording the interview (Vinci et al., 2017). In the initial interview coordination, I specifically identified the intent to seek consent to record the interview session as outlined in the interview protocol (Appendix A). I sought a separate consent acknowledgement for each participant interview event to ensure informed consent. Conditions when choosing a place to conduct the interviews included, but were not limited to, choosing a location, and/or communication technique, free from distraction, provided confidentiality but was conducive to conducting the interview.

I used member checking after each participant's interview. Member checking is also known as participant validation, which is used to explore data collected during the interview to help ascertain data credibility (Birt, Scott, Cavers, Campbell, & Walter, 2016). Providing the data collected during the interview to the participant post-interview is a recognized technique to validate the analysis and interpretation in the findings (Harvey, 2015). Member checking is a valuable source of new data for use in enriching and refining the finding post-interview (Simpson & Quigley, 2016). I transcribed and analyzed the interview recording and field notes. A follow up meeting with the participant was scheduled to present and discuss my preliminary interview findings using an appropriate contact method with face-to-face (physical or video call) being preferred, and the use of email if the participant's circumstances required an alternate method. The member checking process continued until the participant and I concluded the data was accurately interpreted and represented. These member checking sessions become a part of the body of knowledge for the study.

Data Organization Techniques

Data organization is crucial to ensuring the collected data and analytic findings are properly accounted for and represented throughout the research process (Ranney et al., 2015). Characterizing the data from primary sources, interviews and document analysis, and secondary sources to include reflective journals is a key factor in data organization to help process efficiency such as preventing duplication of data, findings, and tasks (Vaismoradi, Jones, Turunen, & Snelgrove, 2016). Coding and grouping of data is enabled through data organization, in turn, allowing the researcher to identify and

describe the themes revealed (Sloan & Bowe, 2015). Maintaining a research log and reflective journal are two popular approaches to organizing research data, each providing the researcher an opportunity to reflect back on the research and how the data organization techniques are progressing while being applied (Peticca-Harris et al., 2016). Journals and logs capture the researcher's thoughts, insights, and experiences throughout the study as well as providing a resource to reflect back on concerns identified during research activities (Orange, 2016). Maintaining a habit of note taking, journals and logs, in all study activities is a vital resource like following up on an idea or connecting two otherwise non-related topics revealing a new theme (Vicary, Young, & Hicks, 2016). I followed a data organization technique to ensure succinct data organization throughout the study's lifecycle. I organized the collected data through the use of coding and grouping of the data from all sources. I created and maintained a log for each participant to document my thoughts and ideas to help identify follow on questions or points to clarify. I used a reflective journal to document my activities during the interview process as an additional source of data for reflection on the process and the interview experiences.

I created and maintained a file system to ensure each participant and unique topic area has separate storage. I grouped the research material by section and sub-sections, for example, section 3 of the study was organized to ensure the themes revealed in the course of the research are documented and maintained for separation. Each participant was assigned a non-descriptive label for use in file and folder naming convention to link all relevant data to the participant, while protecting the participant's identity. I took notes in

my study to assist in documenting activities that may not appear to be relevant. I used those notes to help me reflect upon the study activities and to assist in the investigation of issues and potential research leads. I used an appropriate heading for each entry within the journal to ensure the notes are organized by participant, activity, and topic. I utilized qualitative data analysis software to help organize the data by linking the concepts and topics identified during analysis to the information source like my interview notes and organizational documents. Electronic data was encrypted and saved on an appropriate storage device and secured in a locked file cabinet along with any hardcopy material. I planned to retain the data for 5-years from the study's publication date and have planned to wipe the electronic data, and destroy the hardcopy material using the appropriate methods.

Data Analysis Technique

The qualitative data in this study was collected in textual form, and therefore, based on the work by Bengtsson (2016) a quantitative method like statistical analysis is not used to give meaning to the data. Textual data is raw and must be transformed into information and data analysis provides the technique to identify and explore the information to reveal patterns that are interpreted and documented as themes (Hussein, 2015). Thematic analysis presents a technique to explore, filter, and synthesize qualitative data in the form of descriptive themes (Chowdhury, 2015). Using a coding process can help organize information to form themes and readily provide the source reference for the information that led to the formation of each theme (Sutton & Austin, 2015). My data analysis approach was used to identify patterns in the raw data collected

through semi-structured interviews and organization documents. The patterns represent essential elements of information to help identify and describe themes related to cybersecurity in critical infrastructure to help answer the research question.

Fusch and Ness (2015) described triangulation as the exploration of a phenomenon from different viewpoints and at varying depths, and provided a summary of four types of triangulation; (1) data triangulation is applied to people, time, and space, (2) investigator triangulation is applied to multiple result sets from multiple researchers in a study, (3) theory triangulation is applied to multiple theoretical strategies, and (4) methodological triangulation is applied to data collected by two or more collection methods. Hussein (2015) added a fifth type of triangulation, which is analysis triangulation describing it as a validation technique when qualitative and quantitative data are collected. Triangulation is used to further refine the information created through data analysis with the goal of a greater awareness and understanding of the phenomenon to reveal themes (Chowdhury, 2015). I chose the within-method of triangulation to explore and analyze data collected from semi-structured interviews and organizational documents.

Methodological triangulation requires two or more data sources, and results in a more in-depth exploration and understanding of a phenomenon when the phenomenon is viewed through at least two perspectives (Joslin & Müller, 2016). Within-method of triangulation is used to enrich the data providing an approach to mitigating bias, strengthen the reliability of the results, and enhance data saturation (Fusch, Fusch, & Ness, 2018). In my study, the two main perspectives were semi-structured interviews and

organizational documents used as data collection sources and the application of a data analysis process that included coding to reveal key themes.

To ensure robust and dynamic coding, I first reviewed the data to gain the necessary level of familiarization and generate codes to reflect the research question, and group the codes by topic to guide and promote data organization. I used field notes to document ideas and concepts during data analysis to include the coding process and also applied coding against the field notes as a complimentary data source. The coding was applied against the collected data as often as necessary to explore and identify patterns and associations in the data. Qualitative data analysis software was used to facilitate data coding and organization.

I chose to use the Atlas.ti qualitative data analysis (QDA) software in my study to support data analysis and reporting the findings. QDA provides the researcher a method to achieve a greater breadth and depth of awareness and understanding of the data resulting in rich and descriptive findings (Chowdhury, 2015). There are several popular QDA software products to include nVivo, HyberResearch, N6, MAXqda, Atlas.ti, and Qualrus. A popular choice of QDA software is Atlas.ti with its robust functionality like coding options including open or Vivo, code-recode, merging strategies, categorization, and cross-checking (Paulus, Woods, Atkins, & Macklin, 2017). According to Harrell (2017), QDA software Atlas.ti is used to code, categorize, store, and analyze the research data to support the identification of patterns and associations in the data. Paulus et al. (2017) stated the use of Atlas.ti codes and memo functions enriched and enhanced the study findings through the addition of researcher interpretation and reflection. My

research data was filtered into phrases and sentences to help form codes that described the data. I used Atlas.ti QDA software to perform thematic analysis with keyword queries to group the data into categories based upon the coding to identify patterns in the data. I applied data analysis to identify patterns in the data associated with the research question relevant to strategic factors for successful cybersecurity in critical infrastructure to support the formation of themes. The data included relevant sources such as semi-structured interviews, field notes, and organizational documents. New data revealed during data analysis was added to the study, as appropriate.

Reliability and Validity

Credibility, transferability, dependability and confirmability are the criteria described in qualitative literature to evaluate the reliability and validity of research implementation, evaluation, and value (Morse, 2015). Reliability is the evaluation of whether a study's processes and findings are reproducible (Leung, 2015). For data dependability and confirmability, I used auditing and adherence to the interview protocol (Appendix A). Dependability was supported by thorough documentation of procedures like field notes, coding, and change logs. Confirmability comes into play by acknowledging and describing research biases and assumptions, which were declared in the research process. I used member checking and triangulation to ensure corroboration of the findings. I documented the protocols to enable auditing, for example, the use of an interview protocol that included guidance for member checking. Validity is focused upon the credibility of the study's findings by evaluating the appropriateness of the tools, techniques, and methodology (Palinkas et al., 2015). Credibility and transferability are

supported through data analysis, member checking, triangulation, and the detailed tradecraft documentation in the use of tools, techniques, and methodologies (Morse, 2015). I provided sufficient details for processes and procedures used in my study.

Dependability

Establishing the trustworthiness, or rigor, of the research includes the criteria of dependability, which is to ensure the findings can be repeated (Amankwaa, 2016). Amankwaa (2016) identified the technique of using inquiry audits performed by one or more researchers not engaged in the target research to assess the research process and deliverable to determine if the study findings are supported by the data. Bengtsson (2016) suggested that each procedure used in the study be defined in enough detail to ensure transparency and repeatability. The collected data, and analytic findings, must prove resilient under changing relationships like time and circumstances (Mandal, 2018). Mandal (2018) referred to facilitating an audit through the adequate documentation and description of processes to include data collection and data analysis. To ensure the dependability of my study, I described the study design and methods, documented the relevant processes and procedures, ensured the study participants were comprised of IT and compliance professionals based upon the study's eligibility criteria, and leveraged my study committee overseeing the research design to ensure adherence to the doctoral study governance and guidelines. Following the above steps, I provided the necessary level of detail for my research to be repeated.

Credibility

Credibility is a type of validity, for example, when the participants provide feedback on the accuracy of the findings in relation to the study's context (Allred, Maxwell, & Skrla, 2017). Credibility is a key factor to achieve validity and the use of triangulation provides the researcher an approach to address bias while enriching the data (Fusch & Ness, 2015). The use of triangulation is a method that may increase credibility by gaining a broader and deeper understanding of the phenomenon, as well as identifying convergence of themes across multiple data sources (Hussein, 2015). I used member checking and triangulation of multiple sources of data such as researcher notes, organizational documents and semi-structured interviews to strengthen the study's credibility. Triangulation is key to achieving data saturation through the correlation of data collected from multiple sources. I used the same set of questions for each participant's interview to identify common themes and I conducted member checking with each participant until no new data emerges.

Transferability

Allred et al. (2017) described transferability as the general comparison of research findings to similar studies to determine possible commonality. In qualitative research, to avoid the generalization of the findings, the concept of transferability is left to the reader and future researcher (Fusch, Fusch, and Ness, 2018). The researcher should provide an accurate description of the research methods used in the study to support the concept of transferability and to provide the reader the necessary information to make an informed decision (Sidhu, Jones, & Stevenson, 2017). I provided succinct details of the research

methods and the findings. I provided research design and process descriptions that provide informed awareness and understanding to help determine the transferability of my study. For example, the use of triangulation and member checking to support data saturation and by providing descriptions of processes that were used to include data collection, data analysis, and the use of an interview protocol for the semi-structured interviews.

Confirmability

Confirmability is measured by the extent the study findings represent the participant's input and feedback to the study (Amankwaa, 2016). Assessing qualitative research is crucial and ensuring objectivity is reflected in whether the research could be pursued by another researcher with equal or similar results, which in turn supports trustworthiness and rigour (El Hussein, Jakubec, & Osuji, 2015). The researcher should reveal any influences such as a particular bias to support the concept of confirmability (Brown, Elliott, Leatherdale, & Robertson-Wilson , 2015). I revealed influences such as biases that may hold implications to the research findings. I documented my research to an adequate level of detail to allow another researcher to pursue. Peticca-Harris et al. (2016) emphasized the use of a research log and reflective journal to facilitate data organization and to allow the researcher an opportunity to identify patterns and themes in the data. I memorialized the research information through the use of note taking and a journal.

Transition and Summary

In this section, I presented the tools, techniques, and methodologies planned for use in my study. I chose to use a qualitative multiple case study to accomplish the stated research purpose. The section outlined details on the role of the researcher, participants, research method and design, population and sampling, ethical research, data collection instruments and technique, data organization technique, data analysis, reliability and validity. The next section includes the presentation of findings, implication to professional practice, and implication for social change, recommendations for action and further research, and my reflections.

Section 3: Application to Professional Practice and Implications for Change

This section of the study contains an overview and a presentation of the findings, which describe the main themes resulting from the data analysis. In addition, this section includes applications to professional practice, implications for social change, recommendations for action and further study, reflections, and the summary and study conclusions.

Overview of Study

The purpose of this qualitative multiple case study was to explore cybersecurity strategies used by IT managers and compliance officers to mitigate cyber threats to critical infrastructure. I collected the research data from semistructured interviews, publically available case organization documents, field notes, and reflective journal. I collected 25 publically available documents for analysis and conducted the semistructured interviews with two IT and three compliance participants across four case organizations located in the Pacific Northwest region of the United States.

Four major themes were revealed as a result of this qualitative case study: (a) a robust workforce training program is crucial, (b) make infrastructure resiliency a priority, (c) importance of security awareness, and (d) importance of organizational leadership support and investment. The major themes are consistent with the trends revealed in the literature review and the results from the study support my use of the RAT as the conceptual framework. The four major themes are described and explored in the next section.

Presentation of the Findings

The study's RQ was: What IT cybersecurity strategies are used by IT managers and compliance officers to mitigate cyber threats to critical infrastructure? This section includes a description and exploration of each of the four major themes revealed from this study. I used the within-method for data triangulation to explore and analyze data collected from semistructured interviews and organizational documents related to cybersecurity in the case organizations. The participant transcripts and relevant documents were entered into the Atlas.ti analysis tool resulting in the identification of the four major themes. According to Harrell (2017) and Paulus et al. (2017), qualitative data analysis software like Atlas.ti is used to support the identification of patterns, or themes, and associations in the data, and the software's functionality helps to enrich and enhance the study findings through the addition of researcher interpretation and reflection. The four major themes revealed during the data analysis are linked back to the study's conceptual framework and literature review.

The study participants were IT managers and compliance officers with experience in implementing or managing cybersecurity programs to mitigate cyber threats to critical infrastructure. Each participant had over 10 years of experience as an IT or compliance professional. There were four case organizations representing the critical infrastructure sectors of transportation, healthcare, oil and gas exploration and production, and electric services. The five participants were all experienced in planning and implementation of cybersecurity and compliance programs for organizational strategies in critical infrastructure.

