Understanding Influence Factors in Cyber Resiliency Adoption: A Mixed Methods Study of Cybersecurity Leaders

by

Travis Duane Howard

A Dissertation Presented in Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy, Cyber Leadership

CAPITOL TECHNOLOGY UNIVERSITY

October 2023

UNDERSTANDING INFLUENCE FACTORS IN CYBER RESILIENCY ADOPTION: A MIXED METHODS STUDY OF CYBERSECURITY LEADERS

Approved:

Christopher Mitchell, Ph.D., Chair

Jose de Arimateia da Cruz, Ph.D., Committee Member

Richard Baker, Ph.D., FRAeS, External Examiner

Ian R. McAndrew, Ph.D. FRAeS, Committee Member

Accepted and Signed:

Christopher P. Mitchell, PhD 10/24/2023 | 10:31 AM PDT

Christopher Mitchell, Ph.D. Date

Jose de Arimateia da Cruz, PhD/MPH 10/24/2023 | 10:51 AM PDT

Prof. Jose de Arimateia da Cruz, Ph.D. Date

Richard Baker 10/24/2023 | 1:37 PM PDT

Richard Baker, Ph.D., FRAeS Date
External Examiner

Ian McAndrew 10/24/2023 | 2:15 PM PDT

Ian R. McAndrew, Ph.D., FRAeS Date
Dean of Doctoral Programs
Capitol Technology University

Abstract

National-level cyber resiliency continues to be a critical shortcoming in national defense, particularly in protecting critical infrastructure. Despite significant advances in technology, governance, and frameworks, organizational adoption of cyber resiliency remains a challenge for many public and private sector organizations, particularly within U.S. critical infrastructure sectors. The purpose of this mixed-method research study was to better understand the innovation-decision process for cyber resiliency, and what influences affect adoption or rejection of cyber resiliency innovations at the organizational leadership level. The researcher designed a mixed methods study by which quantitative and qualitative phenomenological data was collected through an online survey instrument and augmented with experiential interviews using a target population of mid-senior, director, and executive level cybersecurity professionals in the United States. The results were interpreted using a test of statistical significance triangulated with phenomenological analysis and representation of the qualitative data both in the survey instrument and interview process. Quantitatively, the results of each binary logistic regression were not significant, indicating that the enabling factors and limiting factors respectively did not significantly predict the odds of adopting the cyber resiliency program. Qualitatively, the phenomenological data presented evidence that organizational influences, such as governance models, management of risks, leadership buy-in, innovativeness, and established policies and procedures represented significant influences on cyber resiliency adoption in an organization.

Keywords: cyber, resilience, cybersecurity, leadership, diffusion, innovation

DEDICATION

To the men and women of the United States Armed Forces, at home and aboard, standing the watch twenty-four hours a day, seven days a week, in defense of the nation, her citizens, democracy, and liberty. “The price of freedom is eternal vigilance.”

To the “cyber-watchers on the wall,” cybersecurity practitioners everywhere who hold the line against criminal and nation-state threats alike, often working thanklessly to keep their organization’s information secure and engaged every day in the “cyber fight” that remains nearly invisible to daily life. You inspire me.

To my wife, Rachel, for her tireless support, unconditional love, and encouragement to complete my research. Together, we do hard things.

To my mother, Diane, who raised a boy to reach for things far beyond his station.

ACKNOWLEDGMENT

This manuscript would not have been possible if not for the support and encouragement of many people in my life. First and foremost, my wife, Rachel, for ensuring I stuck with it even when it seemed certain that I would have to put my studies on hold to attend to our busy life. We achieve the things in our life because we are not just partners, we are a team. If they could read this, I would also acknowledge our many dogs and cats for keeping me grounded and providing an outlet for stress relief when it was needed most (even if they caused some of it); sometimes we are just trying to be the person our pets think we are!

A special thanks to the mentors I've had throughout my career up to this point, who inspired me and offered counsel when I needed it (and if I knew I needed it or not): Rear Admiral Danelle Barrett, U.S. Navy (ret.); Vice Admiral Brian Brown, U.S. Navy (ret.); Vice Admiral Nancy Norton, U.S. Navy (ret.); Nicole Dean, CISO of Accenture Federal Services; Captain James "Geno" Autrey, U.S. Navy (ret.) and Programs Director in the Office of Legislative Affairs; Dr. Jose de Arimateia da Cruz, my co-author of several publications, my academic mentor, and who graciously donated his time to join my dissertation committee and encouraged success; there are many more who influenced and guided me, but I don't have the space on the page.

Finally, I must thank Capitol Technology University and my advisor, Dr. Chris Mitchell as well as the Dean of Doctoral Programs, Dr. Ian McAndrew, for giving me the freedom, encouragement, and academic framework to produce my best work.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

The threats to organizations operating within cyberspace are vast: cyber-attacks are becoming more costly year-over-year, new methods of denial, disruption, and espionage continue to proliferate, and defensive strategies remain inadequate (Nye, 2022). While much of the attention of cybersecurity leaders, and indeed much of the technical and scholarly literature, have been devoted to prevention and detection techniques for information systems (IS) and industrial control systems (ICS), the concept of cyber resiliency – the ability of a system to operate under adverse conditions or stress – has begun to diffuse throughout communities-of-practice and industries as a complimentary security innovation focused on recovery and operational integrity (Kott & Linkov, 2021). Given the volume of cyber-attacks in recent years, calls for building cyber resilience into cyber-physical, industrial control, and information systems have increasingly appeared in professional and scholarly journals, government reports, and mass media. Recent national cyber strategy documents from the last two U.S. Presidents have declared cyber resiliency a central concept in defending the United States' critical infrastructure from cyber-attack, preserving peace and security within the U.S. and its allies, and, ultimately, the continued prosperity of the American economy (U.S. [Executive] Office of the President of the United States [EOP], 2018; 2021).

This study explored challenges, opportunities, and gaps in applying cyber resiliency as an innovation at the organizational leadership level. The goal was to better understand cyber resiliency adoption influence factors, specifically enablers, and limitations, based on the diffusion of innovations theory and, within that theory, the five-step innovation-decision process. Chapter 1 introduces this study. The background

section contains a presentation of the available literature and provides historical and global context, as well as how cybersecurity and cyber-resiliency are complementary capabilities within an organization's cyber-defense strategy. Chapter 1 also presents the research purpose, significance, nature and design, theoretical framework, research questions, assumptions, and limitations, and the chapter concludes with an outline of the remaining chapters.

Background of Study

The rapid expansion of digital and artificial environments, and the impact it has had on society, has been significant. The internet started as a small network of academic and research institutions that has grown from four sites to hundreds of thousands worldwide (Diamond & Bates, 1995). As of November 2021, the world wide web contained 4.36 billion pages of information, with the estimated size of Google's total index in the tens of trillions (WorldWideWebSize.com, 2021). In the digital age, the internet and the world wide web have given way to the term "cyberspace," described as a global domain of interdependent networks and information technology structures (CNSS 4009, 2015). Cyberspace has become an essential societal domain, an interconnected platform of platforms for global communication, information sharing, and economic prosperity measured in billions of U.S. dollars annually (Li & Liu, 2021).

Consider a comparison of cyberspace to the Earth's maritime domain. Nearly 80 percent of U.S. export trade, and 95 percent of the world's total commerce, move across the world's oceans (Wicker & Hendrix, 2018). The maritime domain is a vast interconnected network of oceans, waterways, tributaries, canals, and other naturally occurring or manufactured systems, while cyberspace is an interconnected digital domain

of networks and information systems (CNSS 4009, 2015). Ships navigate the seas, protecting the crew and cargo against natural elements or perilous situations such as maritime piracy or military actions. Most large sea-going vessels, such as container ships, cruise ships, and warships, establish resiliency using watertight compartments, damage control systems such as fire suppression and water pumps, and human repair teams that work to keep the ship afloat even when significantly damaged (Cutler, 2019).

As with ships plying the seas in support of their trade, so, too, is cyberspace used to transport information between disparate data nodes for information sharing, commerce, and even nation-state business, and its crews and cargo must likewise be protected from unique threats within cyberspace. The human workforce defending cyberspace is vast and growing: as of 2021, the information security profession boasts a workforce of practitioners that numbers just over four million people globally, over 30 specializations, and over 50 often-used role titles (International Information System Security Certification Consortium, Inc. [$(ISC)^2$], 2021). However, despite the rapid growth and maturity of the workforce, according to leading cyber threat intelligence firm CrowdStrike (2021), cybersecurity practitioners are increasingly challenged by cybercrime threat actors that continue to find success and profit through intrusions, ransomware, data theft, and extortion techniques.

Twenty-first-century geopolitical conflicts will continue to involve cyber warfare, and a nation's critical infrastructure are targets of interest for cyber-attack (Robinson, Jones, & Janicke, 2015; U.S. Cyberspace Solarium Commission [CSC], 2020). The existence of "gray-zone conflict" ensures non-combatant organizations, such as those supplying citizen services within critical infrastructure sectors, face nation-state-level

cyber threats that are highly resourced. Compared to basic cybersecurity protections such as commercial-level boundary and network intrusion detection and prevention tools, these threats pose an existential threat to non-combatant organizations and their ability to provide acceptable service availability (Carment & Belo, 2020).

Often a misunderstood concept, cyber resiliency focuses on operating through and recovering from disruption and is different from traditional cyber risk management (Linkov & Kott, 2019; Kott & Linkov, 2021). Resiliency is a key capability for organizations that require high degrees of availability (sometimes described as "up-time" by practitioners), even when under duress, and compliments traditional cybersecurity controls that protect confidentiality and integrity of information systems; critical infrastructure "lifeline" sectors are particularly important to establish resiliency: electricity, water, transportation, communications services, and financial services (M. et al., 2018). Although often technical in nature, cyber resiliency can also be described in the context of organizational resilience, whereby the organization absorbs and adapts to the challenges faced to continue performing and even thrive despite those challenges (Kott & Linkov, 2019; Barasa et al., 2018; Butler & Brooks, 2021; Carayannis et al., 2021; Sharkov, 2020).

The U.S. National Institute for Standards and Technology (NIST) has published technical and organizational standards, processes, and frameworks that assist cybersecurity practitioners in performing their roles as engineers, architects, managers, and executive leaders in developing, securing, and operating cyberspace-connected information systems. A primary reference for systems security engineers in the United States is the NIST 800 series of Special Publications (SP). NIST SP 800-37, *Risk*

Management Framework for Information Systems and Organizations, as well as NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, have become part of the official security standards of the U.S. Government, and the de-facto standard for thousands of public and private organizations in the United States (U.S. National Institute for Standards and Technology [NIST], 2021).

According to NIST SP 800-160 Volume 2, *Developing Cyber-Resilient Systems*, a system is considered cyber resilient when it "provides a degree of cyber resiliency commensurate with the system's criticality" (NIST, 2021, p. 3). Appendix D of the same publication describes several techniques that correspond to various technologies and processes comprising "cyber resilient" capabilities, including adaptive response, analytic monitoring, contextual awareness, coordinated protection, deception, diversity of modes, dynamic positioning, non-persistence, privilege restriction, realignment, redundancy, segmentation, substantiated integrity, and unpredictability (NIST, 2021, pp. 89-91). These techniques, along with the defined goals of *anticipating, withstanding, recovering, and adapt*ing, can be applied to a system, mission/business process, and organizational levels to address resiliency across the organization's risk management strategy (NIST, 2021, p. 85).

The national imperative to integrate cyber resiliency capabilities into the national cyber defense strategy of the United States has been made clear in numerous recent publications and reports. Testimony from the U.S. Office of the Director of National Intelligence to the U.S. Senate Select Committee for Intelligence succinctly and publicly summarizes the assessment of the U.S. Intelligence Community (IC) by describing how both state and non-state cyber actors threaten the critical infrastructure of the United

States, and hold U.S. and allied democracies' interests in cyberspace at risk domestically and internationally (U.S. Office of the Director of National Intelligence [ODNI], 2022, pp. 4-5). China, Russia, Iran, and North Korea were all described in the report as involved in disruption, denial, influence, and espionage operations against U.S. and U.S.-affiliated nations (ODNI, 2022, pp. 8-15). Government agencies and the industrial base are not the only targets:

> "U.S. Government entities, businesses, and other organizations face diverse ransomware threats. Attackers are innovating their targeting strategies to focus on victims whose business operations lack resilience or whose consumer base cannot sustain service disruptions, driving ransomware payouts up" (ODNI, 2022, p. 24).

Based on the danger to national security that a lack of cyber resiliency has shown, this research problem is significant to national security, homeland security, and defense communities. It is of value to critical infrastructure sectors requiring higher levels of cyber resiliency to ensure stable services to the population (M. et al., 2018). Additionally, this research is important for senior information security leaders in all organizations who desire a methodical, researched model to adopt resiliency that addresses organizational factors that leaders face when considering an innovative approach or technology for investment.

Problem Statement

National-level cyber resiliency continues to be a critical shortcoming in national defense, particularly in protecting critical infrastructure (U.S. Cyberspace Solarium Commission, 2020). Promoting and building cyber resiliency throughout the national

economy, and critical infrastructure specifically, is a critical factor in establishing deterrence in cyberspace where the chance of widespread system failure has been reduced to a level so as not to make those systems enticing targets for disruption (Nye, 2022). Although cybersecurity and cyber response actions are becoming better understood throughout the public and private sectors, “little is known” about techniques, designs, and implementation of cyber resilience (M. et al., 2018, p. 1).

As noted by the Department of Homeland Security’s (DHS) Cyber Resilience and Response (CRR) Team (2018), cyber resiliency awareness is lacking at the senior decision-maker levels within public and private sector critical infrastructure organizations (M. et al., 2018, p. 36). This observation led to the report's recommendation to find ways to increase public and private sector decision-makers' awareness and understanding of cyber resiliency and its necessity to protect U.S. sovereignty and national security and prevent debilitating attacks against critical infrastructure (M. et al., 2018, p. 36).

Despite significant advances in technical frameworks and modeling and an increasingly robust regulatory environment, organizational adoption of cyber resiliency – particularly in critical infrastructure sectors – continues to lag (M. et al., 2018; U.S. Cyberspace Solarium Commission, 2020). Technical and operational standards guide engineers and managers in implementing cyber resiliency into existing and future system designs. However, before such standards are even adopted, cybersecurity leaders at the senior, director, and executive levels (Chief Information Security Officers, Line-of-Business Information Security Officers, Directors, and similar roles of seniority and influence in a security organization) must navigate complex organizational leadership challenges – physical and technical, informational, cognitive, and social – to adopt cyber

resiliency capabilities (Linkov & Kott, 2019; Keys & Shapiro, 2019). While security professionals understand the risks and imperatives, convincing senior business leaders and boards of directors requires a careful approach that includes communicating risks, costs, and benefits and raising awareness of cyber threats at the executive level.

To better understand these factors, the researcher collected data from a sample of senior, director, and executive-level cybersecurity professionals through an internet-based survey instrument. The data from the survey, correlated with in-depth interviews of human subjects with cyber resiliency implementation experience, was analyzed to understand better innovation-decision influences that led to the adoption or rejection of cyber resiliency in any organization's information security and defensive cyber operations program.

Purpose of Study

This study's purpose was to understand the innovation-decision process for cyber resiliency better and what influences affect the adoption or rejection of cyber resiliency innovations at the organizational leadership level. The method used for this study involved mixed methods, in which the researcher conducted a qualitative internet-based survey of senior-level cybersecurity professionals on cyber resiliency adoption within their organizations, and was further augmented with in-depth interviews of chosen survey participants at the senior levels of cybersecurity decision-making (Creswell & Creswell, 2018).

The researcher used interviews to collect experiential data through shared lived experiences of the individuals who have navigated complex leadership factors, both supportive and inhibitive, that led to an adoption decision for cyber resiliency effects.

Correlating quantitative data with qualitative phenomenological data offered a rich collection of generalized (sample size) and specific (lived experiences) data on how the research subjects within their organizations experienced influences upon cyber resiliency innovation adoption. The mixed-method design is appropriate for a study that involves diffusion of innovations theory as the theoretical framework based on the established research traditions documented in Rodgers (2003). Past studies involving this theory, often referred to as "diffusion studies," have used qualitative research methods that have included "technological innovations, information, and uncertainty" as it relates to social change in a group or community (Rodgers, 2003, p. 12).

In performing this study, the researcher adopted a pragmatic worldview, whereby the objective was to rely as much as possible on the data gathered from the participants and their communicated process for the adoption of cyber resiliency (Creswell & Creswell, 2018). This worldview emphasizes the research problem and solutions, using pluralistic approaches to derive knowledge and applications to understand and potentially solve the problem at the center. Collecting diverse data types best provides a complete understanding of the research questions, and the researcher is not committed to any system or philosophy of understanding reality (Creswell & Creswell, 2018, pp. 10-11).

The researcher sampled a diverse population of senior, director, and executive-level information security professionals located in the United States of America. $(ISC)^2$ (2021) estimates the number of cybersecurity professionals in the United States to be over 1.14 million in 2021 (p. 5). As the total population studied is large, complex, and varied, the researcher used non-probability purposive sampling to derive a suitable sample. Purposive sampling is used when selecting participants based on traits or specific

characteristics (Nardi, 2018, pp. 126-127). The G*Power software was used to calculate sample size based on past studies of comparable design and necessary power to achieve statistical significance. The qualitative sample size for in-depth interviews leveraged the quantitative sample and was collected simultaneously to enrich the quantitative data and provide a greater understanding. The researcher leveraged personal and professional networks of cybersecurity leaders through social media, organizational memberships, professional associations, and communities of practice to achieve the sample size.

Research variables can be constant, unvarying, fixed in meaning, or subjective, with multiple values representing variability (Nardi, 2018, p. 48). The constant variable in this study is the seniority of the participants and their experience level with cyber resiliency concepts and capabilities within their organization. The fundamental subjective construct in this study was influences upon the innovation-decision process, operationalized by using a Likert scale within the quantitative survey questionnaire.

Significance of the Study

The results of this study have the potential to develop increased awareness and understanding of cyber resiliency and adoption methodology amongst organizational decision-makers. As the DHS CRR Team concluded, "the first step on the path to cyber resilience begins with an awareness and understanding of cyber resilience and what it can do to withstand such attacks," and that "the level of awareness and understanding among decision-makers… is very low today" (M. et al., 2018, p. 36). The deeper understanding produced from this study can be applied to any organization or industry vertical. However, it would be fascinating to critical infrastructure in which cyber resiliency is of significant value to the nation. To date, a convergent mixed method study on influences

in adopting cyber resiliency has not been conducted in cybersecurity leadership; to the researcher's knowledge, after an extensive review, very few diffusion studies have been completed within the cybersecurity leadership, policy or risk management research fields. This study presents an original and significant contribution to the body of research.

Furthermore, this study holds significance for U.S. national defense and national security. Within the U.S. Cyberspace Solarium Commission report of 2020, Co-chairmen Senator Angus King (I-Maine) and Representative Mike Gallagher (R-Wisconsin) described cyber resiliency as an essential pillar to deterring aggressors in cyberspace (p. v). Promoting and enabling national cyber resiliency denies the benefits of cyber-attacks by creating a "capacity to withstand and quickly recover from attacks that could cause harm or coerce, deter, restrain, or otherwise shape U.S. behavior" (p. 4). As noted in the National Cyber Strategy of the United States (2018), increasing the resilience and security of information and information systems is a central strategic objective and described as the first of four pillars leading to protecting the nation's national security and promoting the prosperity of the American people (EOP, 2018).

The findings of this study, and the resulting adoption model, will enable organizations central to the nation's cyber strategy to understand better leadership factors leading to the adoption of cyber resiliency. A diffusion study focusing on cyber resiliency has, to the researcher's awareness based on extensive review, not been performed until now. By focusing this study on producing an innovation-decision process model, the researcher hopes that the study's significance aligns with national-level priorities for cyber defense, and makes an original and meaningful contribution to the discipline of

cybersecurity leadership, the collective body of innovation-diffusion research, and the national cyber strategy of the United States.

Finally, this study has implications for future research into cyber resiliency specifically, but also cybersecurity leadership as a wider field of study. There is a notable gap in studies that employ the diffusion of innovations theory that explores information security through the lens of dissemination science – how practices, programs, and policies can be communicated within a social system to influence potential adopters and implementers (Dearing & Singhal, 2020, pp. 308-309). This gap can be addressed by additional studies that focus on new directions in diffusion research, particularly in the implementation of innovations within organizations and industry verticals, that will also assist policymakers in crafting public-private partnerships and government regulations to improve national cyber defense and align to national security priorities.

Nature of Study

This study followed a convergent mixed-methods research design, whereby a statistical analysis of survey data is combined with the lived experiences that a select group of human subjects (participants) experienced with deciding whether to adopt or reject cyber resilience within their organizations. The methodology involved a quantitative approach through an internet-based survey of senior, director, and executive level information security professionals (collectively described as "cybersecurity leaders"), a qualitative approach of in-depth interviews of senior and executive level organizational leaders, followed by correlational analysis. By analyzing the data gathered from this research method, the researcher could understand the conditions, organizational

characteristics, and adoption criteria conducive to a favorable innovation-adoption decision of cyber resiliency concepts.

This mixed-methods design is best suited for research involving the diffusion of innovations theory and follows the diffusion study research tradition. Such studies have become the hallmark of diffusion research, as noted by Rodgers (2003) in reviewing thousands of diffusion research studies in which socioeconomic, political, and organizational factors persist. A purely-quantitative design would be inappropriate for a study of this nature, given the socio-political factors rooted in the social sciences and tangential research interest in leadership theories as they relate to technology innovation adoption. Quantitative study methodology with experimental or quasi-experimental designs and applied behavior analysis for human subjects were out of the scope of this study (Creswell & Creswell, 2018).

A mixed-method study that involves both quantitative (survey) and qualitative (interviews), followed by correlational analysis drawn from lived experiences, combined with the researcher's professional expertise and worldview, allowing for a richer data set and more credible conclusions from this study. Additionally, the methodology focusing on survey data through an internet-based survey of senior cybersecurity professionals, combined with qualitative research through in-depth interviews, accomplished the researcher's goal of developing an understanding of successful cyber-resilience adoption from various perspectives and lived experiences. The data collected from the participants presented a view of characteristics and conditions conducive or limiting to adopting cyber resiliency within an organization's cyber defense strategy.

Hypothesis and Research Questions

In this non-experimental, convergent mixed-methods study investigating cyber resiliency adoption in organizations using the diffusion of innovations theory, the researcher investigated the innovation-decision process for cyber resiliency through a quantitative survey and qualitative interviews of senior, director, and executive level information security professionals ("cybersecurity leadership"). The goal was to understand the statistical significance of the data and converge the quantitative survey results with qualitative in-depth interviews of selected participants with cyber resiliency experience in their current or past organization to answer the research questions. The researcher focused on two research questions for this study:

1. [RQ1] What factors limit the adoption of cyber resiliency in an organization ("limiters")
2. [RQ2] What factors support the adoption of cyber resiliency in an organization ("enablers")

In a two-directional (two-tailed) positive hypothesis (H_α), the researcher posited that there is a statistical relationship between influence factors on cybersecurity leadership and cyber resiliency adoption. Conversely, the null hypothesis (H_0) states that no statistical relationship exists between influence factors on cybersecurity leadership and cyber resiliency adoption. Table 1 summarizes the variables for the study.

Table 1

Variables

Variable	Independence	Measurement	Survey Items
Demographics (De)	Independent	Nominal	De1 through De7
Organizational (O)	Independent	Nominal/Ordinal	O1 through O8
Influences (I)	Independent	Ordinal	I1 through I9

Decision (Di)	Dependent	Nominal	Di1

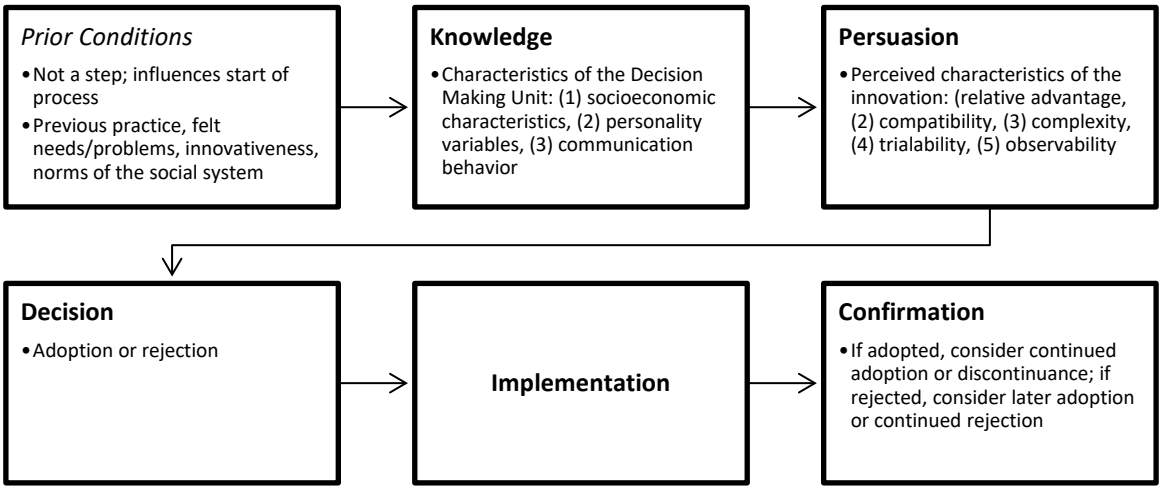
The first research question centered on limitations or challenges that would restrict or prevent the adoption of cyber resiliency. This inquiry supports the research focus by examining constraining factors and characteristics that would limit adoption effectiveness, introduce re-invention of cyber resiliency conceptions to adapt to limiting conditions, or otherwise lead to either an active or passive rejection of cyber resiliency altogether. The second research question focused on enablers of the innovation-decision process that support favorable adoption of cyber resiliency. This inquiry supported the research focus by understanding positive characteristics and accelerators towards an adoption decision. It allowed the researcher to examine limitations or challenges in the context of favorable adoption factors.

Theoretical Framework

Everett Rodgers (2003) postulated in his 1962 book *Diffusion of Innovations*, now in its fifth edition, that for innovations to be adopted in a community, they must be spread using four core elements: the innovation itself; the channels upon which it is communicated; time need for the innovation to be adopted; the social system it is used within. People drive the process, it must be widely adopted to achieve self-sustainment. Additionally, Rodgers proposed a five-step decision-making process for adopting an innovation: (1) knowledge or awareness, (2) persuasion, (3) decision, (4) implementation, and (5) confirmation or continuation (Rodgers, 2003). The process, known as the Innovation-Decision Process Model (IDPM), is illustrated in Figure 1. Rodgers' research forms the primary theoretical framework of this qualitative study, focusing specifically on the five stages of the adoption process.

Figure 1

The Five-Step Innovation-Decision Process Model



Note. Adapted from Rodgers (2003).

Prior to an organization undergoing the innovation-decision process, Rodgers (2003) describes conditions conducive to the diffusion of the innovation; such conditions could include previous practices leading to the innovation, a felt need or problem that must be solved, the overall innovativeness of the organization, and the norms of the social system through which the innovation was diffused. In the knowledge phase, the organization or individual understands how the innovation works and is influenced by the organization's or individual's characteristics, such as personality and socioeconomic status. The organization is then persuaded relative to the perceived characteristics of the innovation and how it would benefit the organization or individual. A decision is then made to adopt or reject the innovation, implement it, and, over time, confirm that the decision was correct (Rodgers, 2003, p. 169).

Table 2 offers a view of questions individuals or decision-making units ask throughout the five phases of the IDPM, along with associated rationales or influences on those questions. With this view, one can see how the process is naturally mapped to an organizational leader's decision-making process. The IDPM offers a theoretical framework for modeling innovation decisions for cyber resiliency and has been used in other diffusion studies examining technology adoption. For example, researchers studying instructional practices at the collegiate level have used the IDPM to investigate adoption of innovative teaching techniques (Andrews, n.d.; Lund & Stains, 2015). More recently, and specific to the information technology field, research conducted by Ashogbon (2021) used the diffusion of innovation theory in cloud computing adoption within organizations. Studying the rationales and influences on the IDPM stages for cyber resiliency adoption, the research can identify potential gaps or areas of improvement that would lead to increased adoption within a social system or community of practice.

Table 2

Questions and Rationales within the IDPM

IDPM Stage	Question or Decision	Rationale and Influences
Knowledge	What is the innovation? How does it work? Why does it work?	Awareness-knowledge How-to knowledge Principles-knowledge
Persuasion	What are the innovation's advantages and disadvantages?	Innovation-evaluation and reduction of uncertainty
Decision	Adoption through trial program Adoption through observing results of trial from others Full adoption without trial Rejection after consideration or trial Rejection without consideration	Adoption: small-scale trial Adoption: trial by others Active rejection Passive rejection
Implementation	Where can I obtain the information? How do I use it? What operational problems am I likely to encounter, and how can I solve them?	Active information seeking, technical assistance from change agents

	What needs to be changed or modified?	Re-invention
Confirmation	Did the right decision get made?	Reduction of dissonance

Note. Adapted from Rodgers (2003).

A significant controversy in diffusion research is the presence of *pro-innovation bias* whereby a key assumption within the study is that the innovation should be adopted, that it should diffuse within a social system more rapidly, and that the innovation should not be re-invented or otherwise modified (Rodgers, 2003, p. 109). Rodgers (2003) cautions that such thinking unnecessarily limits diffusion studies and prevents insight into anti-innovation prevention, such as stopping harmful drug use in a population from spreading throughout a community (pp. 109-112). A key strategy to overcoming pro-innovation bias can be to investigate the diffusion of an innovation before it as diffused completely, thereby avoiding a concentration on successful innovations (Rodgers, 2003, p. 112). As this study investigates cyber resiliency, a nascent and still-diffusing innovation at the time of this study, the researcher has an opportunity to prevent pro-innovation bias.

Another criticism of diffusion studies is the tendency for bias, whereby the researcher takes a favorable view towards the change agencies promoting the innovation rather than the potential adopters (source bias), to blame individuals for problems rather than the system (individual-blame bias), or vice versa (system-blame bias) (Rodgers, 2003, p. 118). Rodgers (2003) cautions researchers to avoid assigning blame when seeking the cause for innovation diffusion and to seek alternatives to using individuals as sole units of analysis (pp. 122-125). This study seeks to prevent bias by also factoring in organization characteristics when surveying individuals, which can then be included in the analysis of why an organization adopted or rejected a cyber resiliency innovation.

A secondary theoretical framework that supports this inquiry into the cyber resiliency innovation-decision process is resilience theory. Born from decision-making analysis in ecological science and a relatively new theory pioneered by Gunderson and Holling (2002), the theory links ecological and human social systems as dependent on change for long-term stability and health. The theory offers "sociological conceptions of scale" and considers “how humans symbolize reality at different organizational levels” (Atwell, Schulte, & Westphal, 2009, p. 3).

As examined by Atwell, Schulte, and Westphal (2009), there are sociocultural linkages between resiliency theory and Rodgers' diffusion of innovations theory. They both study human decision-making and how change can influence those decisions (p. 2). The authors found the two theories complementary, and when examined together, allowed for in-depth interviews of rural farmers in the United States corn belt to yield qualitative data that provided insight into "decisions that affect conservation outcomes" (p. 2). A similar linkage of theories in a diffusion study examining the cyber resiliency innovation-decision process would likewise provide key insights thus far not examined in cybersecurity leadership.

Definitions

Cyber or Cyberspace. Defined as “the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries” (CNSS 4009, 2015, p. 40).

Cyberattack (or cyber-attack). Defined as “a malicious event of an enterprise used by cyberspace to disturb, impair, annihilate, or malignantly control a processing

domain or foundation or to either wreck the uprightness of the information or take controlled data" (CNSS 4009, 2015, p. 40).

Cyber incident. Defined as "actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein" (CNSS 4009, 2015, p. 40).

Cyber Resilience and Cyber-Resilient Systems. While the reviewed literature did not agree on a verbatim definition, a common understanding of characteristics aligns with the definition in the U.S. National Institute for Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 2, defined as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources" (U.S. National Institute for Standards and Technology [NIST], 2021, p. 60). For additional definitions and related terminology or acronyms for cyber-resilient systems engineering, the researcher finds the glossary of the NIST SP 800-160 Volume 2 as germane to the objectives of this study and a shared understanding of cyber engineering principles.

Cybersecurity. Defined as "the prevention of damage to, assurance of, and rebuilding of computers, electronic communication frameworks, electronic communications administrations, wire communication, and electronic communication, including information contained within, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (CNSS 4009, 2015, p. 40).

Cybersecurity Leadership. The researcher defines leadership, based on personal and professional experience and in a general sense, as individuals or groups who possess and communicate a shared vision, provide direction, and spark inspiration in others

within their organization; cybersecurity leadership, in turn, combines this definition of leadership with organizational and professional power to influence, directly or indirectly, cybersecurity program decision-making within an organization. This power is often inherent in senior, director, and executive-level roles in typical organizations. As it relates to an academic field of study, Capitol Technology University (2022) defines the interdisciplinary field of cybersecurity leadership research as the branch of computer science and cybersecurity that focuses on the development of the planning, management, and implementation of the leadership needed for the system to work efficiency.

Diffusion. Defined as "the process by which an innovation is communicated through certain channels over time among the members of a social system" (Rodgers, 2003, p. 35).

Industrial Control System (ICS). Defined as a "general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy)" (CNSS 4009, 2015, p. 61).

Information System (IS). Defined as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" (CNSS 4009, 2015, p. 65).

Information System Resilience. Defined as “the ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs (CNSS 4009, 2015, p. 66). While the definition is similar to cyber resilience and cyber-resilient systems, the researcher found value in considering this definition separately as not all information systems are connected through cyberspace.

Innovation. Defined as “an idea, practice, or object perceived as new by an individual or other unit of adoption” (Rodgers, 2003, p. 36).

Innovation-Decision Process. Defined by Rodgers (2003) as "the process through which an individual (or another decision-making unit) passes from gaining initial knowledge of an innovation, to form an attitude toward the innovation, to deciding to adopt or reject, to implementation of the new idea, and to confirmation of this decision" (p. 168).

Organization. Defined by Rodgers (2003) as “a stable system of individuals who work together to achieve common goals through a hierarchy of ranks and a division of labor” (p. 404). Organizations achieve a predictable structure through predetermined goals, prescribed roles, hierarchical authority, rules and regulations, and informal practices (Rodgers, 2003, p. 404).

Resilience. While no single written definition of resilience is accepted across the reviewed literature, the most basic definition can be described as a system’s ability to experience disturbance and still operate (Barasa et al., 2018; Linkov & Kott, 2019; Gunderson & Holling, 2002).

System. Merriam-Webster (n.d.) defines a system in its simplest form as "a regularly interaction or interdependent group of items forming a unified whole," which can range widely in contexts. For the purposes of this study, a system can be both biological in nature, such as an ecosystem, or engineered, such as a computer system, depending on the context used.

Assumptions

To accomplish this study, several assumptions were necessary based on the chosen nature and design. The sample studied was assumed to be representative of information security professionals at their recorded organizational seniority and experience levels. The responses received from the interviews were assumed to reflect their educated professional opinions of lived experiences with cyber resiliency. Additionally, it was assumed that the participants would conduct themselves professionally and with the degree of transparency needed to deduce accurate conclusions from the information provided.

Scope, Limitations, and Delimitations

The professional field of information security is vast, frequently encounters complex adaptive problem sets, and is the subject of many inter-disciplinary qualitative and quantitative studies. The scope of this study is limited to the topic of cyber resiliency as an innovation at a leadership and organizational level. The scope does not include common cybersecurity topics such as threats, vulnerabilities, governance, risk management, or compliance measures, although cyber resiliency as a concept often intersects all of these topics. This study is a mixed-methods diffusion study focusing on the innovation-decision process for cyber resiliency and does not focus on engineering

frameworks or technical implementation concepts; however, an overview of such available methods is discussed in the literature review within chapter two, which is necessary to establish the existence of "how-to knowledge" which Rodgers (2003) describes as a "fundamental variables in the innovation-decision process" (p. 173).

A key limitation of this study is the volume of available literature on cyber resiliency, particularly regarding socio-political and socioeconomic factors within an organization that leads to adoption, and the application of diffusion of innovations theory to information technology. While diffusion research has produced a rich collection of empirical studies completed over the past 70 years, these studies tend to focus on non-engineering diffusion, such as anthropology, sociology, education, marketing, and public health; engineering technology diffusion studies are not prevalent (Rodgers, 2003, pp. 44-45). The addition of such a study represents a significant contribution to the body of diffusion research concerning engineering technology and information security technology. It contributes to the modern direction of diffusion of innovations research. Additionally, data and literature on past cyber incidents in which resiliency played a key factor can be anecdotal, often periodical, and lacks peer reviewed information or full public disclosure of the root cases and key factors of the incident itself.

Another potential limitation revolves around the experience level of the participants. While the researcher made every effort to reach research subjects with expert knowledge of cyber resiliency implementation, and a lived experience with adoption or rejection of the same, the fact remains that cyber resiliency concepts are innovative and have yet to establish prevalence in common information security frameworks. Thus, the sampling of the cybersecurity practitioner population may have

been limited to those who have perhaps established themselves as “early adopters,” which Rodgers (2003) notes is already predisposed to innovativeness and thus would be more willing to adopt the innovation itself, or participants may have provided speculative or aspirational information rather than lived experiences. To reduce this limitation as a significant factor, the researcher tuned the instrumentation (survey software) to reach research subjects that had a breadth of experience and knowledge across several sectors, public and private, and who have served at the leadership levels of cybersecurity organizations to avoid fallacies in data collection. Research participants were asked to attest to their expertise and experiences with cyber resiliency before proceeding with the survey, and interview participants were deliberately selected based on extensive experience and managerial (decision-making) level.

Time and resource constraints were additional limitations in this study. The university's doctoral program through which the researcher conducted the study did not require nor provide additional resources such as funding or personnel to enable long-term field research objectives that would have allowed for more complex designs, methodologies, and a larger data set from which to conclude. These limitations are inherent to the program's characteristics at the chosen university.

Finally, the design of the study itself presented limitations. Although the design is suitable for a study involving diffusion of innovations theory following the research traditions described in Rodgers (2003), and a convergent mixed method design offers the benefits of an enriched data set and greater depth of conclusions, the very nature of the population and sampling method (purposive) introduces inherent bias from the researcher through non-probability sampling. The researcher's G*Power calculations to derive a

statistically significant sample size based on a large population may be flawed and result in type I (false positive) or type II (false negative) errors and, thus, flawed conclusions or acceptance of the positive or null hypothesis when the opposite is true. Unequal sample size, with qualitative participants derived from the larger quantitative (N) sample, is an inherent limitation of a convergent mixed method design; the researcher attempted to mitigate this limitation by quantitative construct validity and qualitative legitimation through triangulation of the data sets during analysis (Creswell & Creswell, 2018, p. 221). The use of the McFadden (1974) index when testing the hypothesis, further explained in Chapter 3, could also be a limitation compared to other pseudo R2 indices; the researcher chose McFadden over other logistic regression pseudo R2 indices based on recommendations in Smith & McKenna (2013) for linear regression models that are conceptually similar to ordinary least squares (OLS) and straightforward to calculate for binary outcome variables. The researcher consulted outside expertise to perform calculations with SPSS software and to validate the regression testing model as a good fit for the data set.

Boundaries, or delimitations, of the quantitative survey, include: (1) a limited timeframe in which the study instrument (online survey) was available to prospective participants, (2) the medium used for the survey was via the internet to allow for varied geographic locations of the subjects, (3) informed consent from the subjects were collected before participation, and (4) the sample demographics collected relevant data on expertise, experience, and career level, but no personal information including names, locations, detailed work history, or other personally identifiable information except in cases where subjects agreed to be part of the interview pool. Boundaries of the qualitative

interviews included: (1) a limited timeframe to conduct the interview, (2) a one-hour duration maximum per session, (3) personal information collected was limited to name, email address, and synopsis of work history with limited specifics, all of which were collected to facilitate the outreach and scheduling process, were not part of the published results, and were destroyed upon completion of the study. These boundaries were established based on time and resource constraints of the study.

As noted in previous sections of this chapter, the significance of a diffusion study focusing on the cyber resiliency innovation-decision process has applications across the information security field for all organizations. Thus, the generalizability of this study applies across the entire security discipline for leaders seeking knowledge or confirmation within their innovation-decision processes, as cyber resiliency can benefit any organization that wishes to adopt resilience methods to prevent disruption to business operations. As described by the U.S. Cyberspace Solarium Commission (2020), layered cyber deterrence – a strategic defense priority for the nation and one that the commission described as achievable – requires public and private sector entities to "step up and strengthen their security posture" with "enhanced resilience with enhanced attribution capabilities" (pp. vi, v).

Chapter Summary

This study's organization progresses in five chapters, a reference section, and appendices. This chapter introduces the study and serves as a background review, description of the problem, and summary of essential information about the study. Chapter 2 outlines the literature review and serves as a background for the subsequent methodology, analysis, and conclusion. Chapter 3 describes the methodology used,

rationale and assumptions for the qualitative design, protection of human subjects, data collection techniques, data analysis procedures, and known limitations. Chapter 4 analyses the gathered research data, including summarized and pertinent data from the case studies and best practices described by the human subjects in the interview process. Chapter 5 will present the leadership model for implementing organizational cyber resiliency, recommendations for future research, implications for critical infrastructure protection, and concluding remarks from the researcher. The study concludes with a list of references used and subsequent appendices.

Chapter 2: Literature Review

In searching for available literature on this topic, the researcher focused on identifying: (1) critical and up-to-date scholarly works and key industry notes within cybersecurity governance, risk management, policy, strategy, and compliance with national-level resiliency objectives; (2) seminal works relating to the theoretical framework, including diffusion of innovation, the innovation-decision process, resilience theory, and organizational leadership relating to technology innovation-decision methodology; (3) key references supporting the need for cyber resiliency and identifying gaps in research, frameworks, and implementation methodology. In all cases, the researcher used the literature to identify the general and specific problems, define the study objectives based on needs or gaps identified in the literature, and form the basis for the study's methodology through survey questions and population sampling criteria.

This chapter identifies the literature search methodology, selection criteria, literature map of selected works, and overviews of cyber resiliency as a cybersecurity leadership innovation and the theoretical framework that centers on the diffusion of innovation theory and the innovation-decision process. A discussion of current findings within the literature, and notable gaps that support the identified problem, is presented, followed by chapter conclusions and a summary.

Title Searches, Articles, Research Documents, and Journals Researched

The literature review methodology, selection criteria, and how this section is formatted were derived from presentation methods used by Barasa, Mbau, and Gilson (2018). The research methods used in the literature search focused primarily on academic

library databases available through Capitol Technology University and Georgia Southern University. Databases used include ACM Digital Library, EBSCOhost databases including Academic Search Premier, Business Source Premier, Discovery Service, The Capitol Technology University Puente Library Online Catalogue, ProQuest Central, and other virtual library databases. Identified seminal works in book form were purchased (such as through Amazon.com) to add to the researcher's library or borrowed from the Capitol Technology University Puente Library. Keyword searches include "resilience," "cyber resiliency," "innovation," with "decision" or "diffusion," "technology diffusion," "cybersecurity resilience," and combinations thereof.

This study used a selective literature review using selection criteria to sharpen preliminary considerations about the topic of study (Yin, 2016, pp. 72-73). Inclusion criteria to select literature included: (1) works published in the English language, (2) priority on peer-reviewed journals and scholarly studies, not opinion papers or industry presentations, (3) works published since 2008, for literature focusing on the theoretical framework and technology innovation diffusion or decision processes, and (4) works published since 2018 (with some exceptions for significant studies or substantial/consolidated volumes) for technical implementation, cyber resiliency or cybersecurity frameworks, and engineering concepts. For example, a search using EBSCO Discovery Service across all EBSCO databases returned 192 results for "cyber resilience" or "cyber resiliency," limited to scholarly (peer-reviewed) journals and periodicals, available in English, and published between the years 2018 and 2022.

Creswell and Creswell (2018) cautioned researchers on using internet-based or industry-based sources, and such was the focus of this literature search. However,

cybersecurity often relies on internet-based information sharing to identify and disseminate technical information as well as governance, risk management, and compliance frameworks. Where internet-based and industry sources were used, the researcher identified a clear tie to the research and study objectives and used sources trusted within the cybersecurity profession as expert opinions, industry research, or engineering concept designs.

Table 3 provides a literature map of key works researched, selected, and cited to understand the problem specific to cyber resiliency. Not all works cited throughout this manuscript are recorded in Table 3, such as those works supporting general research design and academic discipline, literature on general cybersecurity, risk management, governance, or investment strategies not specific to cyber resiliency, as well as introductory and supporting material discussing the cyber threat landscape.

Table 3

Characteristics of Selected Literature on Cyber Resiliency

Study	Title	Methodology	Supporting Themes	Relationship to Study Objectives
Linkov & Kott (2019)	Cyber Resilience of Systems and Networks	Qualitative	Resiliency in Information Systems	Seminal scholarly work to date on cyber resiliency
Linkov et al. (2013)	Measurable Resilience for Actionable Policy	Qualitative	Resiliency in Nature and Ecological Systems, Resiliency in Human Systems and Organizations	Resilience measurement of complex systems
Ferdinand (2015)	Building organizational cyber resilience: A strategic knowledge-based view of cyber security management	Qualitative	Resiliency in Information Systems	Organizational approach to cyber resiliency
Annarelli et al. (2020)	Understanding the management of	Qualitative	Resiliency in Information Systems	Comprehensive study on cyber resiliency management

Study	Title	Methodology	Supporting Themes	Relationship to Study Objectives
	cyber resilient systems			
Barasa et al. (2018)	What Is Resilience and How Can It Be Nurtured? A Systematic Review of Empirical Literature on Organizational Resilience	Qualitative	Resiliency in Human Systems and Organizations	Significant literature review of organizational resilience discovering key enablers of resiliency adoption
Butler and Brooks (2021)	Achieving operational resilience in the financial industry: Insights from complex adaptive systems theory and implications for risk management.	Qualitative	Resiliency in Human Systems and Organizations	Significant and up-to-date study on resilient complex adaptive systems and conditions for resilience in organizations
Carayannis et al. (2021)	Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience	Qualitative	Resiliency in Information Systems, Resiliency in Human Systems and Organizations	Framework for viewing technological and cultural competencies for cyber resiliency
Sharkov (2020)	Assessing the Maturity of National Cybersecurity and Resilience	Qualitative	Resiliency in Information Systems, Resiliency as a National Cyber Strategy	Significant overview of methodologies for cyber resiliency evaluation and development of national cybersecurity strategies
Groenendaal and Helsloot (2021)	Cyber resiliency during the COVID-19 pandemic crisis: A case study	Qualitative	Resiliency in Information Systems, Resiliency in Human Systems and Organizations	Significant literature review and case study of cyber resiliency during the COVID-19 health crisis
M. et al. (2018)	Cyber Resilience and Response: 2018 Public-Private Analytic Exchange Program [report]	Qualitative	Resiliency in Information Systems, Resiliency as a National Cyber Strategy	Significant government study of techniques and design principles for implementing cyber resiliency within the U.S. critical infrastructure sectors

Historical Overview

The term "resilience" or "resiliency" is not a new concept but is relatively new to information systems security and software engineering. Existing ecological literature describes natural systems – ecological habitats and earth-domain environments – as complex and adaptive. Referring to systems (natural, human, or digital) as complex adaptive systems (CAS) was a key theme throughout the reviewed literature (Woods, 2015; Linkov et al., 2013). Additionally, many sources attempted to either define resiliency or critique another's definition, but a common abridged definition of resilience was generally accepted as a system's ability to experience disturbance and still maintain operations (Barasa et al., 2018; Linkov & Kott, 2019; Gunderson & Holling, 2002). The U.S. National Academy of Sciences defined four attributes of resilience: plan/prepare, absorb, recover, and adapt, and incorporated those attributes in its more expansive definition: "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events (Annarelli et al., 2020).

Resilience has long been a focus within the military and public health sectors (Hynes et al., 2020). Roski et al. (2019) noted that resilience is essential to military services as service members must be prepared to deploy anywhere at any time (para 4). The U.S. Department of Defense (DoD) has instituted several health resiliency programs, focusing on the mental and physical health of its service members, that affect more than 2.1 million personnel, 730,000 civilian personnel, and over 9 million TRICARE beneficiaries (Roski et al., 2019, para 4). Furthermore, resiliency has been a focus of combat readiness for military forces. The United States Navy (2018) refers to combat resiliency through one of four core attributes within the *Design for Maintaining Maritime*

Superiority as "toughness" – the ability to "take a hit and keep going, tapping all sources of strength and resilience" (p. 7).

Outside of the military and public health sectors, core concepts of resiliency have grown in importance as other sectors and industries adapt the general definition to fit new environments and circumstances. Four evolutionary themes of resiliency were derived from the reviewed literature: from resiliency in ecosystems and engineering to human systems and modern organizations, converging into information systems engineering and cybersecurity frameworks, to finally, how resiliency has taken center stage in national policymaking within the United States.