The within-method of triangulation was achieved with two main perspectives of semistructured interviews and organizational documents used as data collection sources and the application of a data analysis process that included coding to reveal key themes. Documents collected included published meeting minutes, guidance, process, procedure, and policies pertaining to organizational functions and support of the respective strategic goals. The first three documents focused on establishing a partnership through information sharing and preparation of organizations in the Pacific Northwest operating in the area of critical infrastructure. Common goals included a collaborative alliance and an understanding of relevant response frameworks to ensure standardization of an informed decision making process and experienced workforce through real-world virtual exercises and training scenarios. The next set of 11 documents focused upon information protection and security with emphasis placed on release of data to external entities, protection of personal data, guidance for compliance with applicable legislature, physical security considerations, and electronic communications. These documents established a core cybersecurity guidance with flexibility to adapt based upon local circumstances without compromising the programs key criteria. For example, workforce cybersecurity training was comprised of specific modules to ensure standardization of the training effect, but it allowed for local leadership to add modules for unique requirements. A single document was received from a case organization that outlined the layered defense of their production environments. This document articulated the concept and implementation in production that spanned three principal service domains. The document also represented where and how cybersecurity, and IT overall, were

incorporated in the organization's strategic plan. Emphasis was placed throughout the document on roles and responsibilities including the need for robust training to establish and sustain the required results. The next batch of seven documents included regional and organizational level guidance for cybersecurity in critical infrastructure along with two annual organizational annual reports and a 2019 worldwide U.S. intelligence threat assessment used to ground the other documentation for risk perception and context. This cache of documents highlighted the focus on cybersecurity amid the increase in sophisticated cyber threats from nation-state actors and other miscellaneous groups. Emphasis was placed upon standardized cybersecurity guidelines that were reinforced and practices on a regular basis to ensure holistic cross-security program synchronization like cybersecurity and physical security. Cybersecurity guidelines for neighboring states and territories were included to represent a comprehensive approach to collaboration in the region such as overlapping training exercises. The final set of three documents condified a broad overlap in cooperation for cybersecurity in critical infrastructure among respective service providers. A purposeful sharing of lessons learned, guidelines, and threat knowledge enabled a higher level of threat awareness, which in today's cybersecurity threat landscape is critical to preventing strategic surprise.

Each of the four major themes identified from analysis of the collected data are described and explored in the following sections and are connected back to the conceptual framework and literature.

Theme 1: A Robust Workforce Training Program is Crucial

The first theme resulting from the data analysis phase was the need for a robust workforce training program. All participant interviews and most of the 25 documents collected revealed the training program as a crucial strategic factor in the success of the respective cybersecurity and compliance programs. All five participants mentioned the challenges introduced by what they described as the typical cybersecurity training program, which use a slide presentation as a "snapshot in time." That approach often resulted in stagnant content that did not provide the needed training effect to achieve the required knowledge, apply that knowledge, and sustain the practical skills in the workforce.

Analysis of the participant input and the case documentation identified a common definition of cybersecurity in critical infrastructure, which is the protection of key IT resources that, if compromised, may result in the degradation or loss of services such as oil and gas distribution, healthcare, and electric and water utilities. All of the participants, supported by the respective case documentation, emphasized the need for the workforce to be adequately trained to perform the day-to-day functions to deliver reliable services. According to He and Zhang (2019), a successful cybersecurity training program should be adaptive and interactive such as incorporating on-the-job training. Nine key best practices for a successful training program were identified by He and Zhang (2019), which included accountability, fun, hands-on, interactivity, just-in-time training, personalization, reinforcement, relevancy, and reward.

Four common factors related to training were identified in the participant interviews and documentation. Information contained in Table 3 represents the distribution of the four factors in the participant interviews and study documents. The data in Table 3 represents the number of participant interviews and/or documentation where one or more of the factors were identified; the numbers do not represent a total count of how many times a specific term was used in the data sources.

Table 3

Distribution of Theme 1

Data sources	Relevant & flexible	Hands-on	Communicate	Effective
Participants	5	5	5	5
Documentation	16	12	10	15

The participants were consistent in their messaging that purposeful updates through robust training is crucial to the cybersecurity program as a key element in the organizational strategy to remain relevant in staying out in front of the advancements in technologies, including the associated cybersecurity tradecraft in critical infrastructure. The convergence of legacy technologies with modern IT capabilities, according to Participant #1, has "revealed unforeseen cybersecurity threats in critical infrastructure that span software, hardware, and network resources." This supports Shoemaker, Davidson, and Conklin (2017) who found that the cyber threat landscape is an enduring challenge for the IT profession. Participants #2 and #3 reported that workforce compliance with cybersecurity policy has improved with a decrease in cybersecurity

incidents across their organizations. Viewing employee performance as a return on investment for the training program has revealed an association with the quality of the training program and the necessary level of awareness and understanding (Lošonczi et al., 2016). Participant #4 highlighted the importance of an organization's investment in training to help increase workforce performance and overall organizational compliance. Compliance and training programs have become crucial strategic factors to the success of an organization's cybersecurity strategy (Adams & Makramalla, 2015; Pham et al., 2017). Participant #3 emphasized the need for training that advances with the threat to ensure proactive workforce skill readiness and the ability to quickly adapt. Adopting a broad set of general cybersecurity best practices was found by Shackelford et al. (2017) not to be the single answer in today's cyber threat landscape, which remains fluid and continues to evolve. Participant #4 and #5 identified a robust workforce training program as a necessary investment to best prepare for encountering threat tradecraft comprising advanced tools, techniques, and methodologies. The training program must adapt to the threat landscape by preparing the workforce with the knowledge and experience needed to incorporate risk perception and instill a culture of compliance such as self-reported behavior (Li et al., 2019).

Relevant and flexible. All participants mentioned the importance of relevance and flexibility in a training program. Relevance and flexibility was highlighted by the participants as key factors for a program to quickly tailor its training effect to satisfy on-demand and custom training requirements, as well as adapt to individual needs and fluid challenges. Participants spoke of the need for a flexible training model to quickly adapt

to the training needs to include knowledge of cybersecurity principals that are reinforced through hands-on learning. Flexible training models were supported by Li et al. (2019) who found that cyber attacks have evolved in their sophistication, which has increased cybersecurity risk requiring the same advances in workforce skills and awareness just to keep pace. When asked "What have you found to be most effective in cybersecurity, compliance, or training strategies?" participant #1 stated, "Training, training, training". Participant #1 went on to identify the cybersecurity training program as a key element in the organization's strategy to establish and sustain an employee's awareness and understanding of how their actions may have consequences. Participants #2 and #4 codified this theme with emphasis placed upon a high probability of experiencing second and third order of effects following the initial consequences, even if the cybersecurity incident appeared minor. Participants #1, #2, and #4 revealed the employee often believed their action would have been different if they were better informed. Educating the workforce in the organization's cybersecurity policy was supported by He and Zhang (2019) who found that positive changes in workforce behavior to support and comply with cybersecurity policy. Each of these participants highlighted the need for employees to gain relevant knowledge and understanding of how their actions may contribute to, or enable, malicious action. Participant #2 identified the strategic importance of cybersecurity training in making informed decisions and the organization's ability to sustain critical infrastructure through, "The employee's awareness and understanding of how to apply the respective IT technical knowledge to their day-to-day functions". The importance of a robust cybersecurity training program was represented by Participant #4

as the increase in sophisticated malicious software capabilities and social engineering efforts direted against the technology and human factors that comprise critical infrastructure operations. Participant #4 identified a deliberate approach that enables the organization's ability to implement a robust cybersecurity training program, "We hire people that are passionate about IT and bring a diverse set of experience (e.g. young college kids who wear t-shirts with their favorite video games to retirees from government agencies). Our workforce keeps us on our toes."

Participants described personal experiences with their respective cybersecurity training programs. Participant #3 emphasized the need for organizational leadership support to provide the necessary level of investment in cybersecurity training resources and to achieve the necessary level of organizational accountability. The level of commitment by the organization's leadership was found by Paliszkiewicz (2019) to be a key factor in an employee's attitude and behavior toward cybersecurity compliance. Implementation was identified as a crucial element that must benefit from fluid planning and preparation. Participant #3 went on to state, "A lesson learned is in implementation, which resulted in providing regional leadership teams with the flexibility to tailor local [training to include cybersecurity] programs in the guidance of the organizational strategy." Maintaining relevancy in the training while personalizing it to cover an employee's preferred learning style was emphasized throughout the data. Participant #5 said, " Most cybersecurity tools are reliant on what is known, such as signatures or definitions used in end-point solutions and firewall intrusion detection systems." The knowledge of a particular technique or method combined with the use of relevant tools is

only a piece to the puzzle. This point was reported by participant #5 as, "User training is one of the most important tools at a company's disposal. The user must be able to identify and report, and they only do this with good training programs." A relevant and flexible training program is the employee's resource to gain the necessary level of awareness and understanding to prosecute their daily functions in the context of cybersecurity implications, and in a broader context the organization's ability to sustain a compliant business model and operational environment.

These factors are supported by the study findings and current literature. He and Zhang (2019) identified relevance, flexibility, and format as major challenges in creating and implementing a successful cybersecurity training program. Coffey, Haveard, and Golding (2018) introduced a concept to remain relevant and flexible a cybersecurity program should focus upon the human sources of vulnerability as well as the technological to ensure holistic security. Elkhannoubi and Belaissaoui (2016), Borum et al. (2015), and Jacobs, von Solms, and Grobler (2016) discussed the nature of critical infrastructure as the convergence of legacy and modern IT resulting in complex architectures and systems within systems, often introducing unforeseen vulnerabilities. A new creative approach to cybersecurity training that embodies the factors of relevance and flexibility was introduced by Seo, Bruner, Payne, Gober, and Chakravorty (2019) leveraging advancements in augmented and virtual reality technologies. The findings support relevancy and flexibility as key factors in a robust workforce training program to keep pace with the dynamic cyber threat landscape and a fluid workforce associated with the protection of critical infrastructure.

Hands-on. The common thread of hands-on learning was prevalent throughout all interviews and further supported in the documentation (Table 3) such as the need for a standardized workforce knowledge baseline along with experience in applying that knowledge in day-to-day functions. Adams and Makramalla (2015) identified limited cybersecurity skills training as a main contributing element to the existence of the human vulnerability challenge in cybersecurity. The study findings are consistent with the interviews, documentation, and literature in identifying a common challenge in today's legacy approach to cybersecurity training. A non-traditional approach is required such as immersive and to break the traditional cycle of using classroom lecture and online advice to teach cybersecurity knowledge (Adams & Makramalla, 2015). Labaka, Hernantes, and Sarriegi (2016) stated the application of cybersecurity as a function in the IT discipline is an enduring strategic challenge, and specifically in the protection of critical infrastructure. A new area of research was introduced, Critical Information Infrastructure Protection, to highlight the influence of modern IT in critical infrastructure to the point of increased unpredictability and unforeseen implications to the infrastructure's hardware, software, networking, and data storage (Alcaraz & Zeadally, 2015; Bou-Harb et al., 2017). Participant #3 identified IoT as an emerging technology, which has "introduced a new threat vector demanding heightened cybersecurity tradecraft and a deeper awareness and knowledge of how technology interacts and communicates." All the participants were consistent in their identification of how the convergence of legacy operational technologies and modern information technologies has elevated the need of immersive

hands-on workforce training as a must have for organizations to ensure strategic success in cybersecurity and compliance programs.

Traditional workforce training often approaches a training event such as a small team exercise or new employee orientation using one of the common learning styles, which include visual, auditory, read/write, and kinesthetic (Cuevas & Dawson, 2018). Participant #2 emphasized reliance upon only one learning style as the majority style for a given training event resulted in the need to provide additional remedial training. The key ingredient that was lacking from the traditional training, according to participant #3, was in hands-on application while keeping the training fun and relevant. Providing an explaination of the cause and effect of the employee action is necessary to better understand the consequences of the action, or lack of action (Cuevas & Dawson, 2018). Participants #1 and #2 identified challenges where the workforce often approached their duties with a perception of low risk, with probable association to their lack of understanding between their duties and cybersecurity procedures. This challenge frequently had a secondary impact of late identification and reporting of indications of malicious activity, as well as the incident reporting. Participant #4 was strongly supportive of applied experience that was reinforced with regular theory and hands-on based training approach. The use of frequent real-world scenario based exercises is not as common as anticipated in a field like critical infrastructure; therefore, it is necessary to use immersive hands-on training events to prepare the workforce (McQuaid, Britton, Minnich, Borrelli, Baker, & Burton, 2019). The study findings are consistent in the

identification and use of hands-on training to strengthen the workforce's understanding and expertise in cybersecurity tradecraft.

Communicate. Communication was identified in the study findings as a common factor necessary for a robust workforce training program. In the context of knowing the intended training target (students), the training must be communicated in a style the students can effectively consume and apply the information to prepare for time-sensitive real-world events. This research supports Brilingaitė, Bukauskas, and Juozapavišius (2019) who found cybersecurity teams comprised of multiple disciplines, introduces the potential for communication challenges involving a broad range of diverse competencies engaged in working a cybersecurity situation. In their work, cybersecurity practitioners must communicate technical information across a given organization's leadership, management, support, and STEM workforces at the level of complexity necessary to effectively communicate the details to enable informed decision making. The participants identified the need for an instructor to have sufficient communication skill to communicate with students of varying levels of knowledge and understanding such as in the fields of cybersecurity, IT, and policy/governance. Four of the five participants emphasized the instructor must be skilled to translate and interleave the respective lexicons for proper interpretation and represent that information in a manner easily understandable, along with clear and concise course material.

Participants #2 and #3 reported they achieved increased workforce and vendor cybersecurity buy-in resulting in less compliance incidents by simply communicating the why and how related to security policies and guidance. This supports Yoon et al. (2016)

who found that cybersecurity skills are not standardized often introducing challenges for training programs to address the common occurrence of disparate training experiences by cybersecurity practitioners in critical infrastructure. Yoon et al. (2016) revealed a reliance on traditional training materials by critical infrastructure providers, including exam based certifications, to provide the required level of expertise adding to the challenges of protecting critical infrastructure. Participants identified communication skills as a key factor in a robust workforce training program to help fill gaps in the content by communicating cybersecurity in real-world context to a workforce comprised of multiple skill levels and disciplines.

Participants #3 and #4 emphasized the increased challenges with critical infrastructure due to the integration of legacy and modern technologies that demand a creative workforce training program in response. Cybersecurity challenges continue to surface more frequently based upon media coverage, which reveals an increase in unforeseen and unpredicted vulnerabilities in the software, hardware, network, and storage components that form the infrastructure. McLaughlin et al. (2016) related the challenges in the combination of cyber and physical components with an emphasis on communication between a diverse range of disciplines. According to Li et al. (2017), communication between workforce teams and with external teams is crucial to achieving the necessary level of awareness to ensure efficient and effective collaboration. Multiple skillsets are needed to manage, support, and maintain the diverse infrastructure components, each of those represent unique considerations with widespread implications to cybersecurity. Participants stated the importance of advancing cybersecurity

workforce training to meet a fluid and sophisticated cyber threat landscape with internal and external communication acting as a pivotal element.

Effective. This factor was described by the participants in the context that to simply fill a box on a checklist included in an appendix to the organization's strategic plan does not meet the intent. This supports other researchers. To be effective the training must prepare the workforce to visualize and recognize what normal activity looks like, and respond accordingly (Harp & Gregory-Brown, 2015). Today's critical infrastructure incorporates diverse technologies spanning basic to complex implementations of operations and IT components (Alcaraz & Zeadally, 2015). The participants also stated that boredom and insufficient training delivery formats often do not meet the many individual learning styles present in the workforce. In those scenarios, the desired training effect is not achieved, which according to the participants is a principal challenge for their organizations. Participants #2, #3, and #5 outlined their challenges related to the workforce's lack of understanding of consequences resulting from their actions, personal and professional. Pursuing this line of inquiry with the participants resulted in the association of their challenges with a lack of effective workforce training.