Resiliency in Ecosystems and Engineering

Ecologists address resilience in two ways: an emphasis on maintaining equilibrium within a natural system and an emphasis on the persistence of the system itself; Gunderson and Holling (2002) describe this in terms of:

- Ecosystem resilience, focusing on the existence of function, and
- Engineering resilience, focusing on efficiency of function (p. 28).

Walker et al. (2002) noted that ecologists recognize that social-ecological systems undergo change and maintain periods of perceived constancy, with self-reinforcing mechanisms that prevent shifts into another configuration (p. 2).

Perhaps the most well-known researchers in the field of social-ecological resiliency, Gunderson and Holling (2002) defined resilience as "to experience disturbance and still maintain…ongoing functions of controls" (p. 294). Ecosystem resilience focuses on how many system disturbances can occur before the structure changes into another stability domain (Gunderson & Holling, 2002; Linkov & Kott,

2019). The magnitude of disruption before an ecological system "flips" to another state or stability domain is a crucial measurement. The literature on ecosystem resilience is consistent with the notion that disruptions to natural systems can and do happen and that resilience may not necessarily mean resisting such disruption but adapting or changing to a new state of existence (Gunderson & Holling, 2002; Hynes et al., 2020; Walker et al., 2002). This essentially defines what is known as the "existence of function" in ecosystem resilience: a system continues to exist, albeit in a different state than before.

A key framework for measuring ecosystem resiliency is the adaptive cycle. Pioneered by Gunderson and Holling in their overall resilience theory, discussed later in this chapter, the adaptive cycle operates on the understanding that ecosystems cycle through four phases: rapid growth, conservation of resources, release of resources, and reorganization (Resilience Alliance, 2010; see Figure 2). These four phases describe how an ecosystem changes, allowing researchers to frame and measure the "existence of function" in ecosystem resilience. Following the development of Gunderson and Holling's resilience theory and the adaptive cycle framework within it,

An international organization, the Resilience Alliance, was founded by ecosystem resilience researchers to further partnerships in this domain and advocate for adaptive assessments of ecosystems. Meant to benefit management systems, such as corporate farming, government land management, or conservation management, a Resilience Alliance adaptive assessment assists in understanding knowns, unknowns, and assumptions about ecosystem management with the ultimate goal of better understanding a system's ecosystem resilience (Resilience Alliance, 2010, p. 50).

The Resilience Alliance also advocates for adaptive governance in ecosystem management, where human use of land and natural systems adapt to the changing relationships between society and ecosystems in ways that allow for better sustainment of resources and an acknowledgment of when ecosystems are best utilized in various stages of the adaptive cycle (p. 8). Walker et al. (2002) examined social-ecological system resilience within the framework of complexity theory and resilience theory, specifically adaptive cycles, and proposed that decreasing natural resilience in the ecosystem (such as over-farming) increases the risk of loss of goods and services for a given regional-scale social-ecological system. Therefore, resilience management aims to prevent the socio-ecological system from shifting into undesirable configurations. It depends on a deeper understanding of the system and the processes that trigger change thresholds (Walker et al., 2002, pp. 2-3).

Contrasting ecosystem resilience (existence of function) is the concept of engineering resilience (efficiency of function). Engineering resilience involves stabilizing a system near an equilibrium state, where resistance to the disturbance and speed to restoration are principal measurements (Gunderson & Holling, 2002). Woods (2015) considered four concepts of engineering resilience in terms of characteristics of the system and its resilience response: (1) resilience as rebound, where the system recovers to its previous state after a surprise event, (2) resilience as robustness where the number of disturbances the system can respond to effectively is expanded, (3) resilience as graceful extensibility where a system can be stretched to handle surprises, and (4) resilience as sustained adaptability where the system is considered a layered network with multiple response options and flexibility to adapt over time. Woods considered preparation to

handle model surprises a key line of inquiry relevant to engineering resilience (Woods, 2015, p. 8).

Engineering resilience is not limited to digital, human-made systems. Instead, it is an established feature of technological, ecological, and sociological systems, making it a more general concept in the literature than just associated with one type of system (Linkov et al., 2013). One key engineering resilience concept is to view these systems as complex and adaptive (Woods, 2015; Linkov et al., 2013). Linkov et al. (2013) proposed a "resilience matrix" that maps the four phases of disaster resilience – defined by the National Academy of Sciences as plan/prepare, absorb, recover, and adapt – with four domains of the U.S. military's Network Centric Warfare doctrine: physical, information, cognitive, and social. The authors argued that, due to the complex systems within each of those domains, only by understanding and measuring the dynamics in each domain related to the phases of an adverse event can designers and managers achieve a holistic view of resilience in any system.

A critical test that brought all fundamentals of resiliency together started in March of 2020, as the COVID-19 health crisis gripped the world, and researchers found a new reason to investigate resiliency concepts. Hynes et al. (2020) found that environmental consequences of climate change, pandemics, and other “shocks” to society and nature demonstrate that resilience must become a prime consideration in any system’s management approach, both to ensure survival and also to take advantage of revealed opportunities for improvement and must compliment risk-based approaches. As COVID-19 stressed nearly technological, ecological, and sociological systems, resilience has

since taken prominence in marketing literature, scholarly and media articles, and worldwide discussions.

Resiliency in Human Systems and Organizations

Organizational resiliency has become a strategic management goal spanning the entire organization: from human resources to information technology, national critical infrastructure, and even private small businesses (Ferdinand, 2015). Gunderson and Holling (2002) identified three key properties driving the adaptive cycle in human organizations. The first, developing potential for change, involves building the organization's cultural capital: networks, friendships, and mutual trust. The second, connectedness, reflects the internal resistance to external variables or the return speed to equilibrium after a disturbance. The third property measures resilience versus vulnerability, or the ability to adapt or be overcome and "flip" to a new state or stability domain. The authors note that innovations occur in "pulses" or surges when uncertainty is high, and controls against that uncertainty are weak or defeated so that new concepts can take hold. Here, the first seeds of cross-pollination between diffusion of innovation and resilience theory begin to show.

The literature on organizational resilience found challenges and opportunities within the researched characteristics. Carayannis et al. (2021) described the concept of *organizational ambidexterity*, which relies on the balance between exploration and exploitation – exploiting existing competencies while exploring new growth opportunities (p. 223). Similarly, Butler and Brooks (2021) developed a model of resilient complex adaptive systems (RCAS) as an answer to designing business architecture for the financial industry that would be better positioned to achieve resilience

and real-time risk response; organizations must have both well-defined operational capabilities, rules and controls, and internal agents capable of anticipation and sense-making as well as coordinating internally and externally (pp. 401-403).

This concept of viewing change as an opportunity or advantage appears unique in the organizational resilience literature and stands in contrast to ecosystem and engineering resilience which focuses on "weathering the storm" and returning to either a changed or status-quo state. Groenendaal (2020) noted four foundational, human-centric characteristics for organizations shifting from planning-driven business continuity management to new opportunities or innovations: adaptability, cohesion, efficiency, and diversity (p. 102). These characteristics both adapt to challenges and seek opportunities within them and are more in line with ecosystem resiliency. In contrast, the system responds, adapts, and potentially "flips" to a new configuration.

Engineering resilience and organizational resilience are characteristics of resiliency in information systems, or cyber resiliency, and several literature authors make a point to include information technology as part of the journey to greater resiliency in technological and sociological systems. Butler and Brooks (2021) emphasized digital transformation as the key to transforming the organization into an RCAS (p. 399). Hynes et al. (2020) recommended building organizational and societal resilience through system design, quantifiable investments, controlling system complexity, managing system topologies, adding redundancies and functionality, and developing real-time decision support tools: all characteristics that point to a convergence of technological and sociological factors influencing resiliency. The "human" element of systems management cannot be separated from the technological adaptation; organizational culture, attitudes,

beliefs, leadership, and employee actions contribute to a holistic management approach for information systems and information security (Rocha et al., 2014, p. 91). Thus, resiliency within information systems and information security (cyber) management is a convergence of technological and sociological conditions and characteristics.

Resiliency in Information Systems: A Convergence of Concepts

Some authors noted the early prominence of resiliency in information systems and cyber-connected systems started with the World Economic Forum (WEF) in 2012, which released a report entitled “Partnering for Cyber Resilience” and contained several resolutions and goals related to resiliency (Bjork et al., 2015). The WEF set a goal of a risk-based approach to system resilience “to survive and quickly recover from attacks and accidents” (World Economic Forum [WEF], 2012, p. 9).

Organizations seeking to be more resilient have found both competitive advantages and existential imperatives (Annarelli et al., 2020, p. 2). The need to achieve resiliency in information systems, and cyber resiliency within cyberspace-connected systems, has arguably never been stronger. In their annual cybersecurity strategic report, Stott and May reported in 2020 that the business perception of cybersecurity is shifting towards strategic priority (54% of respondents) than categorizing it as an unnecessary expense (15%), likely due to well-publicized breaches and the consequences associated with them, such as fines and reputational damage (Rutt, 2020).

Threats to cyberspace-connected information systems are "sporadic and multidimensional," with the potential to inflict very high levels of damage (Li & Liu, 2021, p. 8184). Imperatives to implement resiliency can be even higher in companies that cannot weather damage to their reputation, as opposed to companies with superior

reputations (such as Fortune 200 companies) that could recover more fully from a significant cyber-related incident (Gwebu et al., 2018). Linkov and Kott (2021) agree that cyber resilience has become significant and consequential, particularly for a nation's critical infrastructure, and have focused their recent research and scholarly advocacy around how to measure resiliency, citing an abundance of enhancement techniques and frameworks but a lack of quantification of mission parameters. Petrenko (2019) notes that the main cyber challenges of modern information systems within the context of advanced persistent threat (APT) actors include insufficient resiliency of the system itself, increased complexities of the system architecture, and challenges with identifying quantitative patterns that would detect and respond to advanced threats (pp. 102-103).

With the threat landscape at an all-time high, cybersecurity leadership and a well-governed security organization have important defensive objectives; information security leaders must safeguard their organization, protect critical data, and ensure online services and digital platforms remain resilient to cyber-attacks (Dwivedi et al., 2020, p. 10). Two common themes from the literature on information systems and cyber resiliency emerged to assist information security leaders in understanding and implementing resiliency: characteristics of resilient systems and technical or operational frameworks for implementation.

Annarelli, Nonino, and Palombi (2020) conducted a literature review of cyber resilient system management and described four key attributes of resilient systems derived from the work of Tierney and Bruneau (2007):

- Robustness (resisting disruptive forces),
- Redundancy (meeting functional requirements with replaceable elements),

- Resourcefulness (exploiting resources to diagnose and solve problems), and
- Speed (recover quickly from a disruption) (p. 4).

Woods' (2015) four attributes of engineering resiliency (rebound, robustness, extensibility, and adaptability) would agree with this model as well, as well as the phases of the adaptive cycle (growth, conversation, release, reorganization), albeit in a looser interpretation (Gunderson & Holling, 2002). The U.S. Department of Homeland Security's (DHS) Cyber Resilience and Response (CRR) Team defined cyber resilience as "the ability to adapt to changing conditions, prepare for, withstand, and rapidly recover from disruption" (M. et al., 2018, p. 5). The team emphasized several words in their definition which can be expanded upon further to characterize resiliency in an information system: (1) adapt, where a change in approach or strategy occurs as a result of a disruptive event and learning; (2) prepare, where threats are anticipated and planned for; (3) withstand, where business operations are sustained; (4) recover, where a system is restored to normal operations following an event (p. 4).

A review of cyber resiliency characteristics would not be complete without noting the contributions of the most well-known industry engineering publication on the subject: the NIST SP 800-160 Volume 2, *Developing Cyber-Resilient Systems* (2021). Developed by a public-private partnership of researchers within NIST and designed to be used in conjunction with International Standard ISO/IEC/IEEE 15288, *Systems and software engineering – System life cycle processes*, this publication has come to be viewed by the U.S. Government as the definitive engineering standard for cyber resiliency in federal government information systems (NIST, 2021). The publication, despite taking a decidedly-engineering approach, also views resiliency as a multidisciplinary effort to

achieve implementation, with several key characteristics: (1) focus on the mission or business function, (2) assume a changing environment, (3) focus on the effects of the advanced persistent threat, (4) assume the adversary will compromise or breach the system or organization, and (5) assume the adversary will maintain a presence in the system or organization (NIST, 2021, pp. 77-78).

Interestingly, NIST (2021) draws similarities between cyber-resilient system engineering and biology (and, by extension, natural and ecological systems). Elements of the body, such as the immune system, skin, blood vessels, and other defensive antibodies, are compared to traditional cybersecurity measures in an information system. In contrast, the ability of the body to adapt, heal, and otherwise recover from illness or injury is compared to cyber-resilient systems functionality (NIST, 2021, p. 2). The parallel between engineering and ecosystem resilience is clearly stated, and cyber resiliency can be viewed as a convergence of the stability and resiliency methods described by Gunderson and Holling (2002).

With these common characteristics and assumptions about the operating environment in mind, reviewing common misconceptions of resiliency is essential. Several literature authors note that resiliency is a challenging concept often confused with other related but different concepts, such as risk, robustness, and security (Linkov & Kott, 2019; Butler & Brooks, 2021). The DHS CRR Team noted that a critical differentiation of cyber resiliency from "traditional" forms of cybersecurity is that "cyber resiliency continues to function even after the adversary has penetrated the security perimeter of a network and has compromised cyber assets" (M. et al., 2018, p. 9). Much

of the literature agrees that this key differentiation complements existing cyber defenses rather than a substitute (Linkov & Kott, 2019; Annarelli et al., 2020; Petrenko, 2019).

Even as far back as 2012, the WEF recognized that cyber-connected information systems are inherently vulnerable, noting that “100% risk mitigation is not possible in any complex system" (p. 9). Linkov and Kott (2021) described a key notion of cyber resiliency as the acceptance that a compromise is a likely event and that the focus must be on the ability of the system to recover and adapt rather than resist the attack (p. 1). With these key characteristics and differences from traditional cybersecurity, how can leaders employ resiliency within their organizations?

Several frameworks assist information security leaders, and other organizational executives, in implementing resiliency within their systems. Within the literature, emphasis was made on several leading engineering, implementation, and management frameworks. These frameworks differ from other cyber-related frameworks as they are not inherently technical; many take a holistic view of implementation to include technical, cultural, and managerial, ensuring that cyber resiliency is more in line with contingency planning and disaster recovery where more of the company's corporate structure is involved. A summary of significant frameworks noted in the literature is discussed below.

MITRE / NIST Cyber Resiliency Engineering Framework. Bodeau and Graubart (2011) developed the MITRE Cyber Resiliency Engineering Framework, which consists of four major components: cyber resiliency, threat modeling, applicability domains, and aspects of costs. The framework is built from a set of defined goals, objectives, and practices of resilience engineering focusing on systems security

engineering, security operations and management, and systems engineering for performance and management. The core aspects, while technical, also consider social factors as supporting rather than central to the model (Bodeau & Graubart, 2011). Additionally, this framework is oriented toward cost-effectiveness (Annarelli et al., 2020, p. 4).

Building from the MITRE framework and designed to operate in conjunction with international standards (ISO), NIST developed the Special Publication (SP) 800-160 Volume 2 for developing cyber-resiliency systems with an engineering approach. Like MITRE's work before it, the NIST framework adheres to a construct of goals, objectives, techniques, implementation approaches, and design principles. The framework is designed to be adaptable and, despite taking a decidedly-engineering approach, also views resiliency as a multidisciplinary effort to achieve implementation, with several key characteristics: (1) focus on the mission or business function, (2) assume a changing environment, (3) focus on the effects of the advanced persistent threat, (4) assume the adversary will compromise or breach the system or organization, and (5) assume the adversary will maintain a presence in the system or organization (NIST, 2021, pp. 77-78).

CERT Resilience Management Model (CERT-RMM). Developed by the Software Engineering Institute of Carnegie Mellon University, the CERT Resilience Management Model (CERT-RMM) provides a framework for organizational operational resilience activities. It was designed to enable and promote the convergence of various resilience and business continuity elements, including disaster recovery planning, IT disaster recovery, information security and cybersecurity, and IT operations, as well as tangential functions such as legal, human resources, and others (Software Engineering

Institute [SEI], 2018). Sharkov (2020) describes CERT-CRMM as 26 process areas grouped into four categories: enterprise management, operations management, engineering, and process management (p. 10).

A related hands-on review process, known as the Cyber Resilience Review, was developed by CERT in partnership with the U.S. Department of Homeland Security to tailor the resilience framework to critical infrastructure (p. 16). At the foundational level, CERT-RMM addresses operational resilience through a risk management approach, providing an organizational construct for resilience activities and converging several often-soloed efforts into a series of capability dimensions, institutionalizing it and contextualizing it in terms of risk to the organization (Software Engineering Institute [SEI], 2018).

AMBI-CYBER Architecture. Carayannis et al. (2021) proposed linking organizational ambidexterity - where organizations balance exploration and exploitation of their resources - with cybersecurity concepts to produce an AMBI-CYBER architecture centered around the 7Ps stage gate model: patient, persistent, persevering, proactive, predictive, preventative, and preemptive. The authors then mapped the 7Ps to the NIST cybersecurity framework of identify, protect, detect, respond, and recover. The authors concluded that there is a need for increased collaboration and integration between public and private entities to enhance cybersecurity from a societal perspective (not just technical, but protecting against societal disinformation, attacks on democratic processes, etc.). Ultimately, the authors suggest that cyber resilience as a strategic concept relies on further exploring research and evidence-based findings to refine a combined cybersecurity model that considers technical, organizational, and socio-economic factors.

STRATUS. Developed and proposed at the 2012 IEEE Sixth International Conference on Self-Adaptive and Self-Organizing Systems Workshops (SASOW), a research team proposed a system engineering model known as STRATUS: “strategic and tactical resiliency against threats to ubiquitous systems" to use added overhead resources to detect and diagnose an attack, switch to contingencies, and predict future attacks all through machine-speed computations with minimal human decision-making (Burstein et al., 2012, p. 47; Annarelli et al., 2020). The differentiator between STRATUS and traditional intrusion detection and prevention systems (IDS/IPS) is the ability to predict and respond to potential threats using advanced analysis rather than attempting detection and prevention as attacks unfold (Burstein et al., 2012, p. 49).

Resilience Matrix Framework. Developed by Linkov, Eisenburg, Plourde, Seager, Allen, and Kott (2013), the authors proposed that the National Academy of Sciences resilience categories - plan, absorb, recover, and adapt - can be combined with the U.S. Department of Defense's network-centric warfare doctrine concepts of physical, information, cognitive, and social to produce a matrix framework to measure system resilience (Linkov et al., 2013; Keys & Shapiro, 2019, pp. 66–67).

Managerial Cyber Resilience Framework. Several literature authors proposed, through detailed study and analysis of managerial and technical factors of cyber resilience, a four-phase model for implementation: plan/prepare, absorb, recover, and adapt (Annarelli et al., 2020; Linkov et al., 2013). The most extensive of these phases is the plan/prepare phase, which includes data protection, prevention, testing, and training actions. When an adverse event occurs, such actions contribute to the organization

absorbing and recovering from the event, adapting to new conditions by reviewing the previous phases and updating internal processes or new standards (Annarelli et al., 2020).

Resiliency as a National Cyber Strategy in the United States

The imperative for cyber resiliency as a component of a national security strategy first took shape on the world stage following a report released by the World Economic Forum in 2012 (Bjorck et al., 2015). The report recognized that the increasing connectivity and dependence of organizations, systems, and people worldwide necessitated a resiliency approach to risk and responsibility for cyberspace-connected information systems (World Economic Forum [WEF], 2012, p. 4). The WEF concluded that this increased interdependency for economic prosperity as well as the rapidly evolving cyber risk landscape, the free flow of information to drive economic value, and the inherent vulnerabilities within organizations - primarily human awareness, leadership, and execution – required a commitment to established principals and guidelines measured by a maturity model for organizational cyber resilience (WEF, 2012, pp. 4-5).

The cyber resiliency maturity model adopted by the WEF at the time ranges from stage 1 (the organization is unaware and seeks cyber risk as irrelevant) to stage 5 (the organization is highly connected, shows exceptional awareness, and is an industry leader in cyber risk management), also encompassed WEF's Cyber Risk Framework that presented a simplified view of threats and vulnerabilities, measured values at risk (assets and reputation), and categorized responses by traditional, community, and systemic that C-level executives could understand and implement with a checklist (WEF, 2012, pp. 10-14). While technically, the MITRE Cyber Resiliency Engineering Framework predated the WEF's model as a resiliency framework, it can be described as the first international

model found in the widely-known literature that included non-technical factors (WEF, 2012).

Shortly after the WEF released its international cyber resiliency report, cyber resiliency began to take on a buzzword quality within the United States and globally. In February 2013, U.S. President Barack Obama issued Presidential Policy Directive 21 (PPD-21) and Executive Order 13636, both designed to bolster the cybersecurity and resiliency of U.S. critical infrastructure sectors, demonstrating the American government's immediate attention towards securing what it saw as a critical vulnerability in future cyber-enabled conflicts (DHS, 2015, p. 1). Both landmark executive actions directed further action within the federal government to build upon existing guidance towards strengthening critical infrastructure security, continuing in the National Infrastructure Protection Plan (NIPP) of 2013, in which the word "resilience" appeared 241 times throughout the 57-page document. The vision statement of NIPP 2013 declared "a Nation in which physical and cyber critical infrastructure remains secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened" (DHS, 2013, p. 5).

The U.S. Department of Homeland Security released its National Critical Infrastructure Security and Resilience (CISR) Research and Development (R&D) Plan 2015. The plan had two primary objectives: identify priorities and guide R&D requirements led by DHS for the critical infrastructure community and build upon existing guidance contained within past policies and directives such as PPD-21, NIPP 2013, and others to focus national R&D efforts towards strengthening critical infrastructure resiliency (DHS, 2015, p. 6). The National CISR R&D Plan was the

culmination of the strategies and policies that came before it and collaboration with stakeholders across critical infrastructure communities of practice, think tanks, advisory councils, and cross-governmental steering groups (DHS, 2015). Five R&D priority areas were identified and designated with short (3-5 years) and long-term (10 years) goals, including developing: (1) a foundational understanding of critical infrastructure systems, (2) risk assessment and management approaches, (3) capabilities, technologies, and methods to support security and resiliency, (4) unified and integrated situational awareness using data science capabilities, and (5) a culture of collaboration amongst R&D entities (DHS, 2015, p. 10). While measurement of progress and a detailed path forward were noted in the plan, the researcher could not find more publicly available progress reports. Thus it is unknown whether the priorities detailed in 2015 continue to this day.

In 2018, President Donald Trump signed the second National Cyber Strategy of the United States of America. Within this strategic framework, resilience was featured as the first of four pillars designed to protect, promote, preserve, and advance American prosperity and influence (U.S. [Executive] Office of the President of the United States [EOP], 2018). The key objective of the "protect" pillar was to "increase the security and resilience of the nation's information and information systems," with emphasis on prioritizing the resilience of critical infrastructure and federal government systems (EOP 2018, pp. 6-9).

In 2018, the DHS Cyber Resilience and Response (CRR) team prepared a report with the Public-Private Analytic Exchange Program following a six-month qualitative study on cyber resiliency within U.S. critical infrastructure. The report defined cyber

resilience as "the ability to adapt to changing conditions, prepare for, withstand, and rapidly recovery from disruption" (DHS CRR, 2018, p. 5). The team emphasized several words in their definition which can be expanded upon further to characterize resiliency in an information system: (1) adapt, where a change in approach or strategy occurs as a result of a disruptive event and learning; (2) prepare, where threats are anticipated and planned for; (3) withstand, where business operations are sustained; (4) recover, where a system is restored to full operation following an event (p. 4). Further details of the report's findings are discussed later in this chapter. They are of significant interest to this study in understanding limiters and enablers of the cyber resiliency innovation-decision process.

The Fiscal Year 2019 National Defense Authorization Act (NDAA) chartered the U.S. Cyberspace Solarium Commission (CSC) to answer two fundamental questions for the President and the Congress: (1) what strategic approach will deter cyber aggressors, and (2) what policies and legislation are required to implement the strategy (U.S. Cyberspace Solarium Commission [CSC], 2020). The CSC final report, released to the public in 2020 and included legislative proposals and draft policy language, was groundbreaking in its thoroughness and transparency, calling for government reform, legislation, and policies that will shape responsible behavior and encourage restraint in cyberspace, deny benefits to adversaries through the adoption of national cyber resiliency, and impose costs to deter malicious cyber actors and reduce gray-zone cyber conflict (CSC, 2020, pp. 2-6).