Four factors identified by the participants, were included in the organizational documents and covered in existing literature to comprise the support for the first theme. Across the 25 organizational documents, 53 instances related to Theme 1 were identified. The documentation revealed training as a key factor to the respective organizational strategy. Within the documentation, organizations recognized the need to establish

proactive measures to meet the modern cyber threats that change at the speed of technology. Three documents identified the expansion of training to provide enhanced analytics and pre-incident preparedness to improve response and recovery. Internal exercises were identified in 12 documents to provide hands-on skill application. Enhanced delivery methods were included in 17 documents to help improve the effectiveness and flexibility of the training to adapt to the workforce learning needs. Ten organization documents contained an approach using supplemental and transition certifications to increase relevant professional development training that would codify critical functions requiring special skills and knowledge. Eight documents identified strategic communications to promote the cybersecurity guidance and policy using short, concise messaging to ensure standardization for consistent interpretation across the workforce.

The conceptual theory chosen for this study was RAT, which considers three main criteria that are offender, target, and prevention (guardianship). Protecting key assets identified within critical infrastructure relies upon general IT expertise and more specifically in cybersecurity tradecraft. Participants, organizational documents, and current literature indicate the increased occurrence and sophistication of cyber attacks against critical infrastructure is a significant threat. Key assets within critical infrastructure have been clearly targeted in previous cyber attacks, acknowledging the existence of a motivated and capable offender. Cybersecurity in critical infrastructure depends upon robust workforce training according to the participants, documentation, and literature. The chosen conceptual theory, RAT, is well established in analyzing criminal

behavior applying the prior findings related to virtual and terrestrial environments to include on-line and off-line pattern and behavioral characterization (Leukfeldt & Yar, 2016; Reyns & Henson, 2016). Findings from this study, guided by the RAT, indicate a persistent and highly skilled offender focused upon a target, critical infrastructure. With malware and computer focused criminal activity on the rise in a virtualized target environment, the workforce training program must establish and sustain the workforce to meet the challenge, 24/7. The results of this study revealed that a robust workforce training program is a crucial factor to the success of cybersecurity in critical infrastructure within an organizational strategy.

Theme 2: Make Infrastructure Resiliency a Priority

The second theme resulting from the data analysis phase was the need to make infrastructure resiliency a priority. Analysis of the participant interviews and organizational documentation revealed the goal of achieving cybersecurity infrastructure resiliency as a priority in the organizational strategy. The resource investment to react to the threats far outweighed the return on investment according to participants #2, #3, #4, and #5. Planning a cybersecurity program to incorporate industry best practices while enabling infrastructure resiliency was mentioned by participants #1 and #3 as allowing the organization to balance its defense through preparation and readiness.

All of the participants expressed a need to include infrastructure resiliency as an objective in the organization's cybersecurity program and also noted that incorporating infrastructure resiliency into the cybersecurity program becomes a priority with a sense of urgency if the cybersecurity program relies upon vulnerability based protection measures

alone. The sense of urgency for considering infrastructure resiliency is due to the presence of a sophisticated and persistent cyber threat landscape that continues to remain out in front of conventional cybersecurity protection in critical infrastructure (Pursiainen, 2017). Participants #3 and #4 reported the convergence of IT and legacy OT presents unique challenges that are often outside the ability of vulnerability based measures to protect the respective critical infrastructure environments. Participant #3 reported the use of conventional cybersecurity fundamentals alone resulted in an expenditure of more resources than the anticipated return on investment..

Four common factors related to infrastructure resilience were identified in the participant interviews and documentation. Information contained in Table 4 represents the distribution of the four factors in the participant interviews and study documents. The data in Table 4 represents where one or more of the factors were identified and the numbers do not represent a total count of how many times a specific term was used in the data sources.

Table 4

Distribution of Theme 2

Data sources	Continuity	Assurance	Preparedness	Response
Participants	5	5	5	5
Documentation	8	11	15	14

A principal challenge to cybersecurity in critical infrastructure is the convergence of IT and OT, which often results in unpredicted vulnerabilities that are out of scope of

the existing cybersecurity defensive and preventive measures. IT modernization in support of critical infrastructure has advanced the respective disciplines like software, which has taken on a primary role in the improvement in industrial system performance, as well as the formation of systemic dependencies and interdependencies (Cassotta & Sidortsov, 2019). Critical infrastructure reflects the integration of physical sensors with modern IT forming unique constructs such as system of systems, software as a service, and embedded computing resulting in an order of magnitude increase in cybersecurity risk (Piggin, 2018). With a fluid cyber threat landscape targeting critical infrastructure, attributed in part by the convergence of IT and OT, organizational resiliency as stated by participant #2, "Must be a deliberate strategic priority with the pursuit of technical vulnerabilities overshadowing the goal to provide timely critical services to the community." Participant #5 reported that an increase in Internet and specialized network connectivity represents an increase in the potential for vulnerability relevant to physical sensors, industrial control systems, and other OT such as the IoT.

Participant #1 associated the challenges in skilled workforce availability and capacity to respond to cybersecurity incidents with the unforeseen challenge to convincing leadership that infrastructure resiliency may be a plausible approach to minimize dependency upon conventional vulnerability protection. Fragmented cyber policies and the continued integration of modern IT in critical infrastructure were found by Cassotta and Sidortsov (2019) to increase the possibility of new cyber vulnerabilities, which supported the concept of infrastructure resiliency. Participants #1, #2, #4, and #5 explained resiliency as a necessity to ensure critical services are neither degraded, nor

lost which would be catastrophic to the affected population. The growing integration of the IoT demands a cybersecurity pivot, which participant #3 emphasized as moving away from conventional cybersecurity strategy to infrastructure resiliency. Fifteen documents contained guidance for infrastructure resilience and continuity of operations. Several specific concepts were identified in documentation to support resiliency like continuity of operations with off-site data archiving and the identification of primary and secondary locations for cybersecurity functions. Functions mentioned in the documentation were system and network monitoring, and auditing, for quality control in preparedness and response. Data triangulation of the participant interviews with the collected documents codified the infrastructure resiliency theme.

Continuity. Continuity of the key assets was deemed crucial by all participants and supported in the documentation. This factor represents time-sensitive and stable services provided by key assets during normal and crisis situations with implications to the continuity of services by malicious cyber attacks as a priority concern. To achieve continuity of services in support of infrastructure resiliency the traditional approach to cybersecurity in critical infrastructure must change from a defensive to a proactive approach with knowledge of the cyber threat landscape (Ferdinand, 2015; Pursiainen, 2017). Replacing the status quo is essential to evolving a cybersecurity program to properly defend and protect critical infrastructure key assets (Robert, Morabito, Cloutier, & Hémond, 2015). All participants, and 8 documents, mentioned continuity as a key factor in the pursuit of infrastructure resiliency. Continuity of operational services was emphasized by participants #1, #2, #3, and #5 for key assets that comprise critical

infrastructure. This was supported by approaches in the documentation with back up data respositories that would include data to support cybersecurity functions spanning pre-incident preparedness, analysis, response, and recovery (Table 4). Participants #4 and #5 emphasized the importance of cybersecurity continuity as key assets are transitioned to sustain critical infrastructure operations in geographically separate locations. Approaches in the documentation supported the challenge of geographic diversity through the use of secondary and tertiary cybersecurity points of presense, for example, by leveraging cloud service providers.

Assurance. According to the participants and documents, assurance was identified as a key factor in its application to the underlying IT and OT. Participants #1, #2, and #3 emphasized assurance as a principal concept that is applied to all capabilities in critical infrastructure due to their interoperability and complexities to include information and system assurance that are supported by assurance processes at each level. This supports the need for strong quality control and audit processes as described by Evans, Maglaras, He, and Janicke (2016) to enable and support assurance based processes and procedures. Further emphasized by Yeo, Abualkibash, Banfield, and Ashur (2018) are the challenges raised by critical infrastructure for education and training to create and fill skills needed for cybersecurity assurance. Assurance is a fundamental cybersecurity principle with dependencies of operational and IT auditing processes according to participants #2, #3, and #5 that must be incorporated in any cybersecurity and compliance program as a deliberate element of the organizational strategy. Assurance was mentioned in 11 documents as an element needed to achieve continuity of

operational services (Table 4) . The documents emphasized the need to sustain cybersecurity functions for confidence and reliability of services that are geographically located and remotely managed. An organization's ability to ensure there are no single points of failure in crucial support programs like cybersecurity is necessary according to the participants. Documentation supported the participants with identification of key assurance enablers such as auditing, monitoring, and system component status updates like the known performance variables associated to industrial sensors.

Preparedness. The technology factors relevant to cybersecurity in critical infrastructure remains the principal focus in organizational strategic goals associated with cybersecurity. Key assets that comprise critical infrastructure represent significant services for the respective communities and society. During the interviews, all participants agreed, and most of the documents supported, that preparedness remains a predominant factor to the success of a cybersecurity program. Participants reported the need to carefully plan the cybersecurity program using focal points within the infrastructure that is identified based upon priorities, resource constraints, response and recovery variables, and time sensitive implications in a geographically separated environment. Documentation named preparedness as a key factor in the regional critical infrastructure framework for planning and implementation to address the goal of resilience. Karabacak et al. (2016) supported the need for preparedness in the pursuit of infrastructure resilience with the recognition that minimal concern exists for assessing cybersecurity in critical infrastructure and the focus upon exploration of best practices and recommended checklists continues despite the limited effectiveness and return on

investment. The participants emphasized the need for holistic cybersecurity with preparedness serving as a pivotal factor to ensure physical and virtual threats are addressed in the organizational strategy. The documentation emphasized the need to conduct regular exercises mimicking the capabilities of existing cyber threats to capture the lessons learned for driving improvements to the cybersecurity program.

Response. Assessments of the evolution and maturation of cybersecurity effectiveness continue to use a rubric designed with conventional tradecraft in mind. An informed response to cyber threats according to participants, and supported by documentation, is an essential factor. Continuous data collection, processing, analysis, and reporting is crucial to informed response with pursuit of indications just as important as the reaction to an attack. Every response must be documented and analyzed according to participant #3 to create a knowledge base with categorized information to help anticipate threat activity in dynamic circumstances. Participant #4 mentioned the need for analytics to support predictive threat intelligence to better prepare response functions. Resilience is described by Murdock, de Bruijn, and Gersonius (2018) as resistance to a particular shock and the speed of return to equilibrium, and more generally as the ability to prepare, plan, respond, recover, and adapt to malicious activity. Response to adverse events is a key factor in a cybersecurity program according to participant #1, who also described improvements in response functions as timely resulting in increased effectiveness. Agile response techniques have been modeled through the maturation of the IoT (Russell, Goubran, Kwamena, & Knoefel, 2018). Participants #2, #4, and #5

promoted the use of technology to help automate responses to cybersecurity incidents, and to better document the knowledge learned by the technical and human factors.

Four factors were identified by the participants, also included in the organizational documents, and covered in existing literature that comprise the support for the second theme (Table 4). Participants reported the need to diversify cybersecurity program to include physical and virtual threat vectors. Cyber incidents were expected according to the participants and a strategic shift to achieve infrastructure resiliency makes sense considering the increased sophistication of cyber threats. The documentation supported the need to focus upon resilience for continuity of operational services in critical infrastructure. Fifteen documents included goals to support infrastructure resilience over the use of conventional vulnerability mitigation alone. Participants reported that the application of fundamental cybersecurity practices such as social engineering and email phishing training must not be lost while pursuing infrastructure resilience. Within the documentation, the four factors of continuity, assurance, preparedness, and response were emphasized in the pursuit of infrastructure resiliency while reinforcing fundamental cybersecurity practices to remain relevant and effective against the cyber threats. The results of this study revealed a strategic shift in priority from traditional vulnerability cybersecurity protection to infrastructure resilience is needed in an organizational strategy to meet the modern cybersecurity threat landscape against critical infrastructure. The RAT, chosen as the conceptual theory, states the need for an offender, target, and weak protection with critical infrastructure often surfacing as a common victim by physical and virtual threats. Fischer (2016) identified three similar

criteria in considering cybersecurity risk that align closely with the RAT, which are threats, vulnerabilities, and impacts. Media coverage of the success in sophisticated attacks against critical infrastructure has become more common over the last few decades leading up to 2019 (Cassotta & Sidortsov, 2019). The formation of a "kill chain" model highlights the sense of urgency with an advanced persistent threat as a willing offender, the targetability of critical infrastructure key assets, and common knowledge that cybersecurity in critical infrastructure is a significant concern (Denham, 2015). Key assets comprising critical infrastructure are commonly expected to fall victim to an attack, successful or attempted, at some point in its life cycle. Cybersecurity in critical infrastructure represents physical and virtual investigative challenges spanning technical and human factors.

Theme 3 - Importance of Security Awareness

The third theme resulting from the data analysis phase is the importance of security awareness. In 2008, the Federal Energy Regulatory Commission (FERC) published FERC Order 706, which contained the principle concepts for the standard on protecting critical infrastructure. Security awareness was listed as an original concept in the 2006 FERC order and remains a principle concept for cybersecurity in critical infrastructure. The participants were consistent in their inclusion of security awareness as a factor in risk management throughout the interviews with added emphasis in organizational documentation. This is supported by Hilt (2018) who described six functional areas that must be addressed in the organization's critical infrastructure

planning to ensure robust implementation, which are management, system operations, IT management, human resources, training, and physical security.

Four factors related to the importance of security awareness were identified in the participant interviews and documentation. Information contained in Table 5 represents the distribution of the four factors in the participant interviews and study documents. The data in Table 5 represents where one or more of the factors were identified and the numbers do not represent a total count of how many times a specific term was used in the data sources.

Table 5

Distribution of Theme 3

Data sources	Management	Training	Functions & capabilities	Compliance & cybersecurity
Participants	5	5	5	5
Documentation	10	21	7	14

Participants outlined the importance of security awareness to organizational strategy, which appears throughout the literature review to acquire and maintain indepth knowledge of cyber threat capabilities, as well as the indeginous infrastructure to best visualize the potential security vulnerabilities through an offender's perception of the environment. Participants #1 and #2 commented on the need for the workforce to be security aware with an appropriate level of understanding in cybersecurity to effectively associate their actions, or lack of action, with the relevant cause and effect. Viewing the critical infrastructure from the cyber threat perspective, according to participants #1 and

#2, is necessary to gain the offender's perception of potential vulnerabilities and access opportunities. Contract vendors are a necessity in sustaining critical infrastructure assets like power and water; however, these must be considered according to participants #2 and #3 in the cybersecurity program. The documents contained references to human and virtual threat vectors related to software and hardware developers, and technology support and repair services with the need to extend cybersecurity measures for external variables like vendor software and hardware updates. As a result of advances in cybersecurity tradecraft, participant #3 stated the need to consider human factors as in physical security measures are often overlooked in favor of the technical factors in achieving a balanced security awareness. According to participants #4 and #5 workforce security awareness and organizational policy must keep pace with the cyber threats beginning with "a basic understanding of cybersecurity to relate the implications in their personal and professional lives." Ensuring employee security awareness and understanding of the cyber threat possibilities, as well as the organization's infrastructure is vital to informed response (Knowles et al., 2015). As a crucial risk management element and strategic factor, security awareness depends upon an organization's holistic and intimate understanding of its own operational environment and the many physical elements and virtual architectures operating together to create and enable the key asset environments (Lee & Lim, 2016).