By 2020, the global trend of adopting resilient strategies and operations to ensure success in an interconnected digital world began in earnest and was amplified by crises

such as the COVID-19 pandemic (Annarelli et al., 2020; Groenendaal & Helsloot, 2021). The outbreak of COVID-19 and the subsequent change to workplace dynamics forced changes to enterprise network architecture without suitable cybersecurity controls to match them – for example, remotely-accessed applications or insecurely managed virtual private networks (VPNs) – which consequently have made organizations more vulnerable to cyber-attack. As a result, many public and private sector organizations have turned to better understanding cyber resiliency to combat the effects of malign cyber influences (Groenendaal & Helsloot, 2021).

Joseph R. Biden, upon assuming office as the 46th President of the United States in 2020, released an update to the 2018 National Cyber Strategy via the Interim National Security Strategic Guidance in 2021, the substance of which differed from the previous administration's strategy only in workforce diversity and direct government spending on solutions; the core of the document's statements offers continuity supporting national cyber resiliency (Lin, 2021). By 2022, the Biden Administration has released several executive orders related to cybersecurity and cyber resiliency, perhaps most notably Executive Order 14028, Improving the Nation's Cybersecurity, which makes several bold decisions strengthening public-private partnerships and increasing security within the federal government's networks (The White House, 2021). Expressly, President Biden declared within the executive order that "it is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security" and directed government departments and agencies to "implement Zero Trust Architecture" amongst other cyber resiliency efforts (The White House, 2021, pp. 2-5).

By 2022, the Director of National Intelligence's (DNI) Annual Threat Assessment of the U.S. Intelligence Community warned that "attackers are innovating their targeting strategies on victims whose business operations lack resilience" across the public and private sectors against continuing threats such as ransomware. Nation-states such as Iran, North Korea, China, and Russia continue to threaten critical infrastructure services within the United States and allied nations, and non-military measures have done little to stem the tide of threats against cyber-connected information systems (DNI, 2022). Without an international solution, such as norms and deterrence in cyberspace, cyber resiliency has become imperative in national security strategy for the foreseeable future (Alperovitch, 2022).

In March 2023, The White House released the latest National Cybersecurity Strategy, within which resilience was named in two of the five pillars: (1) defend critical infrastructure, (2) disrupt and dismantle threat actors, (3) shape market forces to drive security and resilience, (4) invest in a resilient future, and (5) forge international partnerships to pursue shared goals (The White House, 2023, pp. 4-6). The executive actions and strategic messaging of the 46th President of the United States declared cyber resilience as the nation's strategic approach to ensuring "our digital ecosystem" is "defensible, resilient, and aligned with U.S. values" (The White House, 2023, p. 4).

Theoretical Framework

This section describes the diffusion of innovation theory (Rodgers, 2003) and the innovation-decision process within the researcher's context of cyber resiliency as a technological innovation. As an additional theoretical framework, resilience theory for

sustainable ecosystems (Gunderson & Holling, 2002) is relevant to the research objectives in understanding other factors that enable resilience, sustainability, and the concept of adaptive cycles in both human and natural systems: essential concepts to understanding resiliency – at a fundamental level – that can be adapted to understanding resiliency for cyber-connected networks. This section concludes with a brief discussion that links both theories together as the core theoretical framework of this study with relevant findings from the literature.

Understanding Diffusion of Innovation and the Innovation-Decision Process

Wejnert (2002) notes that the diffusion of innovations theory began with Tarde (1903) in his book "The Laws of Imitation." Ryan and Gross (1943) published a landmark diffusion study on the diffusion of hybrid-corn use in Iowa, and since then, over 4000 diffusion studies have appeared in journals on topics such as agricultural practices, technology, medical, and policy innovations (Wejnert, 2002; Rodgers, 2003). Diffusion studies have followed the Ryan and Gross (1943) qualitative research methodology through survey-based data collection where participants describe when, where, and from whom they adopted the innovation and the results or consequences (Rodgers, 2003, p. 33).

Rodgers (2003) described four main elements in his diffusion of innovation theory: (1) the innovation itself, (2) the communication path and channels used, (3) the time necessary to diffuse the innovation itself, and (4) the social system through which the innovation diffuses (p. 11). It is important to note that, within the theory context, cyber resiliency is an *innovative technology*, specifically a *technology cluster* where several closely interrelated elements are considered the innovation itself (pp. 13-14).

Rodgers noted in the literature that "more scholarly attention should be paid to technology clusters" (p. 15).

Rodgers (2003) identified five perceived attributes of innovations that can also be viewed with a cyber resiliency lens, as noted within the literature:

1. There should be a relative advantage where the innovation is perceived as advantageous; for cyber resiliency, implementing resiliency measures keeps the organization operational despite malign cyber influences, malware, or denial of service attacks.
2. The innovation must be compatible with the organization's technology, structure, and cultural values; cyber resiliency encounters significant compatibility barriers not just at a technical level (inability to adopt certain tools or network architectures) but through perceived cultural values (such as the need to prepare for operational contingencies versus using insurance to insulate against disruptive events financially). Rutt (2020), within the Stott and May's annual cybersecurity report, noted that 31% of participants perceive cybersecurity as a technical problem and 15% as an unnecessary expense, marking a little less than half of all respondents that indicate significant cultural and organizational barriers to implementing basic cybersecurity measures, let alone more advanced cyber resiliency measures (p. 7).
3. The degree of complexity where the innovation may be challenging to understand or implement; cyber resiliency again, similar to the compatibility attribute, encounters significant headwinds in the complexity and abstract nature of some technical concepts, and the perception that anything that has to do with "cyber" is

highly technical and better left to specialists. Petrenko (2019) notes that the main cyber challenges of modern information systems within the context of advanced persistent threat (APT) actors include insufficient resiliency of the system itself, increased complexities of the system architecture, and challenges with identifying quantitative patterns that would detect and respond to advanced threats (pp. 102-103). As Rodgers (2003) noted, innovations that are simple to understand are adopted more rapidly (p. 16).

4. The trialability of the innovation, where it can be experimented with on a limited scope; cyber resiliency is easy to trial or test through pilot programs, limited roll-out of technical solutions, and scalability of many resiliency tools. Additionally, as Petrenko (2019) describes, cyber resilience serves several IT and risk management disciplines, all having mechanisms at various organizational levels to distribute changes to their programs on a limited scale before enterprise-wide implementation.
5. Finally, the degree to which the results of innovation can be observed or are visible to others; cyber resiliency implementation is potentially hampered within this attribute, as well, as it is likely, not observable outside of an incident (nor do many organizations desire such observability of its disaster recovery and contingency planning processes). Within this attribute, Rodgers (2003) describes another social aspect of adopting innovation: the perceived lack of social prestige in cyber resiliency causes significant barriers.

Rodgers notes that, of the five attributes described above, two characteristics – relative advantage and compatibility – are "particularly important" for explaining the adoption rate (p. 17).

Beyond the innovation itself, communication channels are the second main element of Rogers' diffusion of innovations theory. Communication between humans can be described as homophilous – two or more individuals with similar backgrounds and attributes – or heterophilous in which the individuals communicating are very different in background, specialization, or other personal or professional attributes (Rodgers, 2003, p. 19). Rogers notes, "one of the most distinctive problems in the diffusion of innovations is that the participants are usually quite heterophilous" (p. 19). Such stark differences in background could describe an organization's Chief Information Security Officer, or another senior cybersecurity professional, in communicating with non-technical managers or board members.

Time is the third main element of diffusion and is critical in measuring adoption rates within social systems (Rodgers, 2003, p. 20). Time is required within the innovation-decision process for knowledge, processes, and other adoption decision aids to permeate a social system. The social system, the fourth main element of diffusion, involves interrelated individuals undertaking joint problem-solving and united in common goals or objectives (Rodgers, 2003, pp. 21-22). Cybersecurity professionals are part of a community-of-practice that can be described as a social system by which cyber resiliency can be diffused, with established norms (rules of conduct for certified professionals, such as the $(ISC)^2$ or ISACA Code of Ethics) and communications channels (blogs, forums,

media, and online repositories often shared by security professionals) (Rodgers, 2003, pp. 22-27).

The innovation-decision process, as modeled by Rodgers (2003), is a focus of this study and must be described in greater detail. This five-step process consists of "a series of choices and actions over time through which an individual or a system evaluates a new idea and decides whether or not to incorporate the innovation into ongoing practice" (Rodgers, 2003, p. 168). Knowledge, persuasion, decision, implementation, and confirmation are the five stages. While an overview of the five-step innovation-decision process is offered in both Figure 1 and Table 2, within Chapter 1 of this manuscript, what follows is a description of the behavior that occurs at each stage within the context of cyber resiliency and is informed by the literature.

The Knowledge Stage. Rodgers describes the knowledge stage as when an individual or an organization is exposed to innovation and gains an understanding of its functions and usages (Rodgers, 2003, p. 171). Understanding and awareness are only some of what is needed; Hassinger (1959), as discussed within Rodgers (2003), notes that individuals seldom seek knowledge without first establishing a need (p. 171). Rodgers also notes three types of knowledge: how-to knowledge, principles-knowledge, and awareness-knowledge, with how-to knowledge a "fundamental variable in the innovation-decision process" (pp. 172-173).

Hynes et al. (2020) note that resilience-focused system design, philosophy, and strategies can reduce future financial crises and negative business effects. Furthermore, cyber-attacks cause adverse impacts on firms' reputations, financial markets, and trading volumes (Tosun, 2021). Recent market research demonstrates that organizational leaders

(not just security professionals) recognize a need for cybersecurity investments, with 54% of leadership-level participants noting cybersecurity as a strategic priority in the wake of publicized cyber-attacks, breaches, fines, and reputational damages (Rutt, 2020). This activity indicates an increase in awareness-knowledge.

The volume of research and marketing "chatter" around resilience is increasing. Technology consulting firms like Accenture have produced public white papers around cyber resiliency, raising awareness and promoting solutions such as frameworks and technology adaptations (Accenture, 2018). While much of the industry discussion on resiliency is mired in marketing and promotional material, the core concepts are still served by increasing knowledge of cyber resiliency as an innovative technology cluster (Rodgers, 2003). These materials indicate an opportunity to increase principles-knowledge of cyber resiliency. As noted in the historical overview earlier in this chapter, several engineering frameworks and technical designs exist for implementing cyber resiliency at a technical and organizational level; this indicates a significant volume of how-to knowledge.

The Persuasion Stage. In persuasion, the individual or organization adopts a favorable or unfavorable opinion of the innovation. It is here that an individual may ask, having gained knowledge of the innovation, "what are the innovation's advantages and disadvantages?" (Rodgers, 2003, p. 175). Cyber resilience can be described within the context of the innovation-decision process as a preventative innovation – an innovation adopted to avoid or mitigate unwanted occurrences. Rodgers (2003) notes that this is a relatively weak motivational factor in embracing innovation and can sometimes be strengthened by a cue-to-action created by a change agency (p. 176).

The DHS CRR Team (2018) noted that the government had significant work ahead in improving public-private partnerships for cyber resiliency. Panel discussions with participants found an inherent lack of trust between public and private organizations, particularly with partnerships required by law or regulation; the research team concluded that reforming public disclosure laws and educating organizations about mutually beneficial services such a partnership could provide might increase the diffusion of resiliency cooperation within a community or sector.

The Decision Stage. The decision stage of the innovation-decision process is fairly straightforward to understand – the individual or organization decides to adopt or reject the innovation. If rejection occurs, it could be active or passive. Active rejection happens when the innovation undergoes a trial or pilot but is rejected by the results; passive rejection never really considers the innovation (Rodgers, 2003, p. 178).

Both methods may reject cyber resiliency: active rejection could occur due to a pilot in which technical or organizational barriers were deemed too significant to overcome. In contrast, passive rejection could result from management and industry-related factors. Annarelli, Nonino, and Palombi (2020) described, after an extensive review of available literature, three contextual factors contributing to the management of cyber resilience systems: (1) infrastructure, whether critical or non-critical, (2) industry, whether customer-based (business to business) or consumer base (business to consumer), and (3) ownership, public or private. The interdependencies and management characteristics within these three factors contributed significantly to how a resilience strategy is formulated by management, either proactive or reactive, and the specific technology innovations selected (pp. 2-3).

The Implementation Stage. At the implementation stage, the innovation is put to use. Rodgers (2003) made extensive remarks on re-invention, where adopting an innovation means re-designing or modifying it to suit the individual or organization (p. 180). The literature largely agrees with the idea of re-invention as it applies to cyber resiliency, as many of the frameworks are designed to be adaptive to the organization and create a unique application of the innovation and technology in use (Linkov & Kott, 2019; Ferdinand, 2015; Petrenko, 2019).

The Confirmation Stage. When confirming an innovation decision, the individual or organization seeks to reinforce the decision and could reverse the decision if conflicting messaging is received (Rodgers, 2003, p. 189). Should dissonance occur that changes a decision maker's state of mind, discontinuing the innovation may result in a replacement of the innovation with a different one or disenchantment of the performance of the innovation, and outright rejection follows (pp. 189-190). Confirmation of cyber resiliency decisions can be reinforced by knowledge – both of resiliency itself, its effect on the organization's secure operation, and the competitive advantages gained (Ferdinand, 2015).

Resiliency Theory and Adaptive Cycles in Human Organizations

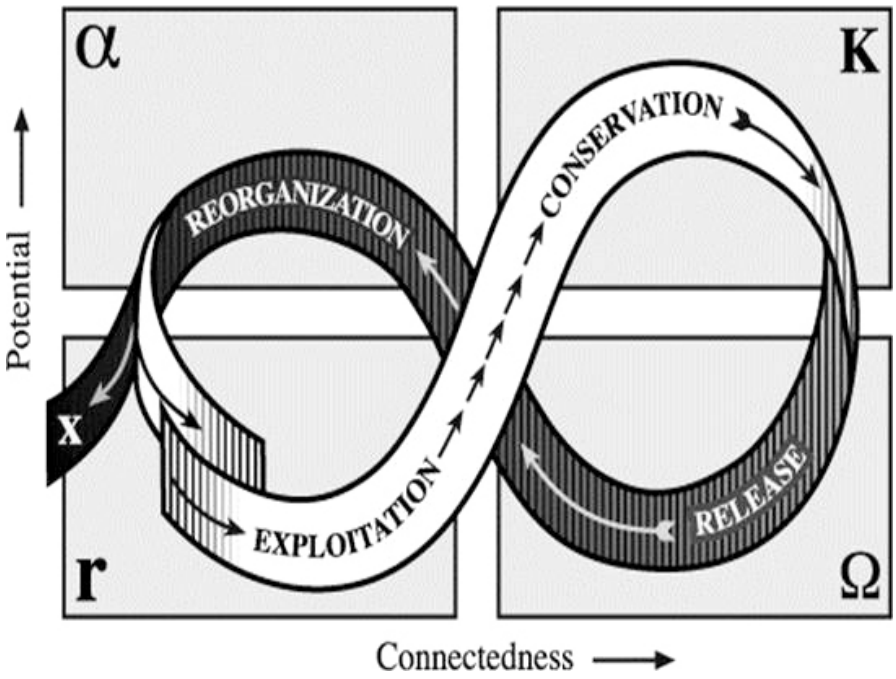
In their substantial edited volume "Panarchy: Understanding Transformations in Human and Natural Systems," Drs. Lance Gunderson and Crawford "Buzz" Holling (2002) produced groundbreaking theories in ecology and natural resiliency that persist today. They summarized how ecologists define resiliency through two aspects of system stability: engineering resilience, where stability near an equilibrium steady state is desired, and ecosystem resilience, where instabilities can change a system into a different

state of behavior (pp. 27-28). While engineering resiliency is a core concept of cyber resiliency as an innovative technology cluster, how resiliency is viewed in human and natural systems is necessary to include in this study as much of resiliency implementation occurs at the organizational and cultural level – human factors that have little to do with the technology architecture or engineering concepts.

Core to Gunderson's and Holling's resiliency theory is the adaptive cycle, developed as a framework to interpret productive ecosystems that exist in temperate regions (Gunderson & Holling, 2002, p. 33). Holling and Gunderson (2002) describe the adaptive cycle of natural and human systems in four states or phases. In the first state, the system is in a state of creative destruction or release (designated omega). The system then undergoes reorganization (designated alpha) and is renewed, followed nearly immediately by exploitation (designated "r"). A lengthy time period proceeds exploitation into conservation (designated "K"), where connectedness and stability are emphasized; for an organization, this can mean the acquisition of "skills, networks of human relationships, and mutual trust" (p. 35). The authors concluded, through extensive research connecting ecological adaptive cycles to human systems and organizations, that there are no known "exceptions to the adaptive cycle pattern" in human organizations, particularly large bureaucracies (p. 59).

Figure 2

Adaptive Cycle



Note. Adapted from the Resilience Alliance (n.d.).

As part of a complex theory of change that includes resiliency, the adaptive cycle has been described in the literature as a way to express the potential for change. Pertinent to this study on cyber resiliency are Gunderson's and Holling's interpretations and explanations for social or economic change within a human system, which are, in turn, informed by national and ecological systems of change. While engineered systems tend to follow engineering resiliency properties, humans and human-developed organizations are adaptive and complex, requiring a theory that can better explain human nature and its place in nature. Gunderson and Holling (2002) describe social change potential as the accumulated networks of relationships between people and institutions; economic potential for change could be represented by knowledge and innovations available and accessible and the ability of humans and organizations to employ foresight potential (p. 49). The literature agrees with the idea of innovation diffusion as a result of relationships, as Rodgers (2003) emphasized social systems as core to diffusion, while Sorenson (2018)

noted innovation policies depend on "thinking about the world as an interconnected structure of relationships" (p. 54).

Gunderson and Holling (2002) described four key features to characterize the adaptive cycle within the context of ecosystem resilience and can be therefore used to describe how a human system (organization) adapts to change: (1) the potential for change increases through a catalyst or series of events, (2) as the potential increases, slow changes gradually expose vulnerabilities, (3) innovations occur in "pulses" when uncertainty is great and controls are weak, (4) these innovations are tests, where some fail and others are adapted to fit the system (p. 51). These features are useful in describing how innovations are adopted at an organizational level. Annarelli, Nonino, and Palombi (2020) found that introducing and continuously developing an "organizational culture of cybersecurity" rather than "pushing the unaware adoption of high-tech tools and techniques" was a significant influencer in adopting cybersecurity innovations within an organization (p. 17). Much of the literature describes a holistic approach within an organization to employ cyber resiliency measures, as much of the implementation relies not just on information technology but all aspects of the organization, including cultural, organizational, leadership engagement, and other human factors (Gwebu et al., 2018; Sorenson, 2018; Barasa, Mbau, & Gilson, 2018; Dor & Elovici, 2016).

Linking Diffusion of Innovations and Resiliency Theory

Atwell, Schulte, and Westphal (2009) found that resilience theory and diffusion of innovations theory are complimentary in explaining how "socio-cultural context constrains, or enhances, the adoption" of innovations in their research (p. 2). Resiliency theory and Diffusion of Innovations theory are "interdisciplinary avenues of inquiry" that

frame human-decision making when faced with uncertainty and change (p. 2). Both theories are adaptable in that they can be applied not just to natural systems but to human-made (digital, mechanical) ones as well.

Rodgers's (2003) diffusion of innovations theory describes how innovative ideas, such as a new technology, diffuse within a social system to enact or react to change; the innovation-decision process describes how an individual or organization knows, opinionates, decides, and confirms the implementation of that innovation. The four key features of the adaptive cycle (Gunderson & Holling, 2002) describe how an innovation is used within an ecological or social system to deal with change or adapt to a new state of existence. Both theoretical frameworks are valuable to understanding how individual decision-makers, or organizational groups, navigate relevant limiters, enablers, and tasks to adopt cyber resiliency as a technology innovation and ultimately deal with the always-changing cyber threat landscape.

Synthesis of the Literature and Notable Gaps

Based on an extensive review of the available literature, common themes emerge in understanding influences in cyber resiliency as an innovation adoption within an organization’s cybersecurity program. Appendix A provides a matrix view of synthesis derived from the literature, while Table 4 summarizes the synthesis to support this section. This section discusses each influence noted in the literature, how they were presented as limiters or enablers of cyber resiliency adoption, and how these influences can be visualized as a conceptual framework for exploring the innovation-decision process, with relevant excerpts from the literature. In addition, notable gaps and research recommendations from the literature are also discussed.

Synthesis of the Literature on Cyber Resiliency

The ten scholarly works that comprise the most influential literature discovered to date on cyber resiliency, as noted in Table 4, described several innovation-decision and operational influences on cyber resiliency that the researcher grouped into nine general categories: (1) technical factors, (2) cultural influences, (3) organizational policies and leadership, (4) workforce and skills, (5) knowledge management and information access, (6) industry and competitiveness, (7) vendor and third-party support, (8) legal and regulatory influences, and (9) resources and funding.

Table 4

Synthesis Summary

Innovation-Decision Influences on Cyber Resiliency	**Number of Literature References**	**Authors Declaring or Inferring Influence as Significant**
Technical Factors	9	Kott & Linkov (2019) Carayannis et al. (2021) DHS CRR (2018)
Cultural Influences	7	Carayannis et al. (2021)
Organizational Influences	8	Kott & Linkov (2019) Barasa et al. (2018) Butler & Brooks (2021) Carayannis et al. (2021) Sharkov (2020)
Workforce/Skills	6	
Knowledge Management and Information Access	8	Linkov et al. (2013) Ferdinand (2015)
Industry and Competitiveness	5	Annarelli et all. (2020)
Vendor and Third-Party Support	4	DHS CRR (2018)
Legal and Regulatory Influences	3	
Resources and Funding	6	Kott & Linkov (2019) Barasa et al. (2018) Groenendaal & Helsloot (2021)

Technical Factors. Perhaps predictably, nearly all of the key works, 9 out of 10, discussed technical factors such as network topology, implementation frameworks and matrices, engineering and design, and innovative concepts that support resiliency such as zero-trust architecture; technical factors were featured prominently in three of the works in particular with focuses on cyber resiliency technical implementation, challenges, and enabling features (Kott and Linkov, 2019; Carayannis et al., 2021; DHS CRR, 2018). Linkov and Kott (2019) describe approaches to improving cyber resilience from a primarily technical perspective, particularly in managing the complexity of the interconnected systems, designing the system topology to make resilience inherent, adding additional functional capacities, designing components to revert to a known safe mode, segmenting network nodes and providing buffering, building and preparing active agents to act on resiliency procedures, consider adversarial capabilities and build to withstand them and conduct high-fidelity and simulation-based analysis to reveal negative impacts (pp. 14-16).

Petrenko (2019) recommended, given the need for resiliency for systems under direct threat of APT actors, and the realities for business optimization and cost-control, the following five key tasks: (1) organizations develop programs for managing business sustainability; (2) sustainability programs should not conflict with regulatory frameworks; (3) sustainability programs should utilize resiliency guidelines such as NIST SP 800-160, MITRE Cyber Resiliency Engineering, ISO 22000 series standards for business continuity management, and national level standards as required; (4) ensure the sustainability program is sustainable through economic analysis and activity-based costing; (5) apply recommendations and guidelines from SANS Institute and Disaster

Recovery Institute International (DRI), and other research organizations, to define and develop sustainability management objectives and technical architectures (pp. 405-408). Petrenko's recommendations blend technical and organizational methods to achieve cyber resilience, a common theme throughout the literature in describing improvement methodology for resiliency and reinforces the concept of a blended approach that does not rely on technical factors.

The DHS CRR (2018) noted in their study that several participants describe technology refresh cycles that are too lengthy, resulting in insecure baselines, operating systems, and information technology architecture that becomes unsustainable. The team noted that this is a key limiter in enabling cyber-resilient network topologies, particularly in the information and communications technology (ICT) industry and critical infrastructure where the critical systems are ICS/SCADA (pp. 16-17). Technical limitations such as these are cited throughout the literature as critical shortcomings in adopting new innovations or modernizing outdated network architecture to enable more resilient technology.

Cultural Factors. Cultural factors include the workforce's prevailing culture, cybersecurity awareness and agency, cultural adaptability to change, and a work culture conducive to new ideas and learning. 6 out of 10 key articles noted cultural influences as significant for cyber resiliency. In one study, socio-economic factors (cultural influences on a societal scale) were cited as particularly substantial in cyber resiliency alongside technical and organizational influences within their proposed AMBI-CYBER framework (Carayannis et al., 2021). Barasa et al. (2018) noted two key cultural factors within an organization, observed from the authors' review of available literature, that contributed to

resiliency: first, that resilient organizations consider challenges as learning opportunities, and second, that organizations maintain a strong emphasis on creativity and innovative solutions (p. 499). Posey et al. (2014) cited several studies to indicate culture matters a great deal in technology use within an organization and concluded that the traditional view of information security as a technical concern is flawed; "security is both a technical and a behavior matter" (p. 564).

Carayannis et al. (2021) proposed linking organizational ambidexterity - where organizations balance exploration and exploitation of their resources - with cybersecurity concepts to produce an “AMBI-CYBER architecture” centered around the 7Ps stage gate model: patient, persistent, persevering, proactive, predictive, preventative, and preemptive. The authors then mapped the 7Ps to the NIST cybersecurity framework of identify, protect, detect, respond, and recover. The authors concluded that there is a need for increased collaboration and integration between public and private entities to enhance cybersecurity from a societal perspective (not just technical, but protecting against societal disinformation, attacks on democratic processes, etc.). Ultimately, the authors suggest that cyber resilience as a strategic concept relies on further exploring research and evidence-based findings to refine a combined cybersecurity model that takes into account technical, organizational, and socio-economic factors (Carayannis et al., 2021).

Organizational Influences. Organizational influences can include security or resilience governance, management of risks and risk-based processes, leadership or executive buy-in on cybersecurity concepts, innovativeness of the organization, as well as general policies, procedures, standards, and guidelines of the organization that have been found to affect resiliency. Some technology-related factors could also be considered

within the organizational policy and leadership group, such as how resiliency is measured alongside other key technology or security-specific metrics; Linkov et al. (2013) noted that the dominant paradigm of quantitative risk assessments in system design, and the fragmentation of resilience knowledge into separate disciplines, are significant barriers that have inhibited progress in resilience measurement of complex systems (p. 10108).

The literature had a great deal to say about organizational policies and leadership influences on cyber resiliency and cybersecurity in general, with 8 out of 10 key articles noting limiters or enablers related to leadership practices, governance, processes, and planning, and five works cited organizational influences as particularly significant (Linkov & Kott, 2019; Barasa et al., 2018; Butler & Brooks, 2021; Carayannis et al., 2021; Sharkov, 2020). Organizational structure and processes were noted as significant factors in information security investments and overall management (Dor & Yuval, 2016, p. 11; Rocha Flores, Antonson, & Ekstedt, 2014).

Ferdinand (2015) noted that organizations that are more aware of the dangers of complacency and recognize the need for organizational learning about changes in cyber threats and defensive techniques are potentially more likely to move through progressive stages of security maturity toward cyber resiliency (p. 190). Additionally, the size or success of the organization may not directly correlate to a commiserate level of cyber resilience or security maturity, suggesting that "the majority of [Financial Times-Stock Exchange] 350 companies are not currently cyber resilient" (p. 191). Ferdinand's conclusions on awareness and organizational learning indicate sizable organizational influences in adopting cyber resiliency.

Leadership practices are a critical enabler for organizational resilience, specifically engaged and dedicated senior leaders with a clear and shared vision for the organization, practicing inclusive decision-making and transparency, and with leadership characteristics aligned to the complex adaptive nature of systems (Barasa et al., 2018). Rutt (2020) noted within the annual Stott and May study on cybersecurity that 54% of executives responding to their survey noted cybersecurity as a strategic priority, with high-growth mid-market firms reporting 83% towards strategic significance and a sizable increase from previous years (p. 7).

Workforce and Skills. 6 out of 10 key works cited workforce-related influences on cyber resiliency, such as the “skills gap” indicating a lack of qualified and interested information security professionals to assume key technical and managerial roles within an organization (Rutt, 2020; $(ISC)^2$, 2021). Annarelli et al. (2020) discovered, through multiple case analyses, that workforce training and awareness, as well as accelerated adoption of artificial intelligence-driven cybersecurity tools, were regarded by the study participants as the future of cybersecurity and directly contributed to cyber resiliency of their organizations (pp. 13-14). Lallie et al. (2021) described the effect the COVID-19 pandemic, beginning in March 2020, had on the workforce through "mass quarantine of staff and the measures put in place to facilitate remote working" that threatened technology resilience and socio-economic structures (p. 13). A skilled workforce was noted as a "critical contributor to resilience." A lack of subject matter expertise in operational technology (OT) cyber systems was found to be a significant challenge in adopting and sustaining resilient industrial control systems within U.S. critical infrastructure (Barasa, Mbau, & Gilson, 2018, p. 499; DHS CRR, 2018, pp. 22-23).

Knowledge Management and Information Access. Access to information and how individuals or organizations categorize, organize, and share knowledge was noted as a key influence on cyber resiliency, with 8 out of 10 works citing influences of knowledge management and information access on cyber resiliency adoption. Two works within the literature reviewed noted knowledge management and access to information as key influences (Linkov et al., 2013; Ferdinand, 2015). Linkov and Kott (2019), in their edited volume on cyber resiliency, observed that a lack of sharing best practices between organizations led to the random adoption of cyber resilient practices (p. 65). Keys and Shapiro (2019), within Linkov and Kott (2019), also described information sharing as key to increasing cyber resilience (p. 85). Barasa et al. (2018) noted that information management, or knowledge management, enables organizational resilience by ensuring "strategies, organizational goals, and achievements are effectively communicated across the organization" (pp. 497-498). Dwivedi et al. (2020), when describing information management during the COVID-19 pandemic, concluded that while access to information is important, safe and reliable access is equal, if not more, paramount (p. 10).

Sorenson (2018) noted that open-access journals and information repositories received more citations and thus enjoyed wider influence than articles behind paywalls. Such lack of access and re-sharing of academic research could greatly influence how-to knowledge and innovation awareness (Rodgers, 2003). Additionally, partnerships between the federal government and the private sector, and the inclusion of all stakeholders, are key enablers of information sharing and, ultimately, resilience adoption (DHS CRR, 2018, pp. 23-24). It is important to note that a key conclusion and recommendation by the DHS CRR team (2018) is to increase information sharing and

public-private partnerships throughout all levels of government in the United States (pp. 34-36).

Access to relevant knowledge and information was noted to be of particular influential value in the innovation adoption of national security technology, along with access to resources and incentives to adopt. Iles et al. (2017) noted that barriers and incentives significantly influenced adoption of national security technology, such as portable radiation detectors within private industry. Specifically, barriers such as cost, usability, technology maturity, the potential for false readings or inaccurate data, and privacy concerns were cited as barriers. Incentives included government-provided training, financial rewards for adoption, and public recognition of adoption (p. 2248). A case study such as this may be useful in explaining the adoption of cyber resiliency as an innovative technology cluster within U.S. critical infrastructure and key industries that the federal government deems of national security importance to protect.

Industry and Competitiveness. What industry vertical or sector an organization operates within, and how it maintains competitive advantage within that industry, was found within the literature to be an influential factor in cyber resiliency, with 5 out of 10 key works noting influences, and one work, in particular, citing significant influences in managing cyber resilient systems. Annarelli, Nonino, and Palombi (2020) described, after an extensive review of available literature, three contextual factors contributing to the management of cyber resilience systems: (1) infrastructure, whether critical or non-critical, (2) industry, whether customer-based (business to business) or consumer base (business to consumer), and (3) ownership, public or private. The interdependencies and management characteristics within these three factors contributed significantly to how a

resilience strategy is formulated by management, either proactive or reactive, and the specific technology innovations selected (pp. 2-3).

Infrastructure, industry, and ownership also affect the various types of cyber threats facing an organization, affecting the investment decision-making process for cybersecurity, including cyber resiliency measures. Dor & Elovici (2016) noted that the risk management process, the decision-makers themselves, potential and realized information security threats, prioritization and budgeting processes, and how cyber-aware the organization have major effects on the information security investment decision-making process (p. 11). Petrenko (2019) notes that systems under direct threat of APT actors find an increased need for cybersecurity investment, including resiliency. The DHS CRR team (2018) recommended that, for the subset of critical infrastructures known as lifeline sectors or strategic infrastructures – electricity, water, transportation, communications, and financial services – prioritization of federal aid in adopting cyber resilience is needed due to threats these sectors face from a "coordinated cyber-attack on the United States" (p. 6).

Vendor and Third-Party Support. How the organization's adopted technology architecture is supported through vendors and third-party organizations – such as managed cloud providers, outside consultancies, or staffing agencies – was found to be an influence on the cyber resiliency innovation-decision process, mainly when confirming an investment decision and continuing its use, with four of the ten key works identifying related influences (Kott & Linkov, 2019; Butler & Brooks, 2021; DHS CRR, 2018; Groenendaal & Helsloot, 2021). Of the literature reviewed, the DHS CRR team (2018) drew significant conclusions within this influence group in understanding cyber

resilience adoption within critical infrastructure, mainly that vendor selection is limited, proprietary code "outlives" its developers and leaves operational systems without adequate support, and vendors aren't designing software, hardware, or services with generally-accepted cybersecurity engineering principals (pp. 17-21).

Accenture (2018), a Global Fortune 500 professional services company operating a subsidiary firm (Accenture Federal Services LLC) as a U.S. federal and defense contractor with knowledge of cybersecurity trends within the public sector, described six steps for improved cyber resiliency in which "demand application security by design" was included amongst the more technical recommendations (p. 6). The report also noted a significant weakness in "extended ecosystem" and "third-party cybersecurity clauses" within federal clients, citing that 20 percent of federal respondents to a proprietary study have enforced active cybersecurity clauses in provider and partner contracts (Accenture, 2018, p. 11). It is clear from the key literature, informed by further academic and industry sources, that support gained or lacking from vendors and contractors is significant in the innovation-decision process for cyber resiliency.

Legal and Regulatory Influences. Of the nine influence groups derived from the key literature on cyber resiliency, legal and regulatory challenges or opportunities appeared the least discussed, with three of the ten key works citing influence. In particular, Keys and Shapiro (2019), within Kott and Linkov (2019), described understanding and managing legal and regulatory requirements for cybersecurity, particularly privacy and civil liberties obligations, as a key best practice in adopting a resilience framework (pp. 73-74). Butler and Brooks (2021) extensively described regulatory risk and requirements in their review of operational resilience within the

financial industry. In their argument, they made regulatory compliance a core recommendation for financial sector firms to transform into resilient complex adaptive systems (RCASs). These conclusions indicate that legal and regulatory influences are tied to industry verticals and geographic locations where various laws and regulations apply varying pressure to innovation-decision influences. Nevertheless, legal and regulatory influences can become significant in industries and regions where requirements for data-centric cyber resiliency, or lack thereof, is a concern for decision-makers.

Resources and Funding. How an organization will resource, cyber resiliency efforts were influential, with six of the ten key works citing resourcing and funding as a factor in adopting and adequately managing cyber resiliency. Access to adequate material resources, specifically financial and technological, was predictably found to be a key enabler in organizational resilience; that is, an organization's financial position was key (Barasa et al., 2018). Kott and Linkov (2019) caution against the costs of cyber resilience innovations when viewed through the lens of cyber risk management, balancing realistic threats and impacts to an organization compared to the resources required to defend or become resilient against emerging threats and technologies with "uncertain intensity and frequency" (p. 7). Groenendaal and Helsloot (2021), in examining a case study of cyber resiliency during the COVID-10 pandemic in the United States, found that "having money at hand" for a faster cyber defense and resiliency response is a "a factor of greater importance" than preparing for the event itself. This statement supports their broader conclusion that an effective response to an incident is paramount (Groenendaal & Helsloot, 2021, p. 443).

Beyond funding, resources also include staffing, hardware and software architecture, and standard operating procedures to assist security practitioners in ensuring the defense and resiliency of the organization's technology. Keys and Shapiro (2019), within Kott and Linkov (2019), cite a study conducted by the Ponemon Institute in which 62% of responding information security practitioners indicated they did not have the resources to understand or defend against external threats. Organizational cyber defenders who can devote appropriate resources to defend against security threats upon detecting an adverse event are key to cyber resilience (Keys & Shapiro, 2019, p. 85).

Notable Gaps in the Literature and Research Recommendations

While the literature review provided a thorough view of influences on cyber resiliency, there are notable gaps and research recommendations in the literature. The fact that the chosen literature spans 20 years or more, despite a stated preference for more current dated works, is indicative of the inevitable research gaps, both in the social science of organizational leadership as it pertains to information technology, cybersecurity, and adoption of cybersecurity concepts as innovations as well as the relatively nascent nature of cyber resiliency as an innovation itself. This section discusses gaps, disagreements, and recommendations on the chosen theoretical framework for this study and cyber resiliency.

This study's theoretical framework has criticisms and calls for directional change, even after hundreds of empirical studies across over 70 years of research tradition (Rodgers, 2003). Kincaid (2004), cited within Dearing and Singhal (2020), described researching diffusion of innovations as comprehensive, comprising both strengths and weaknesses due to its nature as not a singular theory but a "model, framework, or

paradigm" that can be supported or refuted by a number of supporting theories within the social sciences (p. 307). Iles et al. (2017) note a research gap in the "complex interplay of variables" within the diffusion of innovation compared to the variables in the adoption process. Additionally, it is notable that the most recent edition of Rodgers' (2003) seminal work on the diffusion of innovations theory is 19 years old as of this study and needs a review of the most recent diffusion studies and modern technology.

Dearing and Singhal (2020) agreed with this observation. They argued for new directions in diffusion studies that address how innovation is disseminated, implemented, sustained, and positive deviance (PD). It is important to note that while this study employed the diffusion of innovations theory – specifically the innovation-decision process model – as the primary theoretical framework, it also leveraged the supporting Resiliency Theory (Gunderson & Holling, 2002) and addresses Dearing and Singhal's (2020) recommended research direction by pursuing a study within implementation science: "the study of what happens before, and after, adoption occurs, especially in organizational settings" (Dearing & Singhal, 2020, p. 309).

Kott and Linkov (2021), in a newer article following their 2019 edited volume on the same subject, predict confidence in cyber resilience will be challenged as AI-enabled tools and autonomous agents are further embedded within information systems, advocating for further research on these still-nascent topics. Annarelli, Nonino, and Palombi (2020) described a research gap in correlating contextual influences on cyber resiliency (infrastructure, ownership, and industry were specifically cited) to adopting managerial practices. This study aimed to address this research gap by conducting a

diffusion study exploring influences on the innovation-decision process for cyber resiliency.

Chapter Conclusion

This chapter encompassed an extensive review and synthesis of the available literature on cyber resiliency, diffusion of innovations theory, resiliency theory, and key topics related to this study. The nine influence groups identified in the synthesis matrix (see Appendix A), as summarized in Table 3, represent significant limiters or enablers within the innovation-decision process for cyber resiliency. With the notable exception of the “legal and regulatory influences” group, all influence groups were a focus point for one or several works reviewed. While the "technical factors" influence group featured nearly the entire matrix (nine out of ten articles), organizational factors and leadership influences were discussed within five articles as particularly significant influences on cyber resiliency. This indicates that most authors view organizational influences as influential, highly influential, or critical to adopting cyber resiliency.

In comparing this literature synthesis to the five attributes of innovation as described by Rodgers (2003), and the two attributed particularly important in explaining adoption rate (relative advantage and compatibility), the conclusions that can be drawn about innovation-decision influences represent the importance of facilitative leadership, governance, and management when deciding to adopt cyber resiliency as an innovation, on par with or perhaps surpassing technical factors. Completing this literature review and subsequent synthesis analysis greatly informed this study by focusing interview questions around these influence groupings, validating the methodology discussed in Chapter 3, and demonstrating a correlation between the theoretical framework and the literature.

Furthermore, the gaps and future research recommendations noted within the literature demonstrated the significance of the study in the field of cyber leadership.

Chapter Summary

This chapter presented a literature review of cyber resiliency. A historical overview was presented that included how resiliency is viewed in ecosystems and engineering, human systems and organizations, how both concepts converged into cyber and information technology resiliency, and how cyber resiliency is featured within the U.S. as a component of national security strategy. A review of the theoretical framework started with understanding the Diffusion of Innovations Theory and the Innovation-Decision Process (Rodgers, 2003), Resiliency Theory and Adaptive Cycles in natural and human systems (Gunderson & Holling, 2002), and how the two theories are linked in describing resiliency measures within organizations and technology. The researcher discussed a synthesis of the literature and notable gaps, followed by concluding remarks.

Chapter 3 will present the research method and design appropriateness. A discussion of population, sampling, and data collection processes will follow. The validity of the study, both internal and external, will be discussed. Finally, a discussion on data analysis methods, organization, and clarity will be presented, followed by a chapter summary.

Chapter 3: Method

The purpose of this study was to better understand the innovation-decision process for cyber resiliency and what influences affect the adoption or rejection of cyber resiliency innovations at the organizational leadership level. This chapter reviews the research method and appropriateness of the study design. The target population, study sampling, data collection procedures, and rationale are discussed. The validity of the data and the chosen instrumentation, both internal and external, are also provided, followed by a review of how the research data will be analyzed. The chapter concludes with a summary and an outline of the next chapter on the study's pilot and results.

Research Method and Design Appropriateness

The method used for this study involved mixed methods, in which the researcher conducted a quantitative internet-based survey of senior, director, and executive level cybersecurity professionals on cyber resiliency adoption within their organizations and enriched with in-depth interviews of chosen survey participants with relevant decision-making experience. A convergent mixed-method design integrates qualitative and quantitative data within a research study, using open-ended qualitative data with closed-ended questions such as those found on questionnaires (Creswell & Creswell, 2018, p. 14). Based on a review of available designs and a thorough understanding of studies involving the diffusion of innovations theory and resiliency theory, the design follows the research tradition for the diffusion of innovations theory and is appropriate for studying the innovation-decision process in particular.

Research Method

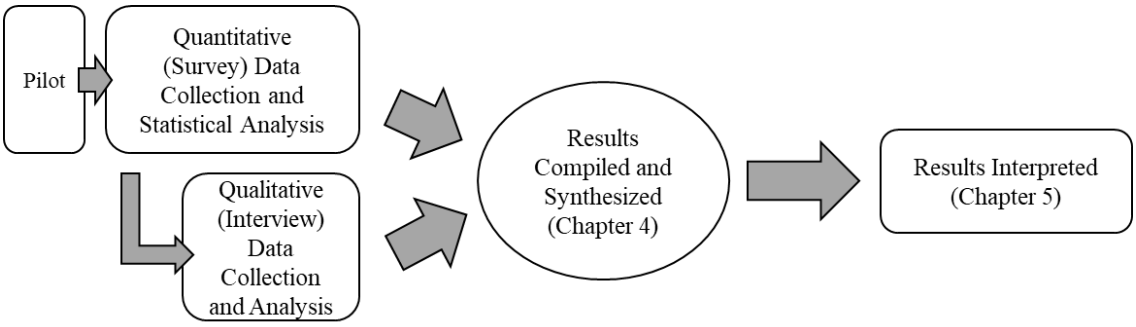
In selecting a method for this study, the researcher first conducted a literature review to understand the problem, sharpen preliminary considerations, and assume a broader perspective on the topic (Yin, 2016, pp. 72-73). Such a review represents a *comprehensive* review, which influenced the design and methodology discussed in this chapter, and refined questions that can be used to tune the research instrument (Yin, 2016). The researcher then tuned and implemented an internet-based survey instrument to collect generalized opinions amongst a target population to achieve a sample size of statistical significance. Concurrent with the survey, the researcher conducted in-depth interviews of selected participants who agreed to follow-up discussions via the survey vehicle. The purpose was to collect experiential data through shared lived experiences of the individuals who have experienced cyber resiliency innovations within an organization.

Through survey research, the quantitative portion of the design allowed for studying trends and opinions through generalizing from a sample to a population and is appropriate in validating or invalidating the influences found during the literature review (Creswell & Creswell, 2018, p. 12). However, in designing this study, the researcher identified variables that cannot be easily measured, such as complex influences upon a social system and individual decision-makers, that warrant a qualitative approach (Creswell & Poth, 2018, p. 45). Adopting a mixed-methods approach using a pragmatic worldview comprised the most appropriate design through which a broad survey can generalize results to a population, then open-ended interviews help explain the initial quantitative survey (Creswell & Creswell, 2018, p. 17).

The overall design for this study followed a convergent (one-phase) design in which quantitative and qualitative data were collected near-simultaneously, with the qualitative sample derived from the quantitative sample (N). The results were then compiled, synthesized, and compared. Qualitative and quantitative instruments (closed-question and open-ended interview questionnaires) were tuned to the same lines of inquiry to match the research questions. A visual of the method is provided in Figure 3, derived from recommended design concepts in Creswell and Creswell (2018).

Figure 3

Convergent Mixed-Methods Design of Study



Design Appropriateness

This design was appropriate to the diffusion of innovations theory research tradition. Rodgers (2003) traced research traditions of nine main categories of diffusion studies, which cover a wide variety of topics and interests, and often use survey interviews and statistical analysis to investigate eight main types of diffusion research, some of the most popular types investigating opinion leadership and innovativeness of individuals and organizations (pp. 43-101). Rodgers challenged future researchers to "dig deeper in directions that theory suggests" (Rodgers, 2003, p. 101). Ryan and Gross (1943) were described, within Rodgers (2003), as the most influential diffusion study that investigated hybrid seed corn adoption in Iowa; they established what has become known

as the "customary research methodology to be used by most diffusion investigators," described as "retrospective survey interviews" in which the researchers sought to understand how an innovation diffused throughout a specific community of practice (Rodgers, 2003, p. 33). Additionally, researching leadership factors and organizational decision-making holds strong philosophical and sociocultural contexts by which a qualitative research design has proven to be a conventional and proven approach (Creswell & Creswell, 2018).

Yin (2016) described eight choices for designing research studies with qualitative characteristics and noted that not all studies start with a concrete research design (p. 84). Furthermore, the pragmatist orientation of the researcher led to a balanced preference for trustworthiness, validity, and triangulation of the data within the study (Yin, 2016, pp. 85-90). Thus, starting with a comprehensive literature review to understand the problem, refine the research questions, and forming a literature synthesis resulting in the description of the nine influence groups upon cyber resiliency decision-making (see Appendix A) was appropriate to influence the study's direction and decision to proceed with a mixed-methods approach.

Ultimately, a mixed-methods approach accomplishes the study's goal and represents the optimum choice for investigating influences upon technology innovation adoption within an organization. A mixed-method approach offers data and theory triangulation and increases the trustworthiness of the study's analysis and subsequent conclusions (Yin, 2016, pp. 86-87). Increasing the study's credibility increases the chances that this study will be viewed as a meaningful contribution to cybersecurity leadership for both public and private institutions that will ultimately benefit national

cyber defenses and the protection of critical infrastructure. Additionally, a review of existing literature on cyber resiliency identified nine generalized influences on cyber resiliency adoption within an organization best explored with a quantitative approach. However, these influences represent a complex and adaptive phenomenon in human decision-making and merit a qualitative approach to understanding lived experiences. When faced with a research problem that seeks to "both generalize the findings to a population as well as develop a detailed view of the meaning of a phenomenon," a mixed-methods approach is optimal (Creswell & Creswell, 2018, p. 19).

Research Questions

The researcher hypothesized a relationship between influence factors on cybersecurity leadership and cyber resiliency adoption. The researcher investigated two primary research questions about influence factors on adopting cyber resiliency and the innovation-decision process. The nine influence categories identified in the synthesized literature review were vital in developing the closed-question survey instrument and qualitative, open-question interview materials.

Research question one (RQ1) asks: What factors support the adoption of cyber resiliency in an organization ("enablers")? In this first research question, the researcher aimed to identify influences that proved beneficial or complementary to adopting cyber resiliency. Research question two (RQ2) asks: What factors limit the adoption of cyber resiliency in an organization ("limiters")? This second question sought to identify influences that prevented or hindered the adoption of cyber resiliency. The study's mixed-method design, using both open-ended and closed-ended questions, supported both research questions.

Population and Sampling

The researcher sampled a diverse population of senior, director, and executive-level information security professionals in the United States. People with experience in cyber resiliency implementation and decision-making were required to understand the research problem, significantly reducing the number of eligible participants in the population. The researcher used purposeful sampling techniques to find suitable study participants by disseminating the survey instrument to groups and networks catering to senior, director, and executive-level cybersecurity decision-makers. Palinkas et al. (2015) described criterion sampling as most common in implementation research involving mixed methods, in which participants are selected that are "especially knowledgeable about or experienced with a phenomenon of interest" (p. 2).

Suitable sample size was calculated using the G*Power method and software. Hyun (2021) noted that studies with inappropriate sample sizes or insufficient power calculations do not provide accurate estimates and can lead to incorrect conclusions (p. 1). Using a software calculation tool, such as G*Power, provides accessibility to the researcher to reach a significant power within the study while staying within cost-effectiveness boundaries (Hyun, 2021).

The sample size (N) for the quantitative survey portion of the data collection methodology was estimated at 82 participants to achieve statistical significance, allowing for 5% type I (false positive) error probability, 20% type II (false negative) error probability, 30% (medium) effect size, and 80% power. Value estimates, such as effect size and desired power, were derived from previous doctoral studies using a quantitative, non-experimental, descriptive-correlational survey approach within the social sciences

where participants were sampled through a purposive selection of self-identified expertise (Thielfoldt, 2022, pp. 4-7). Pearson's *r* correlation was consulted to determine common effect size based on a small to medium effect (.2 to .5), used to measure the association between quantitative variables. A type I error, or false positive, occurs when rejecting a null hypothesis when it is true, and a type II error, or false negative, occurs when the null hypothesis is accepted when the alternative is true (Hyun, 2021). The sample size was determined through an *a priori analysis* within the G*Power software, version 3.1.9.7. Table 5 contains the parameters used in the software to achieve the sample size used for this study.