Without an intimate awareness and understanding of the respective technologies and the resulting cause and effect possibilities there is an increased risk for ineffective implementation. Participants related their experiences with unforeseen security

challenges created as a result of converging IT and OT to enable and support key assets comprising the critical infrastructure. Many of the security challenges were accidental or incidental resulting from a lack of understanding as described by participants #3, #4, and #5. To address these challenges, participants #1, #2, and #4 identified their approach by updating their training content for the cybersecurity program in a collaborative production partnership across the compliance, training, and IT teams. Participants #2, #3, and #5 reported their experience to ensure workforce awareness by adopting a common lexicon and definition across the compliance, training, and IT disciplines within the organization. Those participants also emphasized their advocacy for organization level standardization that was adopted regarding minimum training goals, which included mandatory briefings to explain the security measures and answer workforce questions. Security awareness requires some level of understanding to apply the concepts in day to day functions, and to help achieve the intended results envisioned with a cybersecurity program (Pham et al., 2017). The return on investment was an increased understanding of implications along with an awareness of personal and professional consequences for the individual, customer, and organization. Pham et al. (2017) found that the diversity of perspectives between the workforce and respective programs like cybersecurity and compliance differ in how intentions and behaviors toward cybersecurity compliance are perceived.

Management. Support from all levels of the organization's management is crucial to ensure the respective fundamentals are applied to establish cybersecurity program baselines. Security awareness begins with assessing risk and prioritizing the

risk to the key assets for alignment of the organization's functional areas as a proactive strategic advantage to the cyber threat landscape (Fischer, 2016). Management support of cybersecurity programs is not enough according to participant #1. There must be management buy-in that underpins the strategic implementation of said programs that will ensure the authority to match the responsibility. Participants #2, #3, and #5 declared that without management support and investment in security awareness across the organization, the workforce will not have the necessary understanding of cybersecurity concepts for application in their daily functions. Research by Paliszkiewicz (2019) supported the findings with the identification of leadership as a key factor for a successful cybersecurity program. To achieve a successful cybersecurity program, leadership and management are essential factors according to Amankwa, Loock, and Kritzinger (2018) with emphasis placed upon creating an organizational culture that supports and nurtures compliance. Participants #4 and #5 mentioned trust in management to establish and sustain partnerships within critical infrastructure stakeholders as a key factor to enable cross-organization security awareness in all activities. The concept of trust was corroborated in organization documents with goals to create trust across organizations such as a collaborative cybersecurity relationship for advancing information sharing and data analysis. Documents also identified open communications between leadership and cybersecurity practitioners to build and maintain trust, and emphasized the concept of developing a partnership to address common cybersecurity challenges with emphasis on the sharing and analysis of sensitive information.

Training. Training quickly surfaced as a principal factor to establish and sustain the necessary levels of security awareness in all elements within an organization's structure. Emphasis on training availability and achieving the desired training effects were raised by all of the participants and in most of the documents. The importance of flexible and relevant training in security awareness was described by participants #2 and #4 with a focus on ensuring the training was presented in a progressive manner tailored for the workforce skillset. Highly technical training on security awareness to include cybersecurity concepts and theory are not effective if presented using complex explanations and examples requiring expert knowledge not common to the audience. Pham et al. (2017) found that cybersecurity programs using complex or vague task descriptions to help with security awareness resulted in negative workforce behavior. There is often a difference in technical skills and knowledge between management and the general user in the workforce according to Pham et al. (2017) as well as the lack of special skills training afforded to users asked to perform complex cybersecurity tasks. Participant #1 mentioned a situation involving the human resources (HR) team who received security awareness training that did not achieve its intended training effect. Instead the training resulted in frustrated HR and training teams since the training relied on a technical review of the WannaCry Ransomware Worm to articulate the attack details. Particiants #3 and #5 identified security awareness together with the associated training as a pivotal decision point for risk assessment of the cybersecurity and compliance programs. Miranda (2018) described the importance of a training design for security awareness that incorporated theory and hands-on application to teach the

workforce how to identify and respond to malicious activity. The participants supported this approach with their own training exercise examples that are conducted regularly to test and reinforce security awareness knowledge and response skills. Documents contained information on using regular and random cybersecurity tests and exercises to reinforce security policy and awareness. The importance of security awareness is consistent throughout the documents with focus placed upon the use of hands-on application of new knowledge to form the needed experience in a controlled environment.

Functions and capabilities. Participants were consistent in pointing out how important it is for the workforce to acquire a basic understanding of the organization's systems and architectures. According to the participants, a basic level of understanding will help each employee consume and apply the security awareness information to help create a culture of compliance. Participants #2 and #3 described how their compliance and IT departments began to provide the who, what, when, where, why, and how related to cybersecurity and compliance guidance and policies as a new approach in security awareness training. The example those participants outlined was the extra effort management took to explain how many of the systems are too expensive for the organization to own and maintain. The additional information according to participants #2 and #3 regarding leased systems allowed the workforce to gain a new perspective on cybersecurity training and their role in helping to be an early identifier of possible issues. Participants #1 and #4 reported that providing an explanation of the organization's systems and architectures in the context of cybersecurity tasks might cause a cascade of

negative effects. A compliance incident could be the result that may lead to causing a negative impact to the community and society's trust in the organization responsible for critical infrastructure assets. Participants #3 and #5 reported that helping the workforce achieve a greater understanding of the organization's systems and architectures in turn increases the understanding of the functions and associated organizational capabilities. This builds confidence in performing day-to-day tasks and a confident workforce that believes in the organization will treat it as their own according to participants #1 and #4.

Another example provided by participants #1 and #5 was the use of scenario based training, which presented cyber attacks reported in the media in a practical manner to demonstrate how employee roles within an organization are interconnected. The goal of the cybersecurity tests and exercises according to participant #3 was to give the workforce an informed situational awareness that would enable each employee to interpret actions and activity through a cybersecurity lens. Documents contained goals for creating random tests to reinforce security awareness and conduct exercises to apply cybersecurity procedures as outlined in policy. All participants related their positive experience in educating the workforce on the organization's functions and capabilities with an overall positive impact to the effectiveness of the organization's cybersecurity program. New employee orientation was identified in the documents to help achieve security awareness through the workforce training program, which included basic definitions and descriptions of the organizations functions and capabilities along with the underlying cybersecurity tasks in the context of systems and architectures.

Cybersecurity and compliance. Participants #1, #2, #4, and #5 reported that cybersecurity and compliance are often used interchanbebly in the context of a single program; however, all of the participants stated their organizations included separate and distinct cybersecurity and compliance programs with authority and responsibility for each program residing with the organization's leadership team. Kure, Islam, and Razzaque (2018) described the use of compliance programs to demonstrate security compliance as cybersecurity in critical infrastructure. An enduring challenge identified by participants #2, #3, and #4 was the use of technical and legal terminology by each program. They went on to state the workforce perception is that cybersecurity and compliance were implemented as a single program and the guidance is unnecessarily wordy and complex. Documents reflected the planning and implementation of cybersecurity and compliance programs as deliberate focal points with emphasis on collaboration and communication. The application of compliance was mentioned in the documents with consideration of cybersecurity as well as overarching coverage of critical organization priorities such as financial, logistics, and business compliance programs. Participants #1 and #5 described their use of initial employee inprocessing to articulate the required legal policy forms like a non-disclosure agreement with explanations given during a question and answer session. These participants went on to explain that future cybersecurity and compliance interactions were tailored to each department to ensure everyone was communicating using a common vocabulary and set of definitions. Documents supported the use of new employee orientation as part of the cybersecurity and compliance programs. The documents emphasized integration with the workforce training program. Participants #1

and #5 reported this was particularly helpful in articulating cybersecurity guidance and the associated explanations on why and how to follow the guidance resulted in clarification of the technical terms while the overall focus remained on interpreting and understanding the policy. Miranda (2018) reported that social engineering remains a significant challenge for cybersecurity programs with negative consequences in critical infrastructure such as defeating custom security measures. Training programs that explain cybersecurity tasks with an appropriate level of technical detail often improves workforce behavior and attitude toward security compliance (He & Zhang, 2019).

Most employees perform their daily functions without malice; therefore, when employees do not fully pay attention to the weekly or monthly reminder to use strong passwords, and their lack of compliance with that policy, it is not always with malicious intent (Amankwa, Loock, & Kritzinger, 2018). In such a situation, the employee may create the strong password but write it down to help remember it. Participants #3 and #5 spoke to such a situation in their organizations, which resulted in a vendor gaining access to an account using an employee's credentials. This esculated into a system compromise across the organization according to participants #3 and #5, because the user's credentials represented the highest level of access for the associated databases and systems. Participants #3 and #5 explained that a cybersecurity investigation found the employee did not have the necessary level of security awareness to link the compromised password to any other potential than their account, with the employee asking why does it matter since it was just their account. Research by Pham et al. (2017) revealed that an employee lacking security awareness may engage in risky behavior, whether intentional, accidental,

or incidental. Participant #2 outlined the use of a positive reinforcement measures. When the random security awareness tests were conducted, there were rewards given to the top performers during the test as well as quarterly recognition presentations ranging from paid time off, certificates, and monetary performance awards. Positive reinforcement and program transparency were mentioned by all of the participants as a necessary part of their compliance programs, highlighted as one reason for the increased positive behavior toward cybersecurity and compliance programs. An informed workforce tends to comply with organization cybersecurity policy and guidance with an increased positive attitude for supporting, and championing, a culture of compliance (Amankwa, Loock, & Kritzinger, 2018; He & Zhang, 2019). Amankwa, Loock, and Kritzinger (2018) found that leveraging compliance leadership to support organization cybersecurity resulted in positive workforce behaviors leading to increased successful application of cybersecurity tasks in their daily functions. The use of random cybersecurity tests to include social engineering and physical security scenarios were included in the documents. In addition, the documents included requirements for conducting exercises to test holistic security and compliance program effectiveness such as cross-program collaboration and coordination.

The RAT was chosen as the conceptual theory to help identify and describe the phenomena related to cyber threat landscape activity. Responsibility for identifying known or unknown activity depends upon the organization's compliance and/or cybersecurity programs (Reyns & Henson, 2016). These programs are dependent upon activity indicators that have been associated with key asset services within critical

infrastructure. The criteria for RAT criteria includes an offender, target, and guardian (Leukfeldt & Yar, 2016). Within critical infrastructure the identification and interpretation of activity indicators require special expertise in IT, cybersecurity, tradecraft. Participants, organizational documents, and current literature indicate the increased occurrence and sophistication of cyber attacks against critical infrastructure, and the need for a robust cybersecurity program. Media coverage of the attacks against key asset services that comprise critical infrastructure has revealed the increase in volume, velocity, and sophistication of attacks related to the consequences along with operational and technical details. The RAT is well known for its use in studying criminal behavior within a terrestrial environment, and the use of RAT has been successfully adopted for application to virtual environments (Leukfeldt & Yar, 2016; Reyns & Henson, 2016). Findings from this study, guided by the RAT, indicate a persistent need for cybersecurity and compliance programs working in a collaborative production relationship to defend against a highly skilled offender focused upon critical infrastructure. Key asset services are being digitized to accommodate the convergence of IT and OT, resulting in an increased presence of known and unknown security challenges.

Theme 4 - Importance of Organizational Leadership Support and Investment

The fourth and final theme that was revealed in the data analysis phase is the importance of organizational leadership support and investment. Application of conventional cybersecurity best practices is not enough to achieve holistic protection of the key assets in critical infrastructure (Pursiainen, 2017). Participants #3 and #5

reported that they have incorporated a practice of documentating techniques that comprise best practices, which were revealed from successful conventional IT vulnerability response. The same participants also reported those best practices alone often do not adequately apply to critical infrastructure without modification that requires leadership support to fully integrate the necessary changes across several functional areas. Participant #2 stated that best practices from conventional vulnerability based measures have not provided an adequate baseline that enables the application of enhanced cybersecurity tradecraft. Documents identified the need for organizational leadership and IT coordination, and to ensure the technical staff remain updated on cybersecurity tradecraft in critical infrastructure. Participants #1, #3, and #4 stated the best practices that are documented from day to day experiences, as well as cybersecurity tests and exercises, are used in cybersecurity process reviews to help update workforce training and increase effectiveness of existing policy. The same participants reported that without leadership support in delegating decision authority to the cybersecurity leads, the ability to document the details of the cybersecurity practices and results in a timely manner may be degraded in such fluid circumstances.

Proactive organization leadership was asserted by participants #1, #2, and #4 to be a crucial element in the success of any cybersecurity program. Paliszkiewicz (2019) found that organizational leadership investment in the cybersecurity and compliance programs is necessary for robust return on investment along with workforce trust in leadership to help foster positive behavior toward cybersecurity tasks. Participants #4 and #5 mentioned that the results from cyber risk analysis often do not receive the needed

attention from mid-level and executive leadership. Paté-Cornell, Kuypers, Smith, and Keller (2018) reported proactive leadership with their description of recent cyber attacks in motivating change to organizational cybersecurity approaches. Participants #2 and #3 attributed the lack of basic cyber knowledge to the resulting challenges faced by leadership for consuming the results and the application in planning and decision processes. Documents contained a task to ensure management acquires basic compliance and cybersecurity knowledge to include risk management.

Four factors related to the importance of organizational leadership support and investment were identified in the participant interviews and documentation. Information contained in Table 6 represents the distribution of the four factors in the participant interviews and study documents. The data in Table 6 represents where one or more of the factors were identified. The numbers do not represent a total count of how many times a specific term was used in the data sources.

Table 6

Distribution of Theme 4

Data sources	Communication	Resource investment	Process standardization	Cybersecurity fundamentals
Participants	5	5	5	5
Documentation	21	15	10	19

Participant #5 reported "An effective cybersecurity program in critical infrastructure must provide holistic coverage of key assets with full buy-in from stakeholders and senior leadership that support change in the diverse and dynamic critical

infrastructure operating environments." Documents emphasized the need for the organization to maintain an awareness of modern technologies and to acquire adequate level of understanding of how those technologies may be disruptive to the organization's infrastructure. Critical infrastructure attacks do not have the same level of attention from the media and researchers as mainstream attacks such as those related to Sony Pictures Entertainment, Target Corporation, and the Democratic National Convention, which often results in leadership not having sufficient awareness of the threats and challenges relevant to cybersecurity in critical infrastructure (Mangelsdorf, 2017). Organizational leadership has increased resource investment according to participants #2, #3, #4, and #5 to establish and improve corporate compliance programs in an effort to help drive cybersecurity effectiveness and workforce engagement. Tailored corporate compliance programs may help in the discovery of indicators to support the prediction of possible incidents before or as the circumstances are formed that make an incident probable (Amankwa, Loock, & Kritzinger, 2018). Participants #1, #4, and #5 articulated the positive impacts brought about by the collaboration between their organization's compliance, cybersecurity, and training programs. Participants #2 and #3 highlighted how their leadership teams began emphasizing compliance, cybersecurity, and training programs. The same participants pointed out those programs were driven from the top down that included delegated authority to cybersecurity team leads to help ensure flexible implementation at the appropriate level. Documents revealed the focus on separate compliance and cybersecurity program requirements and tasks with emphasis on leadership training to ensure knowledge and understanding of the program roles.