Table 5

*G*Power a priori Power Analysis Parameters*

Parameter	**Result or Input**
Tails	Two
Effect size (ρ)	0.3
significance level (α)	.05
power (1-β)	0.80
Total sample size (output)	**82**
Actual power (output)	**0.8033045**

The sample size for the qualitative data used in this study, namely experiential narratives from in-depth interviews using open-ended questions along the same inquiry lines as the quantitative data set, was derived from the quantitative sample size itself. In a convergent, one-phase mixed methods design, including the sample of qualitative

participants in the larger quantitative sample is common and preferred to facilitate comparison (Creswell & Creswell, 2018, p. 219).

Data Collection

Nardi (2018) described that reliable and valid information in survey research depends on a well-written questionnaire, dissemination method, and appropriate instrument selection (p. 72). An outline of the questionnaire used for the quantitative survey instrument is provided in Appendix B. The type of data collected within the quantitative instrument included nominal and ordinal measures and collected information on the research variables identified in Table 1: De, O, and I representing independent variables, and Di as the dependent variable. The qualitative data collected through the interview questionnaire included narrative, open-ended questions from which themes and key insights can be coded and analyzed alongside the quantitative data.

The survey instrument used was SurveyMonkey, a leading cloud-based survey platform for corporate, academic, and personal use. This instrument was chosen based on its ability to meet the study's data collection objectives through a modified Likert scale, nominal and ordinal measures, and customized questions with narrative responses. Additionally, the instrument included the ability to statistically analyze and graphically visualize the data directly on the platform with native analytical tools while allowing the ability to export the data for offline analysis through additional analytic software tools. The chosen instrument has been used in published academic studies and is considered validated through extensive use in the research community. To validate the instrument, a pilot study was conducted on a smaller sampling of cybersecurity professionals.

The researcher used personal and professional networks of cybersecurity leaders through social media, organizational memberships, professional associations, and communities of practice to achieve the sample size. A link to the survey was promulgated to prospective participants. The first section of the survey contained detailed information about the study's purpose, objectives, and methodology and required an agreement to informed consent before continuing. The following section used nominal measurements to collect demographic information, with the first two questions determining career level and years of experience to ensure the target population was reached; if "internship/student," "entry," or "associate" career levels were chosen by the participant, the survey concluded, and no further data was collected. The entire survey was designed to be completed within 18-22 minutes, divided into five sections of 37 questions in total (not including informed consent), and included an informed consent and opt-in feature at the end for those agreeing to the qualitative in-depth interview portion of the study.

The qualitative interview questionnaire is provided in this study as Appendix C. The interview protocol leveraged formatting and guidance from Creswell and Poth (2018) with five to seven open-ended questions allowing participants to describe their experiences without leading questions or nominal measures (pp. 165-167). The qualitative data was collected via remote teleconferencing through internet-based software or telephone calls. The interviews were limited to one hour, with data collected limited to the information outlined in Appendix C to ensure the confidentiality and authenticity of the experiential, narrative data.

Protecting the confidentiality and integrity of the data was important in this study. All survey data was encrypted and kept confidential within the SurveyMonkey platform,

the researcher's personal computer or the Capitol Technology University's Microsoft 365 OneDrive storage provided for student use. The researcher utilized the rule of least privileged by maintaining sole custody of all accounts or hard drives containing the data. Correspondence between the researcher and participants was conducted through Capitol Technology University's Microsoft 365 Outlook for student use, with no third parties included.

The researcher could have used other survey research methods beyond computer-assisted and web-based to collect this data, such as self-administered questionnaires, interviews, or telephone surveys (Nardi, 2018, pp. 72-76). A computer-assisted and web-based methodology was the most suitable for this study's quantitative data collection. It was the most expeditious and cost-effective, took advantage of statistical analysis tools provided by the instrument's service provider, and allowed for data exportation for other analysis methods. The study also used the interview method to collect qualitative data about the lived experiences of participants who opted into a virtual interview with the researcher. This allowed for the triangulation of multiple data sources to achieve the study goals.

Validity and Legitimation

Creswell and Creswell (2018) describe validity as the ability to draw meaningful conclusions and valid inferences from data collected by the study instrumentation; a strategy for demonstrating validity ensures accuracy in the findings and convinces readers of the same (p. 251). Internal validity threats occur when the study's procedures inhibit the researcher from drawing accurate inferences from the data. At the same time, external validity threats occur when inaccurate conclusions are drawn from sample data

that is then applied to a larger population (Creswell & Creswell, 2018, pp. 167–172). Threats to validity are well documented by several notable scholars, including Onwuegbuzie (2003) in what is now known as the Quantitative Legitimation Model examining internal and external validity threats to quantitative research from data collection to analysis, the seminal work by Shadish, Cook, and Campbell (2001) on quantitative validity, and finally, Maxwell (1992) which explored validity challenges in qualitative research (Onwuegbuzie & Johnson, 2006). Mixed method research presents significant validity challenges as threats to validity from quantitative and qualitative methodologies are present, namely representation, integration, and legitimation (Onwuegbuzie & Johnson, 2006, pp. 51–52). Additionally, Onwuegbuzie and Johnson (2006) recommend that mixed method researchers refer to qualitative "validity" as "legitimation" to not detract from participants' worldviews or attempt to label lived experiences as invalid for study (p. 55).

The researcher identified the primary internal validity threat to this study as the selection process itself, where specific characteristics of the participants predispose them to particular outcomes, or the methods used to select participants may be limiting the validity of the narrative. The survey was distributed across multiple professional channels and not limited to one or two groups to maximize equal distribution and thereby limit selection-based internal validity threats. Cybersecurity professionals are typically high-performing and highly educated individuals with numerous credentials, and there may be a predisposition to exaggerate their comments or misrepresent their level of expertise through their study responses. The researcher attempted to mitigate this validity risk in

the quantitative survey through informed consent and demographic questions that validated the participants' expertise and experience.

A key challenge to the validity of mixed methods research designs is the problem of integration, where quantitative and qualitative data are converged to corroborate findings of the same phenomenon, a concept described as *sample integration legitimation* (Onwuegbuzie & Johnson, 2006). Sample integration legitimation is reasonably achieved through this study's convergent mixed method design, deriving the qualitative sample from the larger quantitative sample to ensure accurate meta-inferences. The researcher acknowledges unequal sample sizes due to the qualitative sample derivative of the larger (n) quantitative sample inherent to the study's design.

Ultimately, the credibility of this study is accomplished through triangulation and converging lines of inquiry. Triangulation is achieved by using the same concepts for the study's quantitative and qualitative portions, as Creswell and Creswell (2018) recommended to maintain validity in a convergent approach. A joint display to visualize and interpret the data was used to converge the data by theme and influence category, converging on the primary research questions of enabling or limiting factors in the cyber resiliency innovation-decision process.

Data Analysis

Creswell and Creswell (2018) recommended a three-step approach to data analysis in a convergent (one-phase) mixed-methods design: qualitative data coding, quantitative data statistical analysis, and data integration (p. 219). In the first step, the researcher coded the qualitative data collected congruent to the influence categories discovered in the literature review and coded it into the closed-question quantitative

survey. This coding ensures data can be interpreted similarly and qualitative and quantitative data can be merged, displayed, and interpreted effectively (Creswell & Creswell, 2018, pp. 219–220).

In the second step, the researcher analyzed the quantitative data using SPSS data export and analysis through the Intellectus Statistics software. This analysis aimed to determine the statistical significance of limiting or enabling influences on cyber resiliency. Nominal and ordinal measures from the survey were visualized, and descriptive statistics were presented via tables. The dependent variable, or outcome, was adjusted to be dichotomous (adoption or rejection) to fit a binary model. Two-directional hypothesis testing was conducted against the quantitative data collected through a binary logic regression.

The McFadden (1974) model was chosen over others because the outcome was dichotomous, and the R^2 value was calculated first to determine that the model fit the data; the McFadden R^2 method provides for a test that minimizes variance and offers a straightforward method for logistic regression estimation (Smith & McKenna, 2013). A chi-square test was used to compare observed with expected results better understand the relationship between influence factors and the dependent variable (adoption or rejection of cyber resiliency), and was used to test overall model fit (White, 2013). The significance level, alpha, was set at .05, indicating the probability of obtaining the result by chance is less than 5 percent (Nardi, 2018, p. 150).

The third step integrates the qualitative and quantitative in a side-by-side comparison, noting the convergent or dissonant themes from the data (Creswell & Creswell, 2018, p. 220). Steps one and two are represented in the results section of

Chapter 4, while the side-by-side comparison of step three is contained in the findings and interpretation section of Chapter 5.

Chapter Summary

This chapter presented the study's research method as a convergent (one-phase) design in which quantitative and qualitative data were collected near-simultaneously, with the qualitative sample derived from the quantitative sample (N). This design is appropriate to the research tradition for diffusion studies, as noted by Rodgers (2003), and leveraging a convergent mixed method approach enables the researcher to generalize quantitative findings to a population as well as explore the depth of meaning for lived experiences with human decision-makers (Creswell & Creswell, 2018, p. 19). A review of the hypothesis and research questions was discussed.

The researcher sampled a diverse population of senior, director, and executive-level information security professionals in the United States, using G*Power calculation to determine a suitable sample size of 82 participants for the quantitative, web-based, and computer-assisted survey with SurveyMonkey as the chosen quantitative survey instrumentation and analysis platform. A qualitative interview questionnaire was developed following recommended guidelines described by Creswell and Poth (2018), included in Appendix C. All data was collected via internet-based survey instrumentation, teleconference capability, or telephone. This study's discussion on validity and legitimation described how construct validity and triangulation ensure valid data and credible inferences. Data was analyzed in a three-phase approach appropriate to convergent mixed method design: qualitative data coding and categorization, quantitative

statistical analysis, and data integration through joint display (Creswell & Creswell, 2018).

Chapter 4 describes the process and results of the pilot study for both the quantitative survey and qualitative interview. Statistical and qualitative analysis and a display of the findings using the three-phase approach recommended by Creswell & Creswell (2018) follow, culminating in the joint display of convergent quantitative and qualitative data.

Chapter 4: Results

This chapter presents the results of the quantitative and qualitative data collection process. The chapter begins with a brief overview of the pilot study, including a summary of feedback from a standardized debrief questionnaire. The study's results are presented in three sections: demographics, innovation characteristics, and influences on cyber resiliency innovation decisions. The chapter concludes with a summary and introduction to Chapter 5, which focuses on triangulating and interpreting the findings and recommendations for future research.

Pilot Study

A pilot study was completed using cybersecurity professionals outside of the target population, chosen by the researcher, to test and revise the survey and interview questionnaires before data collection began. Nardi (2018) recommends the pilot study participants be like the target population and that both distribution and collection procedures proceed as designed to allow for a full evaluation (p. 102).

The pilot leveraged Capitol Technology University’s pool of graduate students and faculty with expertise and career experience in information security, selecting ten or more willing participants to test the online survey instrument and provide feedback to the researcher for any recommended changes in addition to the time it took to complete the survey. Additionally, participants piloted the qualitative questionnaire through virtual and asynchronous (emailed) interviews and provided feedback to the researcher if instructions need to be clarified or if questions should be revised. Taking advantage of the University student body and staff for the pilot offered opportunities for focused feedback in an academic setting, with participants familiar with research methodology, and provided the

opportunity for individual or group discussion within university channels (Nardi, 2018, pp. 102-103).

The pilot ran in January 2023. There were 11 responses with a 64% completion rate. The typical time spent completing the survey was under 20 minutes (18m:37s). The debrief questionnaire at the end of the pilot yielded feedback summarized in Table 6. Three additional written comments were provided to the researcher separately, which aided in revising the final instrument.

Table 6

Pilot Feedback Summary (n=11)

Debrief Question	**Answers**
How easy or difficult was it to navigate through the survey?	Very Easy (100%)
Were the instructions provided in the survey generally clear or confusing?	Clear (100%)
How long did it take you to complete the survey?	5-10 min (25%) 10-15 min (25%) 15-20 min (50%) Longer than 20 min (0%)
Did you encounter any error messages while working on the questionnaire?	No (100%)
Did you encounter any logic mistakes (I.e., page misroutes or question omissions) while working on the questionnaire?	No (100%)
Were there any terms that were not defined and should be defined?	No (100%)

Debrief Question	Answers
Were you concerned about your data and/or identity privacy as a participant?	No (100%)

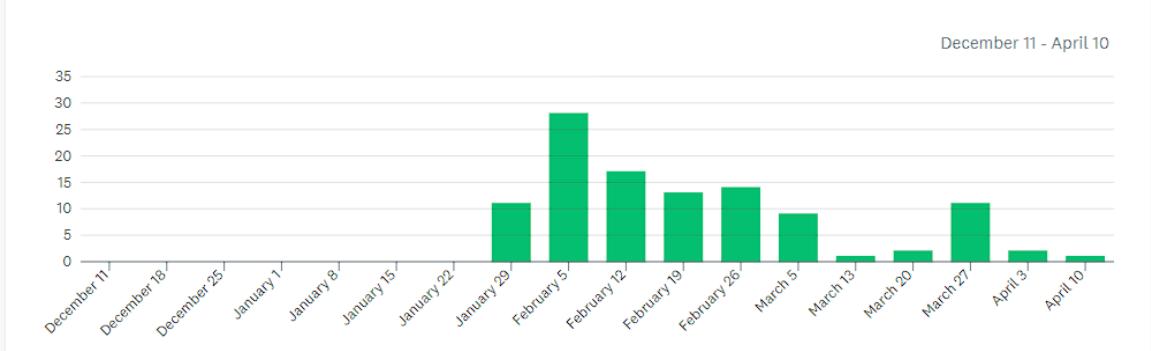
Results

The purpose of this mixed-method research study was to better understand the innovation-decision process for cyber resiliency, and what influences affect adoption or rejection of cyber resiliency innovations at the organizational leadership level. To accomplish the quantitative goals, an online survey was conducted through the SurveyMonkey online platform, promulgated to the target population of mid-senior, director, and executive-level cybersecurity leaders via social media, organizational memberships, professional associations, and communities of practice to which the researcher had access.

The survey instrument reported 109 responses with a 73% completion rate and an average completion time of 11 minutes. The survey was open and promulgated to the target population from January 29, 2023, to April 10, 2023. The survey concluded when survey propagation techniques were exhausted based on the researcher's time and resources and the number of responses met or exceeded the target sample size (n=82). At that time, the researcher closed the collector and compiled the results in binary (SPSS) and database (Microsoft Excel XLS) formats for analysis.

Figure 4

Response Volume of Survey Instrument



Note. The instrument was being developed and tuned from December 11 through January 28, parallel to the pilot study, and responses were not captured.

Any missing data present was removed from the final analysis to prepare for the data analysis. Missing data was defined as any participant who needed to complete the survey questions relating to the limiting factors, enabling factors or the organization's decision. Once missing data was discarded, the total sample size was reduced to 69 participants. In addition, the dependent variable of the decision to adopt or reject the program was turned into a dichotomous variable (adopted and rejected); this was done because of the low number of participants who responded that their organization rejected the program. Before the hypothesis testing, summary statistics were conducted for the demographic data and the variables of interest. Means and standard deviations were conducted for continuous variables, while frequencies and percentages were calculated and presented for the categorical variables.

To answer the two research questions, two separate binary logistic regressions were conducted to determine if the limiting factors and enabling factors predicted the organization's decision to adopt or reject the cyber resiliency program. The following research questions were analyzed throughout the chapter:

Research Question 1: What factors support the adoption of cyber resiliency in an organization ("enablers")?

- Ho1: The enabling factors did not significantly predict the adoption of cyber resiliency in an organization.
- Ha1: The enabling factors significantly predicted the adoption of cyber resiliency in an organization.

Research Question 2: What factors limit the adoption of cyber resiliency in an organization ("limiters")?

- Ho2: The limiting factors did not significantly predict the adoption of cyber resiliency in an organization.
- Ha2: The limiting factors significantly predicted the adoption of cyber resiliency in an organization.

Tables 8 through 19 summarize the demographics, statistics, data used for hypotheses testing, and phenomenological results; all results tables are included in Appendix D.

Summary Statistics

Before the hypothesis testing, summary statistics were calculated and presented for the demographic questions, organizational characteristics, decision to accept or reject the cyber resiliency program, limiting variables, and enabling variables. Precisely, frequencies and percentages were calculated for each of the categorical variables.

Demographic Questions

First, frequencies and percentages were calculated for the demographic questions. For the question of: What is your current career level within the information security field, the most frequently observed response was Mid-Senior (n = 35, 50.72%). The most

frequently observed category of: How many years of experience have you had in the field of information security was Over 20 years (*n* = 28, 40.58%). For the question of: What specialty areas have you worked within during your career, the most frequent response was cybersecurity management (*n* = 62, 89.86%). For the question of: Are you a veteran of the U.S. Armed Forces the most frequent responded answer was No (*n* = 37, 53.62%). The most frequently observed category of Do you, or have you ever, worked within one of the 16 critical infrastructure sectors was Yes (*n* = 61, 88.41%). For the question of: If yes, what Critical Infrastructure sectors have you worked within, the most frequently responded answer was information technology (*n* = 40, 57.97%). Finally, for the question of: During the period in which you experienced cyber resiliency decision-making in your organization, were you the decision-maker and/or responsible for governance and implementation of the cyber resiliency solution, the most frequent participant response was Yes (*n* = 44, 63.77%). Frequencies and percentages are presented in Table 8.

Organizational Characteristics

In addition to the demographic questions, survey questions 9-14 asked participants about the characteristics of the organization they work for. The most frequently observed category of the question: In your organization, how significant was the executive leadership's positive attitude towards change influential in decision-making was Greatly significant (*n* = 50, 72.46%). Next, for the question of: In your organization, to what extent has the role of an "innovation champion" (formalized or informal) at the executive or director level influenced decision-making, the most frequently observed response was to a great extent (*n* = 29, 42.03%). For the question: In your organization, to what extent have EXTERNAL NETWORKS, such as partnerships, vendor agreements,

and consultancies, influenced decision-makers, the most frequent participant response was to some extent (*n* = 49, 71.01%). The most frequently observed category of: In your organization, to what degree is decision-making CENTRALIZED within the organizational structure was to some extent (*n* = 43, 62.32%). The most frequently observed category of: In your organization, to what degree is the employed workforce COMPLEX by possessing high levels of knowledge, expertise, and a wide range of occupational specialties was to a great extent (*n* = 40, 57.97%). For the question of: In your organization, to what degree are rules FORMALIZED through documented policies and procedures, the most frequent response was to a great extent (*n* = 40, 57.97%). Finally, the most frequently observed category of: In your organization, to what degree are UNCOMMITTED RESOURCES, such as funding or people, available for use in new projects in a short amount of time was to some extent (*n* = 45, 65.22%). Frequencies and percentages are presented in Table 9.

Decision to Adopt or Reject the Cyber Resiliency Capability (Organization Decision)

Next, frequencies and percentages were calculated for the outcome variable of the decision to adopt or reject the cyber resiliency capability (organization decision). Frequencies are presented twice, once for the ordinal level variable and once for the dichotomous variable. The variable of organization decision was dichotomized due to the low number of responses to the rejection categories of the ordinal variable. The most frequently observed category of Decision was Adoption through a trial program (*n* = 36, 52.17%). While the most frequently observed category of decision- dichotomous was adoption (*n* = 63, 91.30%). Frequencies and percentages are presented in Table 10.

Limiting Variables

Frequencies and percentages were then calculated for the limiting variables. For the limiting variable of Technical Factors, the most frequent response was somewhat limiting (*n* = 35, 50.72%). The most frequently observed category of the limiting variable Cultural Factors, was somewhat limiting (*n* = 30, 43.48%). The most frequent response for the variable Organizational Influences was somewhat limiting (*n* = 34, 49.28%). The most frequently observed category of Workforce and Skills was somewhat limiting (*n* = 30, 43.48%). The most frequently observed Knowledge Management and Information Access category was somewhat limiting (*n* = 38, 55.07%). For the variable of Industry and Competitiveness, the most frequently observed category was not significantly limiting (*n* = 40, 57.97%). The most frequently observed Vendor and Third-party Support category was somewhat limiting (*n* = 41, 59.42%). The Legal and Regulatory Influences variable was Somewhat limiting (*n* = 26, 37.68%). Finally, the most frequently observed category of Resources and Funding was greatly limiting (*n* = 35, 50.72%). Frequencies and percentages are presented in Table 11.

Enabling Variables

Finally, frequencies and percentages were calculated for the enabling variables. The most frequently observed category of Technical Factors was somewhat enabling (*n* = 41, 59.42%). The most frequent response for the variable of Cultural Influences was somewhat enabling (*n* = 31, 44.93%). For the variable of Organizational Influences, the most frequent participant response was somewhat enabling (*n* = 37, 53.62%). The most frequently observed category of Workforce and Skills was also somewhat enabling (*n* = 41, 59.42%). Next, the most frequently observed Knowledge Management and

Information Access category was somewhat enabling (*n* = 39, 56.52%). For the variable of Industry and Competitiveness, the most frequent participant response was somewhat enabling (*n* = 32, 46.38%). For Vendor and Third-party Support, the most frequently observed response was somewhat enabling (*n* = 35, 50.72%). For the Legal and Regulatory Influences variable, the most frequent participant response was somewhat enabling (*n* = 28, 40.58%). Finally, the most frequently observed category of Resources and Funding was somewhat enabling (*n* = 36, 52.17%). Frequencies and percentages are presented in Table 13.

Hypothesis Testing

Research Question One

To answer the first research question, a binary logistic regression was conducted to examine whether the enabling factors of: technical factors, cultural factors, workforce and skills, knowledge management, organizational influences, industry and competition, vendor third-party support, legal, regulatory, and resources, and funding had a significant effect on the odds of observing the adoption category of organization decision. The reference category for organization decisions was rejection. Before the binary logistic regression, the multicollinearity assumption was assessed and presented. Significance level (alpha) for this test was set at .05, where a corresponding probability (p) value of less than the alpha would indicate significance for the population (Nardi, 2018, pp. 150-151).

Variance inflation factors. Variance Inflation Factors (VIFs) were calculated to detect the presence of multicollinearity between predictors. High VIFs indicate increased effects of multicollinearity in the model. VIFs greater than 5 are cause for concern,

whereas VIFs of 10 should be considered the maximum upper limit (Menard, 2009). All predictors in the regression model have VIFs less than 10. Therefore, the assumption of multicollinearity was met. Table 13 presents the VIF for each predictor in the model.

Results. The results of the overall model were not significant based on an alpha of .05, $\chi^2(9) = 14.77$, $p = .097$, suggesting that the enabling factors of technical factors, cultural factors, workforce and skills, knowledge management, organizational influences, industry and competition, vendor third party support, legal regulatory, and resources, and funding collectively did not have a significant effect on the odds of observing the adoption category of organization decision. McFadden's R-squared was calculated to examine the model fit, where values greater than .2 indicate models with excellent fit (Louviere et al., 2000). The McFadden R-squared value calculated for this model was 0.36. This indicates that the model was an excellent fit. Since the overall model was not significant, the individual predictors were not examined further. Table 14 summarizes the results of the regression model.

Research Question Two

To answer the second research question, another binary logistic regression was conducted to examine whether the limiting factors of: technical factors, cultural factors, workforce and skills, knowledge management, organizational influences, industry and competition, vendor third-party support, legal regulatory and resources and funding had a significant effect on the odds of observing the adoption category of organization decision. The reference category for organization decisions was rejection. Before the binary logistic regression, the multicollinearity assumption was assessed and presented. Significance level (alpha) for this test was set at .05, where a corresponding probability

(p) value of less than the alpha would indicate significance for the population (Nardi, 2018, pp. 150-151).

Variance inflation factors. Variance Inflation Factors (VIFs) were calculated to detect the presence of multicollinearity between predictors. High VIFs indicate increased effects of multicollinearity in the model. VIFs greater than 5 are cause for concern, whereas VIFs of 10 should be considered the maximum upper limit (Menard, 2009). All predictors in the regression model have VIFs less than 10. Therefore, the assumption of multicollinearity was met. Table 15 presents the VIF for each predictor in the model.