Communication. Participants #2, #3, and #5 identified communication between the compliance, cybersecurity, and training programs as a key enabler, and participants #1, #4, and #5 reported the need for those programs to invest in communication resources as an enabler for the leadership team and the workforce. This supports Alcaraz and Zeadally (2015) assertions that encouraging strategic and open communications within the organization at all levels is often related to positive outcomes. This is also supported by Mangelsdorf (2017) who identified communication as the cornerstone of creating an organizational culture to equally address the technology and human organizational elements in the context of cybersecurity and compliance strategy. Documents identified communication as a strategic goal and participants #1, #2, and #4 asserted the importance of strategic communication by the leadership team to ensure the workforce has a clear and consise understanding of the guidance and policy so that implementation is standardized throughout the organization. Participant #3 agreed that standardization was important and achieving it depended almost solely upon consistent leadership messaging. Participants #4 and #5 also supported the assertion by stating leadership communication must be used to align the mid-level leadership with a standardized interpretation of the guidance and policy. Documents contained tasks with the need for communication between compliance, training, and cybersecurity.

Resource investment. Participants #2, #3, and #5 articulated the initial resource investment needed to establish a cybersecurity program to meet today's cyber threat landscape may be expensive and sustainment is an enduring expense. Leadership tools such as risk analysis were identified for resource investment in documents with an

emphasis on incorporating applicable functions in support of cybersecurity and compliance programs.. Documents emphasized the need to identify special training for critical skillsets and participants #1, #4, and #5 reported on the up front expenses of cybersecurity to include a human element that further adds to the expense of establishing and sustaining a cybersecurity program. An organization's leadership team is slow to invest in a cybersecurity program that is designed to address a challenge with a probability of occurring, whether it is a low or high probability since a given challenge does not yet exist (Pham et al., 2017).

Participants #3, #4, and #5 reported the challenges revealed from assigning cybersecurity tasks to non-technical personnel with the understanding those tasks are in addition to their primary job functions. Participants #1 and #2 emphasized that leadership must be aware of the necessary knowledge and experience to perform cybersecurity functions to make informed decisions for assigning tasks. Pham et al. (2017) reported the practice of assigning cybersecurity tasks as additional duties rather than creating dedicated cybersecurity positions resulted in a conflict for the workforce to decide whether to perform the secondary task (cybersecurity) or their primary job tasks. Documents identified separate resource investments to establish independent compliance and cybersecurity programs and participants #1 and #3 reported since the formal cybersecurity program was established the perceived conflict in the workforce between their additional cybersecurity tasks and primary job functions had been resolved.

Process standardization. Participant #1 stated the use of process standardization was instrumental in how the cybersecurity program was able to respond to cybersecurity

threats, and reported a dependency upon leadership support to ensure adequate resource investment for implementation and sustainment of crucial processes. Participants #2 and #3 reported the use of process standardization has established a common foundation for geographically separated entities. Participant #2 highlighted leadership support and investment to establish a standard operating procedure for remote infrastructure monitoring. Participant #5 reported how leadership supported the delegation of authority for process standardization to the department level for accommodation of non-standard circumstances that require tailoring of the cybersecurity tasks. Participant #4 reported on the success of process standardization in delivering persistent results that were easily consumed from diverse functional areas of the organization. Participant #5 revealed the importance of leadership support to the integration of process standardization throughout the organization as a required element in cybersecurity, compliance, and training programs. Documents reinforced this premise with descriptions of standardized data analytics, incorporating machine learning, and threat assessments. Documents identified key areas for leadership support of resource investment as an enabler to standardization that included cybersecurity monitoring, auditing, and incident reporting and all participants reported process standardization as a crucial factor to support the cybersecurity program. Paté-Cornell, Kuypers, Smith, and Keller (2018) found the common approach to cybersecurity in critical infrastructure is to adopt conventional best practices with the expectation that those practices can be adapted to support standardized processes without negative implications to performance and effectiveness. Pham et al. (2017) emphasized the importance of leadership support with the appropriate resource

investment and identified four information security management phases that may support the pursuit of process standardization, which were deterrence, prevention, detection, and recovery. Documents referenced leadership investment to include key program elements for review and assessment to support process stabilization in cybersecurity and compliance programs. Participants #3 and #5 reported the increased sophistication of cyber threats indicates process standardization in cybersecurity may help identify and document the analytic findings for indicators in support of the compliance program, and these participants asserted the importance of leadership support for integrating at all levels within the organization. The same participants went on to state that process standardization has provided a common procedural and reporting foundation that helped attribute incidents more accurately as technical or human fault. Paté-Cornell, Kuypers, Smith, and Keller (2018) emphasized the importance of conducting risk assessment to help inform leadership support processes for allocating resource investments to include budgetary allocations that serves as an example for process standardization. Documents also contained information for incorporating process standardization with leadership support and adequate resource investment to enable cybersecurity program planning and implementation.

Cybersecurity fundamentals. A common thread revealed in data collection and analysis was the insistence conveyed by all participants that leadership support and adequate technical resource investment is required to incorporate cybersecurity fundamentals as a foundational element to the cybersecurity program. Participants #3 and #4 provided several examples of cybersecurity fundamentals such as the use of virus

and malware software on all systems, and daily software updates for applications and operating systems. The documents contained guidance for ensuring cybersecurity fundamentals remained a viable factor in planning and implementation activities. Participant #3 specified the use of traditional cybersecurity fundamentals as the foundation to build and incorporate tailored functionality and measures to protect the critical infrastructure. Hilt (2018) outlined eleven fundamental concepts as the foundation of a good cybersecurity program emphasizing the common availability of concepts and best practices for a program, but often lack the strategies for implementation and sustainment. Participants #4 and #5 reported cybersecurity fundamentals as the stable functions in their programs that set a culture of compliance throughout the organization. Those same participants explained that cybersecurity tasks such as strong passwords, locking terminal screens, safe email attachment handling, and mobile device security are familiar to the workforce resulting in positive security behaviors. Participants #1 and #2 reported the crucial nature of strong passwords as the first line of defense and a cybersecurity fundamental that is also an example of a fundamental enabler for compliance. Participant #3 asserted the inclusion of cybersecurity fundamentals like safe email attachment handling into compliance process guidance as a force multiplier and provided the example of regular exercises to test workforce understanding of how to protect against malicious email attachments. Participants #3, #4, and #5 emphasized the growing concern with challenges stemming from mobile device security on their existing cybersecurity programs.

Critical infrastructure is comprised of one or more complex architectures with a convergence of legacy and modern technologies like serial communications used between actuator systems and sensors that often results in a false sense of security if cybersecurity fundamentals are the sole protection measures (McLaughlin et al., 2016). Documents identified the need to consider the use of customized cybersecurity measures in addition to cybersecurity fundamentals when forming the cybersecurity program. Participants #1 and #5 reported the challenges in workforce training when cybersecurity tasks go beyond the cybersecurity fundamentals. Participant #5 went on to state that the introduction of modern IT, along with the accompanying complex security tasks, resulted in an increase in compliance incidents due to workforce confusion and frustration. Incorporating fundamental cybersecurity tasks remains a necessary element in the cybersecurity program to instill stability and consistency leading up to the transition into next level measures necessary to protect the complex architectures that comprise critical infrastructure (Lošonczi et al., 2016).

The RAT states the need for an offender, target, and weak protection (guardianship) with critical infrastructure with the rise in sophisticated cyber attacks against critical infrastructure, there is a crucial need for leadership support and investment to ensure guardianship. Five offender types were reported by Fischer (2016); criminals, spies, nation-state actors, hacktivists, and terrorists. Critical infrastructure remains a prized target for all offender types with successful attacks increasing in the damage and disruption to key services, as well as negative impacts to social trust (Cassotta & Sidortsov, 2019). Attacks against critical infrastructure may come from

many directions at any time; therefore, a leader's awareness and understanding of their own infrastructure, and their response posture, remains a crucial factor as reported by the participants and organizational documents. The RAT defines an analytic framework that focuses upon the offender, target, and asset defense (guardianship) to study malicious activity and vulnerability indicators, which provides crucial information for leadership awareness. Denham (2015) represented the presence of a kill chain model related to critical infrastructure to enable focused discovery analysis of bounded areas within the infrastructure. Cybersecurity programs are the eyes and ears of the leadership that expects an attack with efforts to include the concepts of infrastructure resilience, and the use of the RAT as an analytic framework (Leukfeldt & Yar, 2016) may provide a needed advantage in understanding offender motivations, intentions, and targeting preference based upon protection posture (Mihelič & Vrhovec, 2018).

Applications to Professional Practice

There findings were compelling and supported current literature on cybersecurity in critical infrastructure along with the organizational documents. Findings from this study are crucial to cybersecurity practitioners, as well as IT compliance, and training professionals in critical infrastructure. These findings are relevant to IT and compliance professionals who can use the strategies revealed in this study to mitigate cyber threats to critical infrastructure. The study revealed key factors that prepare IT and compliance practitioners with crucial knowledge on strategies to help identify elements in the respective program for enhancement. The participants reported their participation in the study helped them identify and focus on key factors with renewed insight to improving

cybersecurity strategy to include new ideas on compliance and training program collaborations. The essential cybersecurity factors revealed in this study provide an advantage to the IT professional's awareness and understanding to influence and enable the workforce and enhance existing strategies. As a result, the improved IT practices will help mitigate the cyber threat offender's perception of critical infrastructure as a target and strengthen cybersecurity protection to reduce the cyber threat opportunities.

The study findings may be used to plan and implement strategies to improve IT practices to meet the modern cyber threats challenges in critical infrastructure. The study found that today's cyber threat offender seeks and applies sophisticated knowledge and understanding of the targeted critical infrastructure and cybersecurity tradecraft to achieve a successful attack. Four themes were revealed by the study: a robust workforce training program is crucial, infrastructure resiliency is a priority, the importance of security awareness, and the importance of organizational leadership support and investment. These are presented as key findings to a successful cybersecurity strategy in protecting critical infrastructure and supporting an organizational compliant environment.

The four themes were identified in the study as essential to cybersecurity in critical infrastructure, and IT professionals may use this knowledge to modify their cybersecurity strategies for application in both conventional IT and critical infrastructure environments. The key factors were identified and discussed for each theme that empowers the pursuit of improved IT practices. The key strategies from this study may improve IT practices to facilitate adapting the current tools, techniques, and

methodologies to mitigate the cyber threat's success in attacking the human and technical elements.

Implications for Social Change

The study findings indicate there could be positive change in strategies used by IT and compliance professionals to mitigate cyber threats in critical infrastructure. Improvements in the protection of critical infrastructure may increase the confidence and trust in the respective service providers by the community and society. A catastrophic failure in critical infrastructure, as a result of malicious attack or natural disaster, has been reported in the news media with the potential to impact national security and public safety.

The study findings identified key factors necessary for improved cybersecurity strategy for protecting key services such as power, water, transportation, financial, and healthcare. The increased occurrence of successful cyber attacks has resulted in the disruption of key utility services and loss of personal financial and healthcare data. Luo (2016) found that concern has increased within communities, and society in general, on the ability of the government and industry to protect its citizens and customers. This study provided an exploration and contextual analysis of strategies in cybersecurity in critical infrastructure that revealed factors to support and enable positive social change through innovative and creative options for IT and compliance professionals. Successful protection of critical infrastructure benefits communities and society by ensuring key services such as healthcare and power are sustained during crisis events. This success also contributes to improving and enhancing the IT body of knowledge by protecting

sensitive industry and consumer data that enables the continued flexibility in using modern technologies like mobile devices in healthcare facilities and smart homes. In addition, the study findings may help improve employee behaviors toward cybersecurity and compliance.

Recommendations for Action

Many key elements of a critical infrastructure are comprised of IT such as the connectivity of physical sensors with geographically remote monitoring operations, placing IT professionals at the forefront of cyber threat mitigation. The strategies identified in this study can contribute or enable IT professionals during strategic planning and implementation. The study also provides greater insight into opportunities for collaboration between cybersecurity, compliance, and training programs. Strategies revealed in this study contribute to the existing body of knowledge for cybersecurity to help meet the complexity and sophistication represented in the cyber threat landscape with possible value added in holistic organizational cybersecurity efficiency and effectiveness. Strategies reported to be effective from this study for IT practitioners include:

- a robust workforce training program is crucial,
- make infrastructure resiliency a priority,
- importance of security awareness, and
- importance of organizational leadership support and investment.

The study findings can be used by organizations and stakeholders within the critical infrastructure industry to create and tailor collaborative cybersecurity and compliance programs.

The first recommendation for IT practitioners is the creation of a robust training program. The study participants emphasized a robust training program in support of cybersecurity in critical infrastructure with key factors of relevancy, flexibility, hands-on application, communication, and effectiveness. The study participants reported these factors as essential to cybersecurity, and compliance, for a cybersecurity program to quickly tailor its training effect to satisfy on-demand and custom training requirements, as well as adapt to individual needs and fluid challenges. The second recommendation to IT practitioners is to make infrastructure resiliency a priority with key factors of continuity, assurance, preparedness, and response. The study participants emphasized the priority of a strategic shift from vulnerability based protection only that includes infrastructure reciliency. The study participants reported resiliency as a necessity to protect and ensure critical services are neither degraded, nor lost, against a dynamic cyber threat landscape targeting critical infrastructure, which if successful would be catastrophic to the affected population. The third recommendation to IT practitioners is to establish and incorporate security awareness throughout the workforce that is tailored for consumption by the targeted audience.

The results of the study underline the crucial need for workforce security awareness with an emphasis for IT practitioners on the factors of management, training, functions and capabilities, and compliance and cybersecurity. Based upon the findings of

this research, IT and compliance professionals should emphasize the importance of security awareness to organizational strategy to acquire and maintain indepth knowledge of cyber threat capabilities, as well as the indigenous infrastructure to best visualize the potential security vulnerabilities through an offender's perception of the environment. The final recommendation is the importance of organizational leadership support and investment to the cybersecurity program. The study identified the key factors for IT practitioners of communication, resource investment, process standardization, and cybersecurity fundamentals. The study findings highlighted the crucial need for proactive organization leadership and IT practitioners in the success of any cybersecurity program. The study findings attributed the lack of basic cyber knowledge to the resulting challenges faced by leadership for consuming the results and the application in planning and decision processes.

Dissemination of the study findings is approached through multiple techniques. I will disseminate a summary of the study to the participating organizations and will present the research findings through scholarly and technical publications. In addition, I may circulate the study findings through presentations at professional conferences and workshops to include corporate and healthcare compliance, project management, law enforcement, and critical infrastructure workforce development.

Recommendations for Further Study

The findings of this study report on the exploration of industry cybersecurity strategy in protecting critical infrastructure. This study revealed strategies used by IT and compliance professionals to mitigate cyber threats to critical infrastructure. The focus

was on organizations in the Pacific Northwest United States that have cybersecurity strategies to mitigate cyber threats to critical infrastructure. Recommendations for further study include similar research in other regions of the United States with consideration for use of a different design methodology and conceptual framework for research diversity. This study has contributed to the literature; however, additional research is warranted as reported in this study's findings.