Results. The results of the overall model were not significant based on an alpha of .05, $\chi^2(8) = 6.88$, $p = .550$, suggesting that the limiting factors of technical factors, cultural factors, organizational influences, workforce and skills, knowledge management, industry and competition, vendor third-party support, and legal regulatory collectively did not have a significant effect on the odds of observing the adoption category of organization decision. McFadden's R-squared was calculated to examine the model fit, where values greater than .2 are indicative of models with excellent fit (Louviere et al., 2000). The McFadden R-squared value calculated for this model was 0.17. This indicates that the model was a good fit. Since the overall model was not significant, the individual predictors were not examined further. Table 16 summarizes the results of the regression model.

Phenomenological Results

Creswell and Poth (2018) present a general template for presenting qualitative results through phenomenological analysis and representation, grounded in methodology found within Moustakas (1994) to ensure "specific, structured methods of analysis" are

undertaken specific to a phenomenological study (pp. 201–202). In this method of analysis, the researcher first presents their personal experiences with the phenomenon studied to address and then sets aside those experiences. Next, the researcher presents a list of significant statements captured from the data collection (interviews), known as data horizontalization. Significant statements are grouped and categorized into meaning units. A description of "what" the participants experienced in the phenomenon provides a textural description of the experience with verbatim examples. Finally, the "how" of the experience presents a structural description of the phenomenon, followed by the researcher's composite description in which the "essence" of the experience is presented, combining the "what" with the "how" (Creswell & Poth, 2018, p. 201).

Drawing from the quantitative sample size, 17 participants opted into the phenomenological data collection portion of the study. Of those participants, eight responded to the researcher and completed the interview questionnaire (provided in Appendix C), resulting in a 47% completion rate. Most interview participants were in the mid-senior cybersecurity career level (5). Additionally, two questions of the survey offered narrative responses: the first (question 36) asked if there were any other influence factors not listed in the survey that were significant in the decision-making process to adopt or reject cyber resiliency measures within the organization and the second (question 38) offered the participant a chance to add comments related to the innovation-decision process for cyber resiliency. In total, 26 responses were made to question 36, and 16 responses were made to question 38, all of which were added to the phenomenological data set.

Researcher's personal experiences with cyber resiliency.

The researcher's personal experiences with cyber resiliency stem from over 23 years of experience in the field of information technology and information security, with 20 years of active-duty military service in the United States Navy, followed by private sector experience as a senior-level information security manager. The researcher's active-duty experience shaped his understanding of resiliency in general, both personal and unit level, including over six years of service in major staff assignments where the researcher observed Navy-wide policy and strategy, the Planning, Programming, Budgeting, and Execution Processes (PPBE) of the Department of Defense, and the Congressional authorization and appropriation processes.

The researcher's private sector experience includes information security program governance, enterprise risk management and client data protection, and compliance with regulatory security requirements; the researcher's organization has implemented several cyber resiliency design principles, including business impact analyses, client-serving mission systems focused on adaptability, reduction of attack surfaces through supply chain risk management and operations security (OPSEC), and anticipating compromise through threat analysis and red teaming (NIST, 2021, pp. 109-113). While the researcher maintains extensive experience in plans, policy, and strategy of organizational resiliency and managerial experience of cyber resiliency implementation in support of national defense programs, he does not assert deep technical expertise at a system engineering or tooling level.

Significant statements made by participants.

Significant statements made by participants are described in Tables 17 and 18 are synthesized from qualitative results derived from both the online survey (questions 36

and 38) and experiential interview results (see Appendix C). A significant number of statements focused on organizational factors that positively or negatively affected the participants, particularly leadership buy-in for cyber resiliency or cybersecurity overall. Table 17 horizontalizes participants' statements on cyber resiliency adoption influences. Table 18 provides significant statements on cyber resiliency or cybersecurity in general. Notably, when offered an opportunity to provide more general comments, participants described cultural influences as well.

While participants described a range of influences during the study, such as funding limitations, lack of on-staff expertise, and regulatory or legal challenges, the most significant statements revolved around organizational influences and particularly support from executive leadership. For those in director or executive-level roles, this meant top-level prioritization and funding support. For those in mid-senior level positions, it was described more broadly. While they believed they had the support of their immediate boss (such as the Chief Information Security Officer), other executive stakeholders held many of the keys to success (such as the Chief Information Officer prioritizing information technology architectural changes to accompany resiliency controls).

Observed themes.

The total number of derived theming instances was 73, divided among nine meaning groups by frequency of mention. Table 19 details the observed themes and frequency, combining qualitative data from the survey instrument and experiential interviews. By grouping themes in this fashion, the researcher could group significant

statements and interpret meanings within broader information units (Creswell & Poth, 2018, p. 201).

Textural description of the phenomenon.

The participants experienced significant non-technical influence factors in cyber resiliency adoption. The most frequent themes were cultural resistance to change as a key limiting factor in the adoption of cyber resiliency capabilities (n=14, 19.18%), organizational governance and regulatory obligations as a primary driver in considering resiliency measures (n=13, 17.81%), and leadership buy-in and decision-maker support as significantly influential in the process of adopting or rejecting cyber resiliency innovations (n=10, 13.70%). While engineering and technical limitations were noted in the phenomenological results, they represented the lowest frequency of mention (n=4, 5.48%).

Participants described cultural resistance to change as a significant limiting factor in implementing cyber resiliency and was the most frequently mentioned factor during the study. One response in the online survey described, "socialization with peers played a somewhat significant role in adoption." Another response described an "approval in principle with rejection in practice," where the stakeholders resisted change by engaging "in a series of non-formal activities to effectively reject" the cyber resiliency capability. An interview subject expressed significant frustration of the innovativeness of local government (city and county) activities, stating "city government is the least innovative of all the governments" and describing cultural and organizational resistance to adoption through "playing politics" and prioritizing "pet projects." One participant offered a narrative on how they overcame cultural resistance:

> In cybersecurity leadership, there is a need to be able to manage and work with people, even those on the leadership team. If I want to implement a cybersecurity resiliency item, depending on what it is, I may have to have necessary conversations with the team so they know what it is and support is [sic] as their own.

Organizational factors such as policies, procedures, strategic direction, or regulatory and legal requirements were frequently experienced by the participants and noted both limiting and enabling influences on cyber resiliency adoption. Several participants who work for the federal government cited instructions and orders that directed their actions. In contrast, others who work in highly regulated industries, such as finance, described legal requirements or equity firm ownership that drove compliance activities that may or may not have included cyber resiliency capabilities. One respondent who worked within the Department of Defense stated, “Cybersecurity in the DoD is greatly influenced by perceived level of mission importance," indicating that the strategic direction of the organization was experienced as a key driver.

Participants also described leadership buy-in of cyber resiliency capabilities as highly influential in adoption or rejection decisions. One interview subject stated, "this is a leadership thing; this is what leaders are supposed to do" when describing prioritizing capabilities that benefit the organization's mission. Another interviewee expressed frustration with their organization's lack of perceived leadership buy-in, stating "there is no accountability." One survey participant offered this narrative of how executive leadership enabled adoption: “Executive level buy-in is key obviously. Having someone

engaged, knowledgeable and championing security at the Executive level made things much easier for us."

Other themes expressed included past incidents or adverse cyber events enabled or accelerated adoption, the commitment of resources, both capital and human either enabled or limited adoption, and flawed implementation or flawed decision-making hampered or reduced the effectiveness of adoption. While still expressed as themes, the least mentioned were perceptions that the organization was innovative or ahead of industry vertical peers and that the chosen engineering design or technical tools limited adoption of cyber resiliency.

Structural description of the phenomenon.

The phenomenon of cyber resiliency adoption as an innovation was studied with participants in the cybersecurity profession at mid-senior, director, and executive level roles within the United States. The majority of respondents to the online survey were in mid-senior level roles with over ten years of experience in the field of information security. The most frequent specialty areas the participants worked within were risk management, cybersecurity management, and vulnerability assessment and management. The majority of participants were not veterans of the U.S. armed forces; however, a significant majority worked, or did work, within one of the 16 critical infrastructure sectors of the United States; the most frequently reported sectors were information technology (service provider), government facilities, and the defense industrial base.

Following the framework of Rodgers (2003), participants offered internal characteristics of organizational structure as related to innovativeness, specifically, centralization (question 10), complexity, formalization, interconnectedness, system

openness (question 11), organizational slack, and leader characteristics (question 9). Understanding the characteristic innovativeness of the participants' organizations provided insight into understanding the phenomenon of cyber resiliency adoption as an innovation, mainly as the participants answered these questions through the lens of their cybersecurity roles and cyber resiliency adoption (Rodgers, 2003, pp. 411-412); the results are detailed in Table 9.

In summary, the majority (over 50%) of participants described their organizations with a low to moderate ("to some extent") degree of centralization in decision-making, interconnectedness to external units that bring innovation, such as partnerships, vendors, and consultancies, and organizational slack through the availability of uncommitted resources. The majority (over 50%) of participants described their organizations with a high ("to a great extent") degree of individual (leader) characteristics and positive attitude towards change, complexity in workforce knowledge and expertise, and formalization through documented policies and procedures. Thus, the majority of surveyed cybersecurity professionals in this study view their organizational structure with a low to moderate degree of centralization, interconnectedness, system openness, and organizational slack and a high degree of leader characteristics, complexity, and formalization (Rodgers, 2003, pp. 411-413).

Composite description of the phenomenon.

The phenomenon studied was influence factors in cyber resiliency adoption within organizations in the United States. Participants were mid-senior, director, and executive-level cybersecurity professionals, with the majority of subjects in both the online survey and experiential interviews at the mid-senior level of decision-making

within their organizations. The study participants described structural characteristics of organizational innovativeness they found themselves in with a low to moderate degree of centralization, interconnectedness, system openness, and organizational slack, and a high degree of leader characteristics, complexity, and formalization.

The participants experienced significant non-technical influence factors in cyber resiliency adoption, the most frequently described as cultural resistance to change, organizational governance and regulatory obligations, and leadership buy-in. Influences expressed by participants but less frequently mentioned were past incidents or adverse cyber events enabled or accelerated adoption, the commitment of resources, both capital and human, either enabled or limited adoption, and flawed implementation or flawed decision-making hampered or reduced adoption effectiveness. Perceptions that the organization as a whole was innovative or ahead of industry vertical peers and that the chosen engineering design or technical tools limited adoption of cyber resiliency were described by some but were the least frequently observed themes.

Chapter Summary

The purpose of this mixed-method research study was to better understand the innovation-decision process for cyber resiliency, and what influences affect adoption or rejection of cyber resiliency innovations at the organizational leadership level. To prepare for the data analysis, missing data points were removed from the final analysis. Missing data was defined as participant who did not complete the survey questions relating to the limiting and enabling factors, and/or the organization decision. In addition, the dependent variable of organization decision to adopt or reject the program was turned into a dichotomous variable (adopted and rejected); this was done due to the low number of

participants who responded that their organization rejected the program. Before the hypothesis testing, summary statistics were conducted for the demographic data and the variables of interest. Specifically, frequencies and percentages were calculated and presented for the categorical variables.

To answer the two research questions quantitatively, two separate binary logistic regressions were conducted to determine if the limiting factors and enabling factors predicted the organizations' decision to adopt or reject the cyber resiliency program. The results of each binary logistic regression were not significant, indicating that the enabling and limiting factors did not significantly predict the odds of adopting the cyber resiliency program. Therefore, the null hypothesis was not rejected.

To accompany the quantitative results, a phenomenological analysis and representation were presented following the general template described by Moustakas (1994) within Creswell and Poth (2018). The researcher presented their personal experiences with the phenomenon, data horizontalization through significant statements, meaning units and themes, a textural description, a structural description, and finally, a composite description. The implications of these results will be further examined in Chapter 5, where the researcher will discuss limitations, interpretations, recommendations for future research, and the researcher's overall conclusions of the study.

Chapter 5: Conclusions and Recommendations

This chapter summarizes the study, findings related to the literature, and a discussion based on the data presented in the previous chapter. Implications for organizational adoption of cyber resiliency and national-level cyber resiliency are discussed, followed by recommendations for future research. The chapter closes with the researcher's concluding remarks and chapter summary.

Summary of the Study

This study's purpose was to better understand the innovation-decision process for cyber resiliency and what influences affect the adoption or rejection of cyber resiliency innovations at the organizational leadership level. In this study, the researcher sought to address a general problem of national-level cyber resiliency within the United States, specifically challenges in organizational adoption of cyber resiliency capabilities. The literature review identified several innovation-decision and operational influences on cyber resiliency that the researcher grouped into nine general categories that formed the analytical framework for the study's instrumentation: (1) technical factors, (2) cultural influences, (3) organizational policies and leadership, (4) workforce and skills, (5) knowledge management and information access, (6) industry and competitiveness, (7) vendor and third-party support, (8) legal and regulatory influences, and (9) resources and funding.

The method used for this study involved mixed methods, in which the researcher conducted a quantitative internet-based survey of senior, director, and executive level cybersecurity professionals on cyber resiliency adoption within their organizations and enriched with in-depth interviews of chosen survey participants with relevant decision-

making experience. The instruments – the online survey and experiential interviews – provided both quantitative and qualitative data from which to study the phenomenon of cyber resiliency adoption within the theoretical framework of Diffusion of Innovations Theory (Rodgers, 2003).

The researcher posed two research questions to guide the study. Research question one (RQ1) asked, "What factors limit adoption of cyber resiliency in an organization," and research question two (RQ2) asked, "What factors support adoption of cyber resiliency in an organization." Quantitatively, the researcher posited, in a two-directional (two-tailed) positive hypothesis (H_α), that there is a statistical relationship between influence factors on cybersecurity leadership and cyber resiliency adoption. Conversely, the null hypothesis (H_0) states no statistical relationship exists between influence factors on cybersecurity leadership and cyber resiliency adoption. The results of each binary logistic regression were not significant, indicating that the enabling and limiting factors did not significantly predict the odds of adopting the cyber resiliency program. Therefore, the null hypothesis was not rejected.

Qualitatively, the researcher collected phenomenological results through two instruments: the online survey and experiential interviews. Tables 16 and 17 draw significant statements from the qualitative data set, and Table 18 provides overall themes and frequency of occurrence. The participants experienced a significant amount of non-technical influence factors in cyber resiliency adoption, the most frequent of which were described as cultural resistance to change, organizational governance and regulatory obligations, and leadership buy-in. Influences expressed by participants but less frequently mentioned were past incidents or adverse cyber events enabled or accelerated

adoption, commitment of resources both capital and human enabled or limited adoption, and flawed implementation or flawed decision-making hampered or reduced adoption effectiveness.

Findings and Interpretations

This section provides findings and interpretations based on the research questions. The researcher offers a discussion on implications for practice and recommendations based on the emerging themes from the analysis, offered through the lens of the theoretical framework following the Diffusion of Innovations Theory and grounded in the reviewed literature (Rodgers, 2003). The researcher interpreted these findings by triangulating the quantitative and qualitative results to identify trends, observation frequencies, and unexpected findings.

Convergent Triangulation of Findings

Triangulation is an approach whereby the convergence of multiple data sources is explored, typically written into a discussion section and merging the two forms of data (quantitative and qualitative) into a joint display (Creswell & Creswell, 2018, pp. 220-221). A triangulation of the results within a joint display enhances the validity of the conclusions if different approaches produce convergent findings and represent the key strength of a mixed methods design (Creswell & Creswell, 2018, pp. 220-221).

To succinctly answer the research questions based on the available data, the researcher developed a convergent triangulation of quantitative and qualitative data, displayed in Table 7. Triangulation was accomplished related to the research questions by determining the percentage of survey responses that described an influencing factor as at least "somewhat" limiting or enabling (omitting responses that indicated a factor was "not

significant") and correlating those percentages to the top three most frequently observed themes from the qualitative data collected from both the survey and experiential interviews.

Table 7

Convergent Triangulation of Findings

Variable	% overall limiting	% overall enabling	Correlation to most frequent qualitative themes
Technical Factors	78.26	**85.51**	
Cultural Factors	**84.06**	78.26	Cultural resistance to change as a key limiting factor
Organizational Influences	**85.51**	**84.05**	Organizational policies, procedures, strategies, or legal requirements as a key driver; Leadership buy-in/support as significant influential
Workforce and Skills	76.81	**82.61**	
Knowledge Management and Information Access	75.36	73.91	
Industry and Competitiveness	42.02	55.08	
Vendor and Third-Party Support	76.81	71.01	
Legal and Regulatory Influences	68.11	60.87	
Resources and Funding	**86.95**	73.91	Commitment of resources as most significant

Note. "Percentage limiting" and "percentage enabling" combines "somewhat limiting" and "greatly limiting" survey responses for each question. Correlation to "most frequent" qualitative themes accounts for the top three most frequent themes detailed in Table 19 (Appendix D). Responses over the 80 percentile are bolded for emphasis.

Aggregating the independent variables from the survey to become dichotomous values provides for a joint display of data when combined with qualitative themes. The

bolded values in Table 7 represent influences at or above the 80th percentile, indicating the strongest influences based on the survey responses. It is important to keep in mind that the variables were measured independently, and survey respondents could have indicated equal measures of limiting and enabling influences. Through this joint display, several interpretations can be made that validate the top three observed themes. In particular, cybersecurity leaders experienced negatively-influencing cultural factors when working to adopt cyber resiliency capabilities, particularly a cultural resistance to change, correlating to a higher percentage of overall limitation in the survey responses compared to enabling effects. Additionally, where commitment of resources was observed as a significant influence factor, the survey responses indicated that resourcing tended towards limiting (86.95) rather than enabling (73.91). Technical factors were overall observed to be enabling (85.51) in favor of cyber resiliency adoption.

Perhaps the most significant and complex triangulation finding can be found in examining organizational influences, with a high percentage of responses indicating both limiting (85.51) and enabling (84.05) influence on cyber resiliency adoption, correlating to strong organizational influence themes in the qualitative data. Buy-in from organizational leadership and organizational policies, procedures, strategies, legal frameworks, and other structural characteristics presented a nebulous but noteworthy influence factor for cyber resiliency adoption.

Unexpected findings include those factors that, according to the data, presented little evidence of significance. Industry and competitiveness received a low response from survey respondents as either a limiting (42.02) or enabling (55.08) factor nor was it present in the qualitative data as an emergent theme. These factors include what industry

vertical the organization finds itself in, the competitive landscape within that vertical, and other external influences related to the industrial sector and maintaining competitive advantage. While much of the literature focused on internal factors for adopting cyber resiliency, Annarelli, Nonino, and Palombi (2020) describe infrastructure – critical or non-critical – and industry sector with "great importance in determining managerial actions to undertake" (p. 3). Findings in this factor disagree with the literature in this regard, which could result from the population sampled. In contrast, the literature sampled European organizations, and this study focused on U.S. organizations, with a significant number of respondents (88.41%) indicating they work within critical infrastructure. This may represent a homogenous sample in which industry vertical factors are already accounted for, and competitiveness is less of a factor than compliance and operational efficiencies.

Based on binary logistic regression testing, the null hypothesis (H_0) could not be rejected, and the researcher found no statistical relationship between influence factors on cybersecurity leadership and cyber resiliency adoption. Several reasons exist for this result, not least of which could be limitations described in Chapter 1 affecting the outcome. Additionally, although the sample size of respondents indicated suitable statistical power, the number of respondents to each question was below the total sample size. It reduced the statistical power of the Likert scale questions used for regression testing, likely due to participants closing the online survey before completion. Nevertheless, the results depicted in Chapter 4, and the corresponding data tables in Appendix D, indicate no apparent trend toward statistical significance; this does not reconcile with the qualitative findings in which participants expressed significant

influences upon decision-making that both connect to the literature and provide additional insight into challenges cyber leaders face when adopting cyber resiliency. Thus, the failure to reject the null hypothesis was another unexpected finding, and further research is required to understand better the statistical significance of influence factors in cyber resiliency adoption.

The findings in this study partly agreed with the literature synthesis described in Chapter 2 and detailed in Appendix A. Cultural, organizational, and resource factors were noted as significant in the literature synthesis and had corresponding high percentages of overall responses in the survey with notable themes in the qualitative data. However, with many key works of literature noting technical factors as highly significant, the researcher should have observed this result in the study. Survey participants found technical factors slightly more enabling (85.51%) than limiting (78.26%) overall, with interview participants offering more on organizational and cultural factors than technical ones. While not insignificant by any measure, with over 75% of respondents reporting an overall significance positive or negative in implementing cyber resiliency, it did not prompt a great deal of discussion within either the survey responses or the experiential interview process. The following sections discuss implications for theory, specifically the Diffusion of Innovations Theory (Rodgers, 2003), and practical implications for cybersecurity practitioners.

Implications for Theory

Diffusion scholars have been conducting research under the theoretical concepts known now as the Diffusion of Innovations since Frenchman Gabriel Tarde wrote about his observations on the "laws of imitation" (Tarde, 1903, p. 140 within Rodgers, 2003, p.

41). Since then, hundreds of diffusion studies have been undertaken by scholars seeking to understand why and how innovations are diffused through a social system and insights into how to manipulate influence factors to affect adoption (Rodgers, 2003, pp. 43-48). Professor Everett M. Rodgers documented the research traditions, history, and methodology of diffusion studies in his seminal work "Diffusion of Innovations," starting in 1962 and culminating in the fifth and perhaps final edition in 2003. Rodgers (2003) identified eight types of diffusion research: (1) earliness of knowing about innovations, (2) rate of adoption of different innovations in a social system, (3) innovativeness, (4) opinion leadership, (5) diffusion networks, (6) rate of adoption in different social systems, (7) communication channel usage, and (8) consequences of innovation (p. 101).

Professor Rodgers also issued a challenge to future diffusion scholars to expand diffusion research beyond "where the ground was soft" and move "in directions that theory suggests" (Rodgers, 2003, p. 101). Rodgers had only begun to theorize how the internet and information technology would create new diffusion networks and influence innovation decisions. This study furthered the Diffusion of Innovations Theory by opening a new type of diffusion research beyond the eight traditions identified in Rodgers (2003) by investigating influence factors on the innovation-decision process. Focusing on the innovation-decision process leads to more significant implications for organizational practice in study findings. It can also impact innovation influencers external to organizations, such as government policymakers, by providing valuable insight into challenges and opportunities in the process.

Since the last edition of Rodgers' work was published in 2003, and his subsequent passing in 2004, additional editions have yet to be published to the detriment of the

diffusion research tradition. However, diffusion studies have continued along new lines of inquiry; perhaps Professor Rodgers would be pleased to see this evolution, yet the theory and the documented research traditions remain static, two decades out of date. A new edition of Rodgers' work, or a scholarly successor, is needed to further theoretical practice and inspire future scholars to undertake diffusion studies. Insight into this critical social science research field is needed by policymakers, organizational leaders, and innovation champions as technology advances rapidly in the 21st century.

Implications for Practice

Based on the findings, the researcher notes two key implications for cyber leaders: (1) leadership buy-in can tip the scales to limit or enable cyber resiliency innovations, and (2) organizations should be prepared to adjust policies and procedures to allow for positive innovations like cyber resiliency. The greatest influences on cyber resiliency investment are cultural and organizational, not technical. Technical barriers are constantly eased through innovative methods like artificial intelligence, cloud solutions, hyper-convergence in IT infrastructure, and other machine-speed methodology to make managing large data processing systems easier. Cyber leaders have access to various tools and techniques that will reduce technical barriers to implication. Cyber leaders must shift to understanding the business, organizational politics, and communicate their resiliency vision to key stakeholders in a way that will generate buy-in and secure the resources to take action. This includes building cross-functional teams, creating partnerships, communicating risks and impacts in business terms, and collaborating with other executives. Technical leadership remains a core requirement for any technologist

leader but more is needed to navigate the innovation-decision process if an adoption decision with sustainable organizational buy-in is desired.

The findings of this study also indicate that public sector organizations, such as government and military, are susceptible to resourcing disruptions. Experiential data collected through the interview process noted significant challenges for government organizations in adopting resiliency innovations and maintaining consistent resourcing throughout the lifecycle. Cyber leaders in public sector organizations must ensure funding levels can meet the solution's implementation, operations, and maintenance needs or risk de facto rejection through resource reductions. Failure to properly resource resiliency at the state, local, and tribal government levels can lead to national cyber defense and resiliency failures. Further, constant shifts in leadership and contracting models result in uneven execution of cyber resiliency implementation or outright rejection of innovations due to political and resourcing reasons and not driven by mission success.

Recommendations for Future Research

The researcher provides several key recommendations for future research in the field of cyber leadership. Future researchers should investigate organizational innovativeness as it relates to cybersecurity in general. Rodgers (2003) described several variables related to organizational innovativeness, such as individual characteristics of leaders in the organization, characteristics of the organizational structure, and external characteristics of how the organization interacts with others outside its structure (p. 411). Additionally, future researchers should undertake diffusion studies of specific cyber resiliency techniques as defined in NIST SP 800-160 Vol. 2 Appendix D. What resiliency

techniques are more likely to be adopted by organizations; what techniques are least likely to be implemented? A study of this nature would have significant implications for practice.