Topics were found in this study that serve as relevant issues in the cybersecurity discipline and the IT skill community. Recommendations for further study:

- Perform studies using a cyber threat lens. This perspective of an organization's infrastructure may reveal a better understanding of crucial indicators such as offender intent and motivation, target selection and exploitation choices, and perceptions into cyber defense tradecraft and effectiveness of guardianship.
- Research how conventional vulnerability based cybersecurity approaches could be enhanced to help enable cybersecurity resiliency.
- Use data science tradecraft to provide a better understanding of critical infrastructure borne of the convergence of IT and OT that presents a complex cybersecurity challenge.
- Focus upon cybersecurity training strategies through collaborative teaming with the compliance and training programs.

Reflections

As a computer scientist, I was confident in my understanding of cybersecurity as I entered into this study. However, the level of effort necessary to ensure focus and rigor in the academic research was a rewarding challenge that has helped me grow personally and professionally. My journey in this study was made whole by the world class faculty and my fellow students who, through team projects and collaboration, helped me identify and overcome biases through the application of knowledge and skills acquired during the program.

The data collection and analysis was a highlight experience with the opportunity to interact with like professionals who were passionate about cybersecurity in critical infrastructure. In addition, the participants showed a high level of positive energy and enthusiasm with many commenting on the opportunity to participate in a study that would help increase the body of knowledge and provide actionable information to improve the cybersecurity and compliance disciplines. The positive attitudes and eagerness to share their experiences and ideas on improving cybersecurity strategic planning and implementation was inspiring and motivating. I was energized by the experience and now view challenges in a new light, knowing I have the skill to collect, process, analyze, and report on the respective challenge to contribute and enable creative and innovative solutions.

This study has given me the necessary personal and professional experience to be successful as a productive member of my chosen profession. My awareness and understanding of research has matured along with gaining academic writing skills that are

critical in how I communicate the results and the lasting impacts that brings to the skill community. With this new found confidence and skillset, I am eager to pursue new study topics and continue building upon this positive experience.

Summary and Study Conclusions

The purpose of this qualitative multiple case study was to explore cybersecurity strategies in protecting critical infrastructure. The case organizations in the study represented critical infrastructure in the pacific northwest region of the United States. Data triangulation was performed using the interview and member checking data, and the organizational documents to help answer the study's research question. The data analysis phase of the study revealed four principal themes related to cybersecurity strategies in protecting critical infrastructure, which were (a) a robust workforce training program is crucial, (b) make infrastructure resiliency a priority, (c) importance of security awareness, and (d) importance of organizational leadership support and investment. These themes represent positive findings that help support successful cybersecurity strategies in protecting critical infrastructure. As reported by the U.S. House Permanent Select Committee on Intelligence (2014), sophisticated threats have demonstrated the motivation, access, and capability to attack our critical infrastructure with the intent of causing significant damage that degrades or denies our ability to provide basic services and resources such as power, water, and fuel.

References

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: an attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1). Retrieved from http://timreview.ca/article/861

Ahlmeyer, M., & Chircu, A. M. (2016). Securing the Internet of things: A review. *Issues in Information Systems, 17*(4). Retrieved from https://pdfs.semanticscholar.org/12bf/f696d912535ab235c4e67a1e72c39cef2fe2.pdf

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53-66. doi: 10.1016/j.ijcip.2014.12.002

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305,* 357-383. Retrieved from http://sameekhan.org/pub/A_K_2015_IS.pdf

Ali, P. A., & Johnson, S. (2017). Speaking my patient's language: Bilingual nurses' perspective about provision of language concordant care to patients with limited English proficiency. *Journal of Advanced Nursing*, *73*(2), 421-432. doi:10.1111/jan.13143

Allred, P. D., Maxwell, G. M., & Skrla, L. (2017). What women know: Perceptions of seven female superintendents. *Advancing Women in Leadership*, *37*, 1-11. Retrieved from http://scholarlycommons.pacific.edu/cgi/viewcontent.cgi?article=1092&context=e

d-facarticles

Almalki, M., Gray, K., & Sanchez, F. M. (2015). The use of self-quantification systems for personal health information: big data management activities and prospects. *Health Information Science and Systems*, *3*(S1), S1. doi: 10.1186/2047-2501-3-s1-s1

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information & Computer Security*, *26*(4), 420-436. doi:10.1108/ics-09-2017-0063

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*(3). Retrieved from http://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=6e937b5e-10c1-40ec-8b9f-09d448fffd38%40sessionmgr103

Asiamah, N., Mensah, H. K., & Oteng-Abayie, E. F. (2017). General, target, and accessible population: Demystifying the concepts for effective sampling. *Qualitative Report*, *22*(6), 1607. Retrieved from http://nsuworks.nova.edu/tqr/vol22/iss6/9

Auffret, J. P., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., . . . Warweg, P. (2017). Cybersecurity leadership: Competencies, governance, and technologies for industrial control systems. *Journal of Interconnection Networks*, *17*(01), 1740001. doi:10.1142/s0219265917400011

Baldi, M. (2016). Cybersecurity defense for industrial process-control systems. *Chemical Engineering*, *123*(7), 36.

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

Baxter, S., Muir, D., Brereton, L., Allmark, C., Barber, R., Harris, L., ... & Baird, W. (2016). Evaluating public involvement in research design and grant development: Using a qualitative document analysis method to analyse an award scheme for researchers. *Research Involvement and Engagement*, *2*, 13-13. doi:10.1186/s40900-016-0027-x

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy,* 169-217. doi:10.1086/259394

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research.*. Washington, DC: U.S. Department of Health and Human Services. Retrieved from https://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

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

Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. *Qualitative Research*, *15*(2), 219-234. doi:10.1177/1468794112468475

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

Bochkov, A., Lesnykh, V., Zhigirev, N., & Lavrukhin, Y. (2015). Some methodical aspects of critical infrastructure protection. *Safety Science*, *79*, 229-242. doi:10.1016/j.ssci.2015.06.008

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information & Computer Security, 23*(3), 317-332. doi:10.1057/9781137455550.0020

Bou-Harb, E., Lucia, W., Forti, N., Weerakkody, S., Ghani, N., & Sinopoli, B. (2017). Cyber meets control: A novel federated approach for resilient CPS leveraging real cyber threat intelligence. *IEEE Communications Magazine*, *55*(5), 198-204. doi:10.1109/MCOM.2017.1600292CM

Bowden, C., & Galindo-Gonzalez, S. (2015). Interviewing when you're not face-to-face: The use of email interviews in a phenomenological study. *International Journal of Doctoral Studies*, *10*(12), 79-92. doi:10.28945/2104

Brantingham, P. L., & Brantingham, P. L. (1993). Environment, routine and situation: Toward a pattern theory of crime. *Advances in Criminological Theory*, *5*(2), 259-94. doi:10.4324/9781315128788-12

Brilingaitė, A., Bukauskas, L., & Juozapavišius, A. (2019). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security, 88,* 101607. doi:10.1016/j.cose.2019.101607

Brown, A., & Danaher, P. A. (2017). CHE Principles: facilitating authentic and dialogical semi-structured interviews in educational research. *International Journal of Research & Method in Education*, 1-15. doi:10.1080/1743727x.2017.1379987

Brown, K. M., Elliott, S. J., Leatherdale, S. T., & Robertson-Wilson, J. (2015). Searching for rigour in the reporting of mixed methods population health research: A methodological review. *Health Education Research*, *30*(6), 811-839. doi:10.1093/her/cyv046

Busse, C., Kach, A. P., & Wagner, S. M. (2016). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods, 20*(4) 574-609. doi:10.2139/ssrn.2713980

Butler, A., Hall, H., & Copnell, B. (2016). A guide to writing a qualitative systematic review protocol to enhance evidence-based practice in nursing and health care. *Worldviews on Evidenced-Based Nursing, 13*(3), 241-249. doi:10.1111/wvn.12134

Cabrera, E. (2016). Protecting critical infrastructure from cyberattack. *Risk Management*, *63*(8), 32-33. Retrieved from https://ezp.waldenulibrary.org/login?qurl=https%3A%2F%2Fsearch.proquest.com%2Fdocview%2F1831184017%3Faccountid%3D14872

Candell, R., Zimmerman, T., & Stouffer, K. (2015). *An industrial control system cybersecurity performance testbed* (National Institute of Standards and Technologypaper 8089). Washington, DC: U.S. Department of Commerce. doi:10.6028/nist.ir.8089

Cassotta, S., & Sidortsov, R. (2019). Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North. *Energy Research & Social Science*, *51*, 129-133. doi:10.1016/j.erss.2019.01.003

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative Report, 21*(5), 811-831. Retrieved from http://nsuworks.nova.edu/tqr/vol21/iss5/2

Cedergren, A., Johansson, J., & Hassel, H. (2017). Challenges to critical infrastructure resilience in an institutionally fragmented setting. *Safety Science, 110,* 51–51. doi:10.1016/j.ssci.2017.12.025

Chaves, A., Rice, M., Dunlap, S., & Pecarina, J. (2017). Improving the cyber resilience of industrial control systems. *International Journal of Critical Infrastructure Protection*, 17, 30-48. doi:10.1016/j.ijcip.2017.03.005

Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394-402. doi:10.1016/j.chb.2017.03.061

Chowdhury, M. F. (2015). Coding, sorting and sifting of qualitative data analysis: Debates and discussion. *Quality & Quantity*, *49*(3), 1135-1143. doi:10.1007/s11135-014-0039-2

Cilluffo, F. (2016). *Emerging cyber threats to the United States* [Testimony before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies]. Washington, DC: George Washington Center for Cyber and Homeland Security. Retrieved from http://docs.house.gov/meetings/HM/HM08/20160225/104505/HHRG-114-HM08-Wstate-CilluffoF-20160225.pdf

Cintuglu, M. H., Mohammed, O. A., Akkaya, K., & Uluagac, A. S. (2017). A survey on smart grid cyber-physical system testbeds. *IEEE Communicatios Surveys & Tutorials*, 19(1), 446-464. doi:10.1109/comst.2016.2627399

Coffey, J. W., Haveard, M., & Golding, G. (2018). A case study in the implementation of a human-centric higher education cybersecurity program. *Journal of Cybersecurity Education, Research and Practice*, *2018*(1), 4. Retrieved from https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/4

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 588-608. doi:10.2307/2094589

Cohen, L., Kluegel, J., & Land, K. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review*, 505-524. doi:10.2307/2094935

Cong, H., Dang, D., Brennan, L., & Richardson, J. (2017). Information security and people: A conundrum for compliance. *Australasian Journal of Information Systems, 21,* 1-16. doi:10.3127/ajis.v21i0.1321

Cook, A., Janicke, H., Smith, R., & Maglaras, L. (2017). The industrial control system cyber defence triage process. *Computers & Security, 70*, 467-481. doi:10.1016/j.cose.2017.07.009

Cuevas, J., & Dawson, B. L. (2018). A test of two alternative cognitive processing models: Learning styles and dual coding. *Theory and Research in Education*, *16*(1), 40-64. doi:10.1177/1477878517731450

de Fuentes, J. M., González-Manzano, L., Tapiador, J., & Peris-Lopez, P. (2017). Pracis:

Privacy-preserving and aggregatable cybersecurity information sharing. *Computers & Security, 69,* 127-141. doi:10.1016/j.cose.2016.12.011

Denham, B. (2015). Three cyber-security strategies to mitigate the impact of a databreach. *Network Security*, *2015*(1), 5–8. doi:10.1016/s1353-4858(15)70007-3

DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, *35*(2), 291-300. doi:10.1007/s10669-015-9540-y

Dunn, M., Kaufmann, M., & Søby Kristensen, K. (2015). Resilience and (in) security: Practices, subjects, temporalities. *Security Dialogue*, *46*(1), 3-14. doi:10.1177/0967010614559637

Ebersold, K., & Glass, R. (2015). The impact of disruptive technology: The Internet of Things. *Issues in Information Systems, 16*(IV), 194-201. Retrieved from http://www.iacis.org/iis/2015/4_iis_2015_194-201.pdf

El Hussein, M., Jakubec, S. L., & Osuji, J. (2015). Assessing the FACTS: A mnemonic for teaching and learning the rapid assessment of rigor in qualitative research studies. *Qualitative Report*, *20*(8), 1182-1184. Retrieved from http://nsuworks.nova.edu/tqr/vol20/iss8/3

Elkhannoubi, H., & Belaissaoui, M. (2016). A framework for an effective cybersecurity strategy implementation. *Journal of Information Assurance & Security*, *11*(4). doi:10.1109/isda.2015.7489156

Esposito, G., & Freda, M. F. (2016). Reflective and agentive functions of narrative writing: A qualitative study on the narratives of university students. *Integrative*

Psychological and Behavioral Science, *50*(2), 333-357. doi: 10.1007/s12124-015-9323-5

Esteves, J., Ramalho, E., & De Haro, G. (2017). To improve cybersecurity, think like a hacker. *MIT Sloan Management Review*, *58*(3), 71. Retrieved from http://ilp.mit.edu/media/news_articles/smr/2017/58314.pdf

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *9*(17), 4667-4679. doi:10.1002/sec.1657

Fagerholm, F., Kuhrmann, M., & Münch, J. (2017). Guidelines for using empirical studies in software engineering education. *PeerJ Computer Science, 3*(1), 131-166. doi:10.7717/peerj-cs.131

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on Internet of Things. *International Journal of Computer Applications*, *113*(1). doi:10.5120/19787-1571

Federal Energy Regulatory Commission. (2008). Mandatory reliability standards for critical infrastructure protection. *Order*, *706*. Retrieved from https://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf

Ferdinand, J. (2015). Building organisational cyber resilience: A strategic knowledge-based view of cyber security management. *Journal of Business Continuity & Emergency Planning, 9*(2), 185-195. Retrieved from https://web-a-ebscohost-com.ezp.waldenulibrary.org/ehost/pdfviewer/pdfviewer?vid=1&sid=7c1b69f4-21f2-4557-824f-dbf6d29c6155%40sdc-v-sessmgr01

Fischer, E. A. (2016). *Cybersecurity issues and challenges: In brief* (Congressional Research Service Report 7-5700). Retrieved from https://pdfs.semanticscholar.org/65e3/4c9bb7330fcfec378394b5d308b6a323947d.pdf

Fischerkeller, M. P., & Harknett, R. J. (2017). Deterrence is not a credible strategy for cyberspace. *Orbis*, *61*(3), 381-393. doi:10.1016/j.orbis.2017.05.003

Fitzgerald, M. (2015). Gone fishing—for data. *MIT Sloan Management Review, 56*(3). Retrieved from http://ilp.mit.edu/media/news_articles/smr/2015/56315Wx.pdf

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A review on internet of things for defense and public safety. *Sensors, 16*(10), 1644. doi:10.3390/s16101644

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. doi:10.5590/JOSC.2018.10.1.02

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. Q*ualitative Report*, *20*(9), 1408. Retrieved from http://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=1049&context=sm_pubs

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

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. Security Studies, 24(2), 316-348. doi:10.1080/09636412.2015.1038188

Genge, B., Graur, F., & Haller, P. (2015). Experimental assessment of network design approaches for protecting industrial control systems. *International Journal of Critical Infrastructure Protection*, *11*, 24-38. doi:10.1016/j.ijcip.2015.07.005

Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, *10*, 3-17. doi:10.1016/j.ijcip.2015.04.001

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *Qualitative Report*, *20*(11), 1772.

Gergen, K. J. (2015). From mirroring to world-making: Research as future forming. *Journal for the Theory of Social Behaviour*, *45*(3), 287-310. doi:10.1111/jtsb.12075

Giorgi, A. (1997). The theory, practice, and evaluation of the phenomenological method as a qualitative research procedure. *Journal of Phenomenological Psychology*, *28*(2), 235-260. doi:10.1163/156916297x00103

Grady, C. (2015). Enduring and emerging challenges of informed consent. *New England Journal of Medicine*, *372*(9), 855-862. doi:10.1056/nejmc1503813

Grenier, R. S., & Dudzinska-Przesmitzki, D. (2015). A conceptual model for eliciting mental models using a composite methodology. *Human Resource Development*

Review, *14*(2), 163-184. doi:10.1177/1534484315575966

Guest, G., Namey, E., Taylor, J., Eley, N., & McKenna, K. (2017). Comparing focus groups and individual interviews: Findings from a randomized study. *International Journal of Social Research Methodology*, *20*(6), 693-708. doi:10.1080/13645579.2017.1281601

Gyunka, B. A., & Christiana, A. O. (2017). Analysis of human factors in cyber security: A case study of anonymous attack on Hbgary. *Computing & Information Systems, 21*(2), 10-18.

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security, 66,* 52-65. doi:10.1016/j.cose.2016.12.016

Harrell, M. (2017). Synergistic security: A work system case study of the target breach. *Journal of Cybersecurity Education, Research and Practice, 2017*(2) , Article 4. Retrieved from https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1027&context=jcerp

Harp, D., & Gregory-Brown, B. (2015). *The state of security in control systems today* [White paper]. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042

Harvey, L. (2015). Beyond member-checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education*, *38*(1), 23-38. doi:10.1080/1743727x.2014.914487

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

Hege, I., Dietl, A., Kiesewetter, J., Schelling, J., & Kiesewetter, I. (2018). How to tell a patient's story? Influence of the case narrative design on the clinical reasoning process in virtual patients. *Medical Teacher*, 1-7. doi:10.1080/0142159x.2018.1441985

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2017). Code saturation versus meaning saturation: How many interviews are enough? *Qualitative Health Research*, *27*(4), 591-608. doi:10.1177/1049732316665344

Hilt, D. W. (2018). Critical infrastructure protection required on electric grid continually changing. *Natural Gas & Electricity*, *34*(8), 9-15. doi:10.1002/gas.22040

Holland, J. M., Rozalski, V., Beckman, L., Rakhkovskaya, L. M., Klingspon, K. L., Donohue, B., ... & Gallagher-Thompson, D. (2016). Treatment preferences of older adults with substance use problems. *Clinical Gerontologist*, *39*(1), 15-24. doi:10.1093/med/9780199392063.003.0010

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2016). Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology*, 1-22. doi:10.1177/0306624x16679162

Horne, C. A., Maynard, S. B., & Ahmad, A. (2017). Organisational information security strategy: Review, discussion and future research. *Australasian Journal of Information Systems*, *21*. doi:10.3127/ajis.v21i0.1427

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

Hussein, A. (2015). The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of comparative social work*, *4*(1). Retrieved from https://www.researchgate.net/profile/Ashatu_Hussein/publication/260041595_The_use_of_Triangulation_in_Social_Sciences_Research_Can_qualitative_and_quantitative_methods_be_combined/links/551a7c270cf26cbb81a2df1e/The-use-of-Triangulation-in-Social-Sciences-Research-Can-qualitative-and-quantitative-methods-be-combined.pdf

Industrial Control Systems Cyber Emerency Response Team. (2016). *ICS-CERT annual assessment report FY 2016*. Washington, DC: National Cybersecurity and Communications Integration Center. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

Jacobs, P. C., von Solms, S. H., & Grobler, M. M. (2016). Towards a framework for the development of business cybersecurity capabilities. *The Business & Management Review*, *7*(4), 51. Retrieved from

https://cberuk.com/cdn/conference_proceedings/conference_40254.pdf

Joslin, R., & Müller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. *International Journal of Project Management*, *34*(6), 1043-1056. doi:10.1016/j.ijproman.2016.05.005

Kaba, A., Baumann, A., Kolotylo, C., & Akhtar-Danesh, N. (2017). A descriptive case study of the changing nature of nurses' work: The impact of managing infectious diseases requiring isolation. *American Journal of Infection Control*, *45*(2), 200-202. doi:10.1016/j.ajic.2016.06.036

Kallio, H., Pietila, 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. doi:10.1111/jan.13031

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection, 15,* 47-59. doi:10.1016/j.ijcip.2016.10.001

Karanasios, S., Allen, D., & Finnegan, P. (2015). Information systems journal special issue on: Activity theory in information systems research. *Information Systems Journal*, *25*(3), 309-313. doi:10.1111/isj.12061

Katina, P. F. (2015). Emerging systems theory–based pathologies for governance of complex systems. *International Journal of System of Systems Engineering*, *6*(1-2), 144-159. doi:10.1504/ijsse.2015.068806

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. doi:10.1108/jkm-08-2016-0353

Kim, S. Y., & Miller, F. G. (2015). Informed consent for pragmatic trials: The integrated consent model. *New England Journal of Medicine*, 370(8), 769-772. doi:10.1056/nejmhle1312508

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, *9*, 52-80. doi:10.1016/j.ijcip.2015.02.002

Kung, T. H., Richardson, E. T., Mabud, T. S., Heaney, C. A., Jones, E., & Evert, J. (2016). Host community perspectives on trainees participating in short-term experiences in global health. *Medical education*, *50*(11), 1122-1130. doi:10.1111/medu.13106

Kure, H., Islam, S., & Razzaque, M. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), 898. doi:10.3390/app8060898

Kuutti, K. (1991). Activity theory and its applications to information systems research and development. *Information Systems Research: Contemporary Approaches and Emergent Traditions*, 529-549.

Labaka, L., Hernantes, J., & Sarriegi, J. M. (2016). A holistic framework for building critical infrastructure resilience. *Technological Forecasting and Social Change, 103,* 21-33. doi:10.1016/j.techfore.2015.11.005

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431-40. doi:10.1016/j.bushor.2015.03.008

Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, *3*, 18-23. doi: 10.1016/j.mfglet.2014.12.001

Lee, K. B., & Lim, J. I. (2016). The reality and response of cyber threats to critical infrastructure: A case study of the cyber-terror attack on the Korea hydro & nuclear power co., ltd. *KSII Transactions on Internet & Information Systems*, *10*(2). doi:10.3837/tiis.2016.02.023

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, *72*, 26-59. doi:10.1016/j.cose.2017.08.005

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280. doi:10.1080/01639625.2015.1012409

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

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change*, *67*(1), 3-20. doi:10.1007/s10611-016-9645-3

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five

approaches. *Health promotion practice*, *16*, 473–475. doi:10.1177/1524839915580941

Li, J. Q., Yu, F. R., Deng, G., Luo, C., Ming, Z., & Yan, Q. (2017). Industrial internet: A survey on the enabling technologies, applications, and challenges. *IEEE Communications Surveys & Tutorials*. doi:10.1109/comst.2017.2691349

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. doi:10.1016/j.ijinfomgt.2018.10.017

Li, S., Tryfonas, T., & Li, H. (2016). The internet of things: A security point of view. *Internet Research, 26*(2), 337-359. doi:10.1108/intr-07-2014-0173

Liu, X., Dong, M., Ota, K., Yang, L. T., & Liu, A. (2016). Trace malicious source to guarantee cyber security for mass monitor critical infrastructure. *Journal of Computer and System Sciences,* 1-26. doi:10.1016/j.jcss.2016.09.008

Lloyd, J., & Hopkins, P. (2015). Using interviews to research body size: Methodological and ethical considerations. *Area*, *47*(3), 305-310. doi:10.1111/area.12199

Lošonczi, P., Nečas, P., & Naď, N. (2016). Risk management in information security. *Journal of Management*, (1), 28.

Luo, X. (2016). Security protection to industrial control system based on defense-in-depth strategy. *WIT Transactions on Engineering Sciences*, 113, 19-27. doi:10.2495/IWAMA150031

Maitra, A. K. (2015). Offensive cyber-weapons: Technical, legal, and strategic

aspects. *Environment Systems and Decisions*, *35*(1), 169-182. doi:10.1007/s10669-014-9520-7

Mandal, P. C. (2018). Trustworthiness in qualitative content analysis. *International Journal of Advanced Research and Development*, *3*(2), 479-485.

Mangelsdorf, M. E. (2017). What executives get wrong about cybersecurity. *MIT Sloan Management Review*, *58*(2), 22. Retrieved from http://web.mit.edu/smadnick/www/wp/2017-01.pdf

Massacci, F., Ruprai, R., Collinson, M., & Williams, J. (2016). Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers. *IEEE Security & Privacy*, *14*(3), 52-60. doi:10.1109/msp.2016.48

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology, 28*(1), 417-442. doi:10.1146/annurev.soc.28.110601.140752

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

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE, 104*(5), 1039-1057. Retrieved from http://web.mit.edu/smadnick/www/wp/2017-01.pdf

McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice, 31,* 30-52. doi:10.1177/1043986214552607

McQuaid, P., Britton, B., Minnich, M., Borrelli, D., Baker, J., & Burton, B. (2019).

University and government unite to address homeland cybersecurity issues. *Software Quality Professional*, *21*(3). doi:10.1109/ths.2018.8574161

Melewar, T. C., Foroudi, P., Dinnie, K., & Nguyen, B. (2017). The role of corporate identity management in the higher education sector: an exploratory case study. *Journal of Marketing Communications*, 1-23. doi:10.1080/13527266.2017.1414073

Mertens, P., & Barbian, D. (2015). Researching "grand challenges". *Business & Information Systems Engineering*, *57*(6), 391-403. doi:10.1007/s12599-015-0405-1

Mihelič, A., & Vrhovec, S. (2018). Obligation to defend the critical infrastructure? Offensive cybersecurity measures. *Journal of Universal Computer Science*, *24*(5), 646-661. Retrieved from https://pdfs.semanticscholar.org/9ece/464dd9338ad95dc05ae9039f37e692c598c7.pdf

Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, *14*(2), 5-10. Retrieved from http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf

Molina-Azorín, J. F. (2016). Mixed methods research: An opportunity to improve our studies and our research skills. *European Journal of Management and Business Economics, 25*(2), 37-38. doi:10.1016/j.redeen.2016.05.001

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative

inquiry. *Qualitative health research*, *25*(9), 1212-1222. doi:10.1177/1049732315588501

Murdock, H., de Bruijn, K., & Gersonius, B. (2018). Assessment of critical infrastructure resilience to flooding using a response curve approach. *Sustainability*, *10*(10), 3470. doi:10.3390/su10103470

Mursu, Á., Luukkonen, I., Toivanen, M., & Korpela, M. (2007). Activity theory in information systems research and practice: Theoretical underpinnings for an information systems development model. *Information Research, 12*(3), n3. Retrieved from https://files.eric.ed.gov/fulltext/EJ1104804.pdf

Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, *70*, 436-454. doi:10.1016/j.cose.2017.06.010

National Cybersecurity & Communications Integration Center & Federal Bureau of Investigation. (2016). *GRIZZLY STEPPE – Russian malicious cyber activity.* Retrieved from https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Orange, A. (2016). Encouraging reflexive practices in doctoral students through research journals. *Qualitative Report, 21*(12), 2176-2190. Retrieved from http://nsuworks.nova.edu/tqr/vol21/iss12/2

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 and*

Mental Health Services Research, *42*(5), 533-544. doi:10.1007/s10488-013-0528-y

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems*, *59*(3), 211-217. doi:10.1080/08874417.2019.1571459

Paté-Cornell, M. E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis*, *38*(2), 226-241. doi:10.1111/risa.12844

Paternoster, R., Jaynes, C. M., & Wilson, T. (2017). Rational choice theory and interest in the "fortune of others". *Journal of Research in Crime and Delinquency, 54*(6). doi:10.1177/0022427817707240

Paulus, T., Woods, M., Atkins, D. P., & Macklin, R. (2017). The discourse of QDAS: Reporting practices of ATLAS. ti and NVivo users with implications for best practices. *International Journal of Social Research Methodology*, *20*(1), 35-47. doi:10.1080/13645579.2015.1102454

Payette, J., Anegbe, E., Caceres, E., & Muegge, S. (2015). Secure by design: Cybersecurity extensions to project management maturity models for critical infrastructure projects. *Technology Innovation Management Review*, *5*(6), 26.

Pearson, M. L., Albon, S. P., & Hubball, H. (2015). Case study methodology: Flexibility, rigour, and ethical considerations for the scholarship of teaching and learning. *Canadian Journal for the Scholarship of Teaching and Learning*, *6*(3), 12. doi:10.5206/cjsotl-rcacea.2015.3.12

Perrotta, C. (2017). Beyond rational choice: How teacher engagement with technology is mediated by culture and emotions. *Education and Information Technologies*, *22*(3), 789-804. doi: 10.1007/s10639-015-9457-6

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

Petocz, A., & Newbery, G. (2016). Challenges in conducting and interpreting qualitative research. *Review of General Psychology, 17*(2), 216-223. Retreived from https://vuws.westernsydney.edu.au/bbcswebdav/pid-2142124-dt-content-rid-19505381_1/courses/100983_2016_1h/eContent/Week%207%20Challenges%20in%20qual%20research/4thYrRM16PetoczNewbery.pptslides.pdf

Pham, H. C., Pham, D. D., Brennan, L., & Richardson, J. (2017). Information Security and People: A Conundrum for compliance. *Australasian Journal of Information Systems*, *21*, 1-16. doi:10.3127/ajis.v21i0.1321

Piggin, R. (2018). Cyber resilience 2035. *ITNOW*, *60*(1). doi:10.1093/itnow/bwy014

Ponomarev, S., & Atkison, T. (2016). Industrial control system network intrusion detection by telemetry analysis. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 252-260. doi:10.1109/tdsc.2015.2443793

Popescul, D., & Radu, L. D. (2016). Data security in smart cities: Challenges and solutions. *Informatica Economica, 20*(1), 29. doi:10.12948/issn14531305/20.1.2016.03

Pursiainen, C. (2017). Critical infrastructure resilience: A Nordic model in the making?.

International Journal of Disaster Risk Reduction (Article in press). doi:10.1016/j.ijdrr.2017.08.006

Qassim, Q., Jamil, N., Abidin, I. Z., Rusli, M. E., Yussof, S., Ismail, R., . . . Daud, M. (2017). A Survey of SCADA Testbed Implementation Approaches. *Indian Journal of Science and Technology*, *10*(26). doi:10.17485/ijst/2017/v10i26/116775

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. doi:10.1016/j.giq.2015.02.001

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences*, *6*(2), 1-5. doi:10.4172/2162-6359.1000403

Ranney, M., Meisel, Z., Choo, E., Garro, A., Sasson, C., & Morrow Guthrie, K. (2015). Interview-based qualitative research in emergency care part II: Data collection, analysis, and results reporting. *Academic Emergency Medicine, 22*(9), 1103-1112. doi:10.1111/acem.12735

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119-1139. doi:10.1177/0306624x15572861

Reyns, B. W., Henson, B., & Fisher, B. S. (2015). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice, 32*, 148–168. doi:10.1177/1043986215621378

Rimando, M., Brace, A., Namageyo-Funa, A., Parr, T. L., Sealy, D.-A., Davis, T. L., . . . Christiana, R. W. (2015). Data collection challenges and recommendations for early career researchers. *Qualitative Report, 20*(12), 2025. Retrieved from https://nsuworks.nova.edu/tqr/vol20/iss12/8

Robert, B., Morabito, L., Cloutier, I., & Hémond, Y. (2015). Interdependent critical infrastructures resilience: Methodology and case study. *Disaster Prevention and Management, 24*(1), 70-79. doi:10.1108/dpm-10-2013-0195

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

Rousseau, D. (2015). General systems theory: Its present and potential. *Systems Research and Behavioral Science*, 32(5), 522-533. doi:10.1002/sres.2354

Russell, L., Goubran, R., Kwamena, F., & Knoefel, F. (2018). Agile IoT for critical infrastructure resilience: Cross-modal sensing as part of a situational awareness approach. *IEEE Internet of Things Journal*, *5*(6), 4454-4465. doi:10.1109/jiot.2018.2818113

Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access*, *4*,

1375-1384. doi:10.1109/access.2016.2549047

Sandelowski, M. (2000). Focus on research methods-whatever happened to qualitative description? *Research in Nursing and Health*, *23*(4), 334-340. doi:10.1002/1098-240x(200008)23:4<334::aid-nur9>3.0.co;2-g

Sapaty, P. S. (2016). Towards global goal orientation, robustness and integrity of distributed dynamic systems. *International Relations*, *4*(6), 418-425. doi:10.17265/2328-2134/2016.06.006

Sarstedt, M., Bengart, P., Shaltoni, A. M., & Lehmann, S. (2017). The use of sampling methods in advertising research: A gap between theory and practice. *International Journal of Advertising*, 1-14. doi:10.1080/02650487.2017.1348329

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Anonymising interview data: Challenges and compromise in practice. *Qualitative Research*, *15*(5), 616-632. doi:10.1177/1468794114550439

Seo, J., Bruner, M., Payne, A., Gober, N., & Chakravorty, D. (2019). Using virtual reality to enforce principles of cybersecurity. *Journal of Computational Science*, *10*(1). doi:10.22369/issn.2153-4136/10/1/13

Shackelford, S., Sulmeyer, M., Craig, A., Buchanan, B., & Micic, B. (2017). From Russia with love: Understanding the Russian cyber threat to US critical infrastructure and what to do about it (Kelly School of Business Research Paper 17-42). *Nebraska Law Review, 96.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2978305

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber

security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129. Retrieved from https://s3.amazonaws.com/academia.edu.documents/41883983/17_Paper_31121548_IJCSIS_Camera_Ready_pp._129-136.pdf?response-content-disposition=inline%3B%20filename%3DComparative_Analysis_of_Various_National.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20191216%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191216T035037Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=1141dc6a53dfedc77d37c3ce8f0017577ab7d4ebfbecac8662105a3c6c34461e

Shoemaker, D., Davidson, D., & Conklin, A. (2017). Toward a discipline of cyber security: Some parallels with the development of software engineering education. *EDPACS*, *56*(5-6), 12-20. doi:10.1080/07366981.2017.1404867

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

Sidhu, K., Jones, R., & Stevenson, F. (2017). Publishing qualitative research in medical journals. *British Journal of General Practise*, *67*(658), 229-230. doi:10.3399/bjgp17x690821

Simpson, A., & Quigley, C. F. (2016). Member checking process with adolescent students: Not just reading a transcript. *Qualitative Report*, *21*(2), 377. Retrieved

from http://nsuworks.nova.edu/tqr/vol21/iss2/12

Singh, A., & Hess, T. (2017). How chief digital officers promote the digital transformation of their companies. *MIS Quarterly Executive*, *16*(1). Retrieved from https://pdfs.semanticscholar.org/100e/616568ea2edcc558300b30d61ebe1fe8ece3.pdf

Skyttner, L. (1996). General systems theory: Origin and hallmarks. *Kybernetes*, 25(6), 16-22. doi:10.1108/03684929610126283

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

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. doi:10.1016/j.ijinfomgt.2015.11.009

Sorsa, M., Kiikkala, I., & Åstedt-Kurki, P. (2015) Bracketing as a skill in conducting unstructured qualitative interviews. *Nurse Researcher. 22*(4), 8-12. doi:10.7748/nr.22.4.8.e1317

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: Towards a 'digital criminology'? *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17-33. doi:10.5204/ijcjsd.v6i2.355

Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the US power grid. *Electricity Journal*, *30*(3), 30-35. doi:10.1016/j.tej.2017.02.006

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *Canadian Journal of Hospital Pharmacy*, *68*(3). doi:10.4212/cjhp.v68i3.1456

Tas, I. D., Yetkiner, A., & Ince, M. (2017). The analysis of articles related to curriculum and instruction field in educational researcher journal (2005-2016). *European Scientific Journal*, *13*(16). doi:10.19044/esj.2017.v13n16p305

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. doi:10.1080/13645579.2015.1019263

Thames, L., & Schaefer, D. (2016). Software-defined cloud manufacturing for industry 4.0. *Procedia CIRP*, *52*, 12-17. doi:10.1016/j.procir.2016.07.041

Turley, E. L., Monro, S., & King, N. (2016). Doing it differently: Engaging interview participants with imaginative variation. *Indo-Pacific Journal of Phenomenology*, *16*(1-2), 153-162. doi:10.1080/20797222.2016.1145873

Twining, P., Heller, R. S., Nussbaum, M., & Tsai, C. C. (2017). Some guidance on conducting and reporting qualitative studies. *Computers & Education*, 106, A1-A9. doi:10.1016/j.compedu.2016.12.002

Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. *Computer Law & Security Review* (in press), 1-26. doi:10.1016/j.clsr.2017.12.004

U.S. Department of Health and Human Services Office for Civil Rights. (2017). *Breach report*. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

U.S. House Permanent Select Committee on Intelligence. (2014, November 20). *Cybersecurity threats: The way forward* [Hearing]. Retrieved from Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security website: https://www.hsdl.org/?view&did=759985

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice*, *6*(5), 100-110. doi:10.5430/jnep.v6n5p100

Valentinov, V., & Chatalova, L. (2016). Institutional economics and social dilemmas: a systems theory perspective. *Systems Research and Behavioral Science*, *33*(1), 138-149. doi:10.1002/sres.2327

Vermeulen, P. (2015). *Failed to connect: An analysis of European decisiveness in cybersecurity policy* (Master's thesis). Retrieved from https://openaccess.leidenuniv.nl/bitstream/handle/1887/38208/2015-11-01%20Final%20Thesis%20(2)%20Petra%20Vermeulen%20s1555391.pdf?sequence=1

Vernon-Bido, D., Padilla, J. J., Diallo, S. Y., Kavak, H., & Gore, R. J. (2016). Towards modeling factors that enable an attacker. In *Proceedings of the Summer Computer Simulation Conference* (p. 46). Society for Computer Simulation International. doi:10.22360/summersim.2016.scsc.055

Vicary, S., Young, A., & Hicks, S. (2016). A reflective journal as learning process and contribution to quality and validity in interpretative phenomenological analysis. *Qualitative Social Work*. doi:10.1177/1473325016635244

Vinci, A., Rijo, R., de Azevedo Marques, J., & Alves, D. (2017). Development and proposal of a reference tool for semi-structured interviews for the characterization of the management in mental health networks. *Procedia Computer Science*, *121*, 511-518. doi:10.1016/j.procs.2017.11.068

von Bertalanffy, L., & Sutherland, J. W. (1972). General systems theory: Foundations, developments, applications. *IEEE Transactions on Systems, Man, and Cybernetics*, (6), 592-592. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4309376

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: analysis of attack-proneness of information systems applications. *Management Information Systems Quarterly*, *39*(1), 91–112. doi:10.25300/misq/2015/39.1.05

Wang, K., Du, M., Yang, D., Zhu, C., Shen, J., & Zhang, Y. (2016). Game-theory-based active defense for intrusion detection in cyber-physical embedded systems. *ACM Transactions on Embedded Computing Systems*, *16*(1), 18. doi:10.1145/2886100

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review, 31*(5), 618-627. doi:10.1016/j.clsr.2015.07.002

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

Weisburd, D. (2015). The law of crime concentration and the criminology of place. *Criminology*, *53*(2), 133-157. doi:10.1111/1745-9125.12070

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: an

exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*. doi:10.1016/j.cose.2018.02.001

Welsh, B. C., Zimmerman, G. M., & Zane, S. N. (2018). The centrality of theory in modern day crime prevention: Developments, challenges, and opportunities. *Justice Quarterly*, *35*(1), 139-161. doi:10.1080/07418825.2017.1300312

Williams, C., Asi, Y., Raffenaud, A., Bagwell, M., & Zeini, I. (2016). The effect of information technology on hospital performance. *Health Care Management Science*, *19*(4), 338-346. doi: 10.1007/s10729-015-9329-z

Williams, M. L. (2015). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology, 56*, 21–48. doi:10.1093/bjc/azv011

Wirtz, B. W., & Weyerer, J. C. (2017). Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats. *International Journal of Public Administration*, *40*(13), 1085-1100. doi:10.1080/01900692.2016.1242614

Wolf, M., & Serpanos, D. (2017). Safety and security of cyber-physical and internet of things systems [Point of View]. *Proceedings of the IEEE*, *105*(6), 983-984. doi:10.1109/jproc.2017.2781198

Wolf, S. M., Clayton, E. W., & Lawrenz, F. (2018). The past, present, and future of informed consent in research and translational medicine. *Journal of Law, Medicine & Ethics*, 46, 7-11. doi:10.1177/1073110518766003

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam,

and Stake. *Qualitative Report*, *20*(2), 134-152.

Yeo, L. H., Abualkibash, M., Banfield, J., & Ashur, S. (2018, May). Infrastructure challenges in an information assurance education: An implementation case. In *2018 IEEE International Conference on Electro/Information Technology* (pp. 0583-0588). IEEE. doi:10.1109/eit.2018.8500236

Yeoh, W., & Popovič, A. (2016). Extending the understanding of critical success factors for implementing business intelligence systems. *Journal of the Association for Information Science and Technology*, *67*(1), 134-147. doi:10.1002/asi.23366

Yoon, J., Dunlap, S., Butts, J., Rice, M., & Ramsey, B. (2016). Evaluating the readiness of cyber first responders responsible for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *13*, 19-27. doi:10.1016/j.ijcip.2016.02.003

Young, D., Lopez J. Jr., 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. doi:10.1016/j.ijcip.2016.04.001

Young, J. C., Rose, D. C., Mumby, H. S., Benitez-Capistros, F., Derrick, C. J., Finch, T.,. . . Parkinson, S. (2018). A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution*, *9*(1), 10-19. doi:10.1111/2041-210x.12828

Zainal, Z. (2017). Case study as a research method. *Jurnal Kemanusiaan*, *5*(1). Retrieved from http://www.jurnal-

kemanusiaan.utm.my/index.php/kemanusiaan/article/viewFile/165/158

Zhu, K., He, X., Xiang, B., Zhang, L., & Pattavina, A. (2016). How dangerous are your smartphones?: App usage recommendation with privacy preserving. *Mobile Information Systems*, 2016, 1-10. doi:10.1155/2016/6804379

Appendix A: Interview Protocol

Interview: Exploring Industry Cybersecurity Strategy in Protecting Critical Infrastructure

Eligibility Criteria

Eligibility criteria will be used to identify potential interview participants. Participants will represent experience in cybersecurity related to critical infrastructure environments as managers and/or practitioners whose daily activities entail functions of compliance, training, auditing, technical and non-technical controls. To be selected, the candidate must satisfy at least two of the three eligibility criteria, which included:

a. IT or compliance professional with responsibilities associated with critical infrastructure services/functions;
b. Two or more years of cybersecurity experience as a manager or practitioner;
c. Prior or current knowledge of cybersecurity strategy/implementation in critical infrastructure.

Interview Script

1. Introduce myself and thank the participant.

   Good morning or evening. Thank you for participating in this study as an interview participant.

2. Confirm the participant's informed consent and address questions and/or concerns.

   I would like to discuss the consent form, and ask if you would like a signed copy. The main points of the consent are to ensure you understand this interview is voluntary, you can stop the interview at any time, and the

interview will be conducted in a manner to ensure no harm to the participant and the researcher.

3. Verify the interview procedure concerning audio recording and the steps I will take to protect the participant's privacy, and the confidentiality of the material.

   The interview will be audio recorded and I will take written notes. The interview will be limited to one hour. Inform the participant that I will not use any identifying information to include their name, address, organization name, and location. Explain how the files containing the interview material will be password protected and material storage (e.g. thumb drive, hard copy) will be stored in a locked container with access by the researcher only.

4. Confirm the participant is ready to begin the interview. Allow for a short break, if necessary, and if a break is taken then ask to agree upon a time to return from a break.
5. When the participant is ready, begin the audio recording. State the date and time, participant's assigned identification number for the study, and whether this is the initial or follow up interview.
6. Start the interview by asking the first question and continue until the final question. Once the participant has indicated he/she has answered the question, and does not have additional responses, proceed to ask additional questions based upon the participant's answer, if applicable. If an additional clarifying question is not needed, then proceed to the next interview question.

A. What is your current work role?

B. What is your experience either, direct or indirect, with cybersecurity or compliance functions?

C. What are the tools and techniques used in cybersecurity or compliance? How would you describe the usefulness of those tools and techniques?

D. What has prompted the need for cybersecurity or compliance strategy based upon your experience?

E. What have you found to be most effective in cybersecurity, compliance, or training strategies? What strategies have you found to be ineffective?

F. What impact has cybersecurity, compliance, or training practices had upon one another based upon your experience?

G. What factors play a role in the decision of how to implement cybersecurity, compliance, or training practices based upon your experience?

H. What are the advantages and disadvantages of workplace cybersecurity or compliance practices in your experience?

I. What are the advantages and disadvantages of workplace training programs in your experience?

J. What internal and external lessons learned based upon your experience can you discuss in deciding which practices to consider?

K. What other considerations would you like to discuss regarding cybersecurity, compliance, or training strategies?

L. What suggestions or recommendations might you have for questions to add or remove?

M. Do you have a recommendation for one or more candidates to interview?

7. Ask the participant if they want to share any more information about the topics.
8. Ask the participant if they are aware of any documentation that might be relevant to the topics discussed.
9. Explain the concept of member checking and schedule a follow-up interview to review my interpretations with them.
10. Stop audio recording.
11. Thank the participant for partaking in the study. Confirm the participant has my contact information for any follow up questions and concerns.

Appendix B: Training Certificate from the National Institute of Health Office of Extramural Research

Certificate of Completion

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

Date of Completion: 03/10/2017

Certification Number: 1623717

NIH National Institutes of Health
Office of Extramural Research