Specific to cyber resiliency, future researchers should build upon the synthesis of the available literature and results of this study, using the nine categories of influence factors identified in the literature review, to develop a framework for successful cyber resiliency innovation implementation. Additionally, a longitudinal study that can examine longer-term implementations of cyber resiliency innovation adoption would further the field of research and offer practical implications for cyber leadership.

Conclusions and Chapter Summary

This study sought to better understand influence factors in cyber resiliency adoption at an organizational level. The implications of this research affect any organization that conducts business using the internet, where attackers prowl the "cyber sea lanes" seeking targets for data theft, ransomware, and intelligence gathering. It is often said that every internet-connected public and private organization finds itself on the "cyber battlefield," it is not a matter of if a hack occurs, but when. Cyber-resilient systems reduce operational impacts and make it difficult for cyber threat actors to achieve their ultimate goals of disruption and profit.

Organizational cyber resiliency impacts the national security of the United States and has become a vital component in national defense strategy and policy. In the latest version of the National Cybersecurity Strategy (2023) developed and published by the Biden Administration, the word "resilience" or "resilient" can be found a total of 67 times in a 35-page document. Thought-leadership groups such as the Cyberspace Solarium

Commission have identified cyber resiliency as vital to denying benefits to cyber attackers targeting U.S. critical infrastructure. Research into cyber resiliency is needed now more than ever.

This chapter presented a summary of the study, interpretations of the results, recommendations for future research, and the researcher's conclusions. Interpretations followed the original research question one (limiters) and two (enables), and implications for theory and practitioners were discussed. This study's quantitative and qualitative results add to the growing body of research on cyber leadership and cyber resiliency. The data collected and presented offer an opportunity for future research design and interpretation. The researcher hopes that future scholars and practitioners will build upon this study, learn from its limitations, and leverage its strengths to ultimately serve the greater good and make cyberspace a safer, more prosperous domain for everyone. Adverse cyber events happen every day at machine speed, and cyber resiliency is the crucial tool in a cyber leader's toolbox, weathering its effects without catastrophic consequences for the organization or, perhaps, the nation; there is no time to waste.

References

Accenture. (2018). *The Nature of Effective Defense: Shifting from Cybersecurity to Cyber Resilience*. Washington, D.C. Accenture Federal Services LLC. https://www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/local/en/accenture-shifting-from-cybersecurity-to-cyber-resilience-pov.pdf

Alperovitch, D. (2022). The Case for Cyber-Realism. *Foreign Affairs*, *101*(1), 44–50. https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism?utm_medium=newsletters&utm_source=fatoday&utm_campaign=The%20Case%20for%20Cyber-Realism&utm_content=20220107&utm_term=FA%20Today%20-%20112017

Alu, A. A., Ayoung, D. A., & Abdulhamid, N.G. (2021). Exploring the prospects of big data analytics in colleges of education in Ghana. *Journal of African Education (JAE)*, *2*(3), 81–106. https://doi.org/10.31920/2633-2930/2021/v2n3a4

Andrews, T. (n.d.). Innovation-Decision Model. Accelerating Systemic Change Network. https://ascnhighered.org/ASCN/change_theories/collection/innovation_decision.html

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly*, *41*(3), 893–916. https://doi.org/10.25300/MISQ/2017/41.3.10

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering*, *149*.

Ashogbon, A. D. (2021). *Examining the Role of Diffusion of Innovation Theory in Cloud Computing Adoption: International Marketing Organization Perspective* (Order No. 28722218). Available from ProQuest One Academic. (2581862302). https://www.proquest.com/dissertations-theses/examining-role-diffusion-innovation-theory-cloud/docview/2581862302/se-2

Atwell, R. C., Schulte, L. A., & Westphal, L. M. (2009). Linking Resilience Theory and Diffusion of Innovations Theory to Understand the Potential for Perennials in the U.S. Corn Belt. *Ecology and Society*, *14*(1). https://doi.org/10.5751/ES-02787-140130

Barasa, E., Mbau, R., & Gilson, L. (2018). What Is Resilience and How Can It Be Nurtured? A Systematic Review of Empirical Literature on Organizational Resilience. *International Journal of Health Policy and Management*, *7*(6), 491–503. https://doi.org/10.15171/ijhpm.2018.06

Birks, D. F., Fernandez, W., Levina, N., & Nasirin, S. (2013). Grounded theory method in information systems research: its nature, diversity and opportunities. *European Journal of Information Systems*, *22*(1), 1–8. https://doi.org/10.1057/ejis.2012.48

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In A. M. Correia, S. Costanzo, L. P. Reis, & A. Rocha (Eds.), *Advances in Intelligent Systems and Computing: Vol. 353. New Contributions in Information Systems and Technologies: Volume 1* (1st ed., Vol. 353, pp. 311–316). Springer International Publishing; Imprint: Springer. https://doi.org/10.1007/978-3-319-16486-1_31

Bodeau, D. J., & Graubart, R. (2011). *Cyber Resiliency Engineering Framework* (11-4436). Bedford, MA. The MITRE Corporation. https://www.mitre.org/sites/default/files/pdf/11_4436.pdf

Burstein, M., Goldman, R., Robertson, P., Laddaga, R., Balzer, R., Goldman, N., Geib, C., Kuter, U., Mcdonald, D., Maraist, J., Keller, P., & Wile, D. (2012). STRATUS: Strategic and Tactical Resiliency against Threats to Ubiquitous Systems. In Institute of Electrical and Electronics Engineers (Ed.), *2012 IEEE Sixth International Conference on Self-Adaptive and Self-Organizing Systems Workshops, Lyon, France, 10.09-14.09.2012* (pp. 47–54). IEEE Computer Society. https://doi.org/10.1109/SASOW.2012.17

Butler, T., & Brooks, R. (2021). Achieving operational resilience in the financial industry: Insights from complex adaptive systems theory and implications for risk management. *Journal of Risk Management in Financial Institutions*, *14*(4), 395–407.

Capitol Technology University. (2022). *Doctor of Philosophy (PhD) in Cybersecurity Leadership*. https://www.captechu.edu/degrees-and-programs/doctoral-degrees/cybersecurity-leadership-phd

Carayannis, E. G., Grigoroudis, E., Rehman, S. S., & Samarakoon, N. (2021). Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience. *IEEE Transactions on Engineering Management*, *68*(1), 223–234. https://doi.org/10.1109/TEM.2019.2909909

Carment, D., & Belo, D. (2020). Gray-zone Conflict Management: Theory, Evidence, and Challenges. *Journal of European, Middle Eastern, & African Affairs*, 1–18.

Cohen, J. (1988). *Statistical power analysis for the behavior sciences* (2nd ed.). West Publishing Company.

Committee on National Security Systems. (2015). *Committee on National Security Systems (CNSS) Glossary 4009*. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Method Approaches* (5th ed.). SAGE Publications.

Creswell, J. W [John W.], & Poth, C. N. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed.). SAGE Publications.

CrowdStrike. (2021). *2021 Global Threat Report.* CrowdStrike Inc. https://go.crowdstrike.com/crowdstrike-global-threat-report-2021.html?utm_campaign=brand&utm_content=&utm_medium=sem&utm_source=goog&utm_term=crowdstrike%202021%20global%20threat%20report&gclid=CjwKCAiA24SPBhB0EiwAjBgkhj_a7gdq1TKD8Ah5JPYjl6Rg9x1EQVONQyftp-VbdFF1zt4MozX-pxoCHX0QAvD_BwE

Cutler, T. J. (2019). BlueJacket's Manual. *Naval History*, *33*(6), 6–7.

Dearing, J. W., & Cox, J. G. (2018). Diffusion Of Innovations Theory, Principles, And Practice. *Health Affairs (Project Hope)*, *37*(2), 183–190. https://doi.org/10.1377/hlthaff.2017.1104

Dearing, J. W., & Singhal, A. (2020). New directions for diffusion of innovations research: Dissemination, implementation, and positive deviance. *Human Behavior and Emerging Technology*(2), 307–313. https://doi.org/10.1002/hbe2.216

Dehlawi, Z., & Abokhodair, N. (2013, June 4 - 2013, June 7). Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. In Institute of Electrical and Electronics Engineers (Ed.), *2013 IEEE International Conference on Intelligence and Security Informatics* (pp. 73–75). IEEE. https://doi.org/10.1109/ISI.2013.6578789

Diamond, E., & Bates, S. The ancient history of the Internet. *American Heritage*, *46*(6), 34. https://www.americanheritage.com/ancient-history-internet

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security*, *63*, 1–13. https://doi.org/10.1016/j.cose.2016.09.006

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., Gupta, B., Lal, B., Misra, S., Prashant, P., Raman, R., Rana, N. P., Sharma, S. K., & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, *55*, 1–20. https://doi.org/10.1016/j.ijinfomgt.2020.102211

El-Alfy, E. S. M., Eltoweissy, M., Fulp, E. W., & Mazurczyk, W. (2019). *Nature-inspired cyber security and resiliency: Fundamentals, techniques and applications / edited by El-Sayed M. El-Alfy, Mohamed Eltoweissy, Errin W. Fulp, Wojciech Mazurczyk*. *IET security series: Vol. 10*. Institution of Engineering and Technology.

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.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23.

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of Cyber Systems with Over- and Underregulation. *Risk Analysis : An Official Publication of the Society for Risk Analysis*, *37*(9), 1644–1651. https://doi.org/10.1111/risa.12729

Groenendaal, J., & Helsloot, I [Ira] (2021). Cyber resilience during the COVID-19 pandemic crisis: A case study. *Journal of Contingencies and Crisis Management*, *29*(4), 439–444. https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-5973.12360

Groenendaal J., & Helsloot, I [I.] (2020). Organisational resilience: Shifting from planning-driven business continuity management to anticipated improvisation. *Journal of Business Continuity & Emergency Planning*, *14*(2), 102.

Gunderson, L. & Holling, C. S. (2002). Panarchy Understanding Transformations in Human and Natural Systems. https://www.semanticscholar.org/paper/efdf0ba2679228335bbc3fd058a7ac94375ef96a

Gwebu, K. L., Wang, J., & Wang, L. (2018). The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *Journal of Management*

Information Systems, *35*(2), 683–714. https://doi.org/10.1080/07421222.2018.1451962

Hudson, J. F. (2021). Mission Assurance in Joint All-Domain Command and Control. *Air & Space Power Journal*, *35*, Article 151186358, 18–32.

Hynes, W., Trump, B., Love, P., & Linkov, I. (2020). Bouncing forward: A resilience approach to dealing with COVID-19 and future systemic shocks. *Environment Systems and Decisions*, *40*(2), 1–11. https://doi.org/10.1007/s10669-020-09776-x

Hynes, W., Trump, B. D., Love, P., Kirman, A., Galaitsi, S. E., Ramos, G., & Linkov, I. (2020). Resilient Financial Systems Can Soften the Next Global Financial Crisis. *Challenge*, *63*(6), 311–318. https://doi.org/10.1080/05775132.2020.1822660

Iles, I., Egnoto, M., Fisher Liu, B., Ackerman, G., Roberts, H., Smith, D. (2017). Understanding the Adoption Process of National Security Technology: An Integration of Diffusion of Innovations and Volitional Behavior Theories. *Risk Analysis: An International Journal*, *37*(11), 22–46.

Institute of Electrical and Electronics Engineers (Ed.) (2012). *2012 IEEE Sixth International Conference on Self-Adaptive and Self-Organizing Systems Workshops, Lyon, France, 10.09-14.09.2012*. IEEE Computer Society.

Institute of Electrical and Electronics Engineers (Ed.) (2013, June - 2013, June). *2013 IEEE International Conference on Intelligence and Security Informatics*. IEEE.

Intellectus Statistics [Online computer software]. (2022). Intellectus Statistics. https://analyze.intellectusstatistics.com/

International Information System Security Certification Consortium, Inc. (2021). *A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)2*

CYBERSECURITY WORKFORCE STUDY, 2021. Tampa, FL. https://www.isc2.org/Research/Workforce-Study#

Kang, H. (2021). Sample size determination and power analysis using the G*Power software. *Journal of Educational Evaluation for Health Professions*, *18*, 17. https://doi.org/10.3352/jeehp.2021.18.17

Keys, B., & Shapiro, S. (2019). Chapter 4: Frameworks and Best Practices. In I. Linkov & A. Kott (Eds.), *Cyber Resilience of Systems and Networks. Cyber Resilience of Systems and Networks* (pp. 69–92). Springer International Publishing.

Kott, A., & Linkov, I. (2021). To Improve Cyber Resilience, Measure It. *Computer*, *54*(2), 80–85. https://doi.org/10.1109/MC.2020.3038411

Lallie H. S., Shepherd, L. A., Nurse, J., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X. (2021, June). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*. https://doi.org/10.1016/j.cose.2021.102248

Lee, R. M., Assante, M. J., & Conway, T. (2016, March 18). *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. Washington, D.C. Electricity Information Sharing and Analysis Center; SANS Industrial Control Systems. https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lin, H. (2021, Mar 10). How Biden's Cyber Strategy Echoes Trump's. *Lawfare*. https://www.lawfareblog.com/how-bidens-cyber-strategy-echoes-trumps

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S. E., & Seager, T. P. (2013). Measurable Resilience for Actionable Policy. *Environmental Science and Technology*, *17*(18), 10108–10110.

Linkov, I., & Kott, A. (Eds.). (2019). *Cyber Resilience of Systems and Networks*. *Cyber Resilience of Systems and Networks*. Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3_1

Louviere, J. J., Hensher, D. A., & Swait, J. D. (2000). *Stated choice methods: Analysis and Applications.* Cambridge University Press. https://doi.org/10.1017/CBO9780511753831

Lund, T. J., & Stains, M. (2015). The importance of context: An exploration of factors influencing the adoption of student-centered teaching among chemistry, biology, and physics faculty. *International Journal of STEM Education*, 2(1), 13.

Lundblad, J. P. (2003). A Review and Critique of Rogers' Diffusion of Innovation Theory as it Applies to Organizations. *Organization Development Journal*, *21*(4), 50–64. https://www.proquest.com/scholarly-journals/review-critique-rogers-diffusion-innovation/docview/197971687/se-2?accountid=44888

M., P., Bruenjes, R., Cohen, M., Freeman, J., Graf, R., Kilani, M., O'Leary, C., Pashley, C., Ryan, J., Shannon, G., Walters, G., & Wills, T. (2018). *Cyber Resilience and Response: 2018 Public-Private Analytic Exchange Program*. Washington, D.C. U.S. Department of Homeland Security.

https://www.dhs.gov/sites/default/files/publications/2018_AEP_Cyber_Resilience_and_Response.pdf

Martiny, K. M., Toro, J., & Høffding, S. (2021). Framing a Phenomenological Mixed Method: From Inspiration to Guidance. *Frontiers in Psychology*, *12*, 602081. https://doi.org/10.3389/fpsyg.2021.602081

McGrath, R. E., & Meyer, G. J. (2006). When effect sizes disagree: The case of r and d. *Psychological Methods, 11*(4), 386–401. https://doi.org/10.1037/1082-989X.11.4.386

McFadden, D. (1974). Conditional logit analysis of qualitative choice behavior. In P. Zarembka (Ed.), *Frontiers in econometrics* (pp. 104-142). New York: Academic Press.

Menard, S. (2009). *Logistic regression: From introductory to advanced concepts and applications.* Sage Publications. https://doi.org/10.4135/9781483348964

Merriam-Webster. (n.d.). *System*. Merriam-Webster.com dictionary. Retrieved July 4, 2022, from https://www.merriam-webster.com/dictionary/system

Miller, A. R., & Tucker, C. (2009). Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records. *Management Science*, *55*(7), 1077–1093. https://doi.org/10.1287/mnsc.1090.1014

Onwuegbuzie, A., & Johnson, R. B. (2006). The Validity Issue in Mixed Research. *Research in the Schools*, *13*(1), 48–63. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.534.5506&rep=rep1&type=pdf

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and Policy in Mental Health*, *42*(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Peiser, J. (2021, February 9). A hacker broke into a Florida town's water supply and tried to poison it with lye, police said. *The Washington Post*. https://www.washingtonpost.com/nation/2021/02/09/oldsmar-water-supply-hack-florida/?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202

Petrenko, S. (2019). *Cyber Resilience*. *River Publishers Series in Security and Digital Forensics Ser*. River Publishers. https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=2277642

Popp, D. (2010). Exploring Links Between Innovation and Diffusion: Adoption of NOX Control Technologies at US Coal-fired Power Plants. *Environmental and Resource Economics*, *45*(3), 319–352. https://doi.org/10.1007/s10640-009-9317-1

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, *51*(5), 551–567. https://doi.org/10.1016/j.im.2014.03.009

Resilience Alliance. (n.d.). *Adaptive Cycle [Infographic]*. Retrieved May 29, 2022, from https://www.resalliance.org/adaptive-cycle

Resilience Alliance. (2010). *Assessing Resilience in Social-Ecological Systems: Workbook for Practitioners*. Revised Version 2.0. https://www.resalliance.org/files/ResilienceAssessmentV2_2.pdf

Rice, M. E., & Harris, G. T. (2005). Comparing effect sizes in follow-up studies: ROC Area, Cohen's d, and r. *Law and Human Behavior, 29*(5), 615–620. https://doi.org/10.1007/s10979-005-6832-7

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, *49*, 70–94. https://doi.org/10.1016/j.cose.2014.11.007

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

Rodgers, E. M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.

Roski, J., Gillingham, B., Millegan, J., Zitelman, D., Batten, S., & Delaney, E. (2019, Aug 12). *Building Resilience For Greater Health And Performance: Learning From The Military.* Health Affairs Blog. https://www.healthaffairs.org/do/10.1377/forefront.20190807.768196/full/

Rutt, J. (2020). *Cyber Security in Focus 2020.* Stott and May. https://resources.stottandmay.com/cyber-security-in-focus-2020

Seligman, L. (2006). Sensemaking throughout adoption and the innovation-decision process. *European Journal of Innovation Management*, *9*(1), 108–120. https://doi.org/10.1108/14601060610640050

Sharkov, G. (2020). Assessing the Maturity of National Cybersecurity and Resilience. *Connections: The Quarterly Journal*, *19*(4), 5–24. https://doi.org/10.11610/Connections.19.4.01

Smith, T. J. & McKenna, C. M. (2013). A comparison of logistic regression pseudo R^2 indices. *Multiple Linear Regression Viewpoints*, 39(2), 17-26.

Software Engineering Institute. (2018). *Overview of the CERT® Resilience Management Model (CERT®-RMM)*. Carnegie Mellon University. https://www.youtube.com/watch?v=nbi9_WtQasA

Sorenson, O. (2018). Innovation Policy in a Networked World. *Innovation Policy and the Economy*, *18*, 53–77. https://doi.org/10.1086/694407

Starke, P. (2013). Qualitative Methods for the Study of Policy Diffusion: Challenges and Available Solutions. *Policy Studies Journal*, *41*(4), 561–582. https://doi.org/10.1111/psj.12032

Sun, C.-C., Hahn, A., & Liu, C.-C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020

The White House. (2021, May 12). *Executive Order on Improving the Nation's Cybersecurity*. Washington, D.C. United States Government. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

The White House. (2022, January 27). *Fact Sheet: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Water Sector*. Washington, D.C. United States Government. https://www.whitehouse.gov/briefing-

room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/

The White House. (March 2023). *National Cybersecurity Strategy*. United States Government. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

The White House. (July 2023). *National Cybersecurity Strategy Implementation Plan*. United States Government. https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

Thielfoldt, K. (2022). Internet of Medical Things Cybersecurity Vulnerabilities and Medical Professionals' Cybersecurity Awareness: A Quantitative Study. https://www.proquest.com/dissertations-theses/internet-medical-things-cybersecurity/docview/2660020655/se-2

Todd, P., & Benbasat, I. (1987). Process Tracing Methods in Decision Support Systems Research: Exploring the Black Box. *MIS Quarterly*, *11*(4), 493. https://doi.org/10.2307/248979

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795. https://doi.org/10.1016/j.irfa.2021.101795

Tran, H., Campos-Nanez, E., Fomin, P., & Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *Computers & Security*, *61*, 19–31. https://doi.org/10.1016/j.cose.2016.05.001

U.S. Cybersecurity and Infrastructure Security Agency. (July 2020). *SECURING INDUSTRIAL CONTROL SYSTEMS: A UNIFIED INITIATIVE*. FY 2019-2023.

Washington, D.C. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf

U.S. Cybersecurity and Infrastructure Security Agency. (2020, July 23). *Alert (AA20-205A): NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems* (AA20-205A). U.S. Department of Homeland Security. https://www.cisa.gov/uscert/ncas/alerts/aa20-205a

U.S. Cyberspace Solarium Commission. (2020). *Cyberspace Solarium Commission Final Report*. Washington, D.C. https://www.solarium.gov/report

U.S. Department of Homeland Security. (2013). *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience.*

U.S. Department of Homeland Security. (November 2015). *National Critical Infrastructure Security and Resilience Research and Development Plan*. Washington, D.C. United States Government. https://www.dhs.gov/sites/default/files/publications/National%20CISR%20R%26D%20Plan_Nov%202015.pdf

U.S. Government Accountability Office. (March 2021). *WEAPON SYSTEMS CYBERSECURITY: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors*. GAO-21-179. Washington, D.C. United States Government. https://www.gao.gov/assets/gao-21-179.pdf

U.S. National Institute for Standards and Technology. (November 2021). *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach: SP 800-160*

Vol. 2 Rev. 1. Washington, D.C. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final

U.S. Navy. (December 2018). *A Design for Maintaining Maritime Superiority: Version 2.0*. Washington, D.C. United States Government. https://media.defense.gov/2020/May/18/2002301999/-1/-1/1/DESIGN_2.0.PDF

U.S. Office of the Director of National Intelligence. (February 2022). *Annual Threat Assessment of the U.S. Intelligence Community*. Washington, D.C. United States Government. https://docs.house.gov/meetings/IG/IG00/20220308/114469/HHRG-117-IG00-Wstate-HainesA-20220308.pdf

U.S. Office of the President of the United States. (September 2018). *National Cyber Strategy of the United States of America*. Washington, D.C. United States Government. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

U.S. Office of the President of the United States. (March 2021). *Interim National Security Strategic Guidance*. Washington, D.C. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

U.S. Senate. (August 2020). *Federal Cybersecurity: America's Data Still at Risk.* United States Government.

Walker, B., Carpenter, S. R., Anderies, J. M., Abel, N., Cumming, G., Janssen, M. A., Lebel, L., Norberg, J., Peterson, G. D., & Pritchard, R. (2002). Resilience Management in Social-ecological Systems: a Working Hypothesis for a Participatory Approach. *Conservation Ecology*, *6*(1). https://doi.org/10.5751/ES-00356-060114

White, J. L. (2013). Logistic regression model effectiveness: proportional chance criteria and proportional reduction in error. *Journal of Contemporary Research in Education*, 2(1). https://egrove.olemiss.edu/jcre/vol2/iss1/3.

Correia, A. M., Costanzo, S., Reis, L. P., & Rocha, A. (Eds.). (2015). *Advances in Intelligent Systems and Computing: Vol. 353*. *New Contributions in Information Systems and Technologies: Volume 1* (1st ed. 2015). Springer International Publishing; Imprint: Springer. https://doi.org/10.1007/978-3-319-16486-1

Wejnert, B. (2002). Integrating Models of Diffusion of Innovations: A Conceptual Framework. *Annual Review of Sociology*, *28*(1), 297–326. https://doi.org/10.1146/ANNUREV.SOC.28.110601.141051

Wendt, J. (2021). *HYCU R-Score: Independent Assessment Tool Measures Ransomware Recovery Readiness.* DCIG, LLC. https://www.getrscore.org/wp-content/uploads/2021/09/DCIG-HYCU-R-Score-Product-Review.pdf

Wicker, R., & Hendrix, J. (2018). The Naval Imperative. *National Interest*(155), 70–77.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, *141*, 5–9. https://doi.org/10.1016/j.ress.2015.03.018

World Economic Forum. (2012). *Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines.*

Yin, R. K. (2016). *Qualitative Research from Start to Finish* (2nd ed.). Guilford Press.

Appendix A: Synthesis Matrix of Cyber Resiliency Influences Within the Reviewed Literature

Innovation-Decision Influences	Linkov & Kott 2019	Linkov et al. 2013	Ferdinand 2015	Annarelli et al. 2020	Barasa et al. 2018	Butler & Brooks 2021	Carayannis et al. 2021	Sharkov 2020	M. et al., 2018	Groenendaal & Helsloot 2021
Technical factors	F	X	X	X		X	F	X	F	X
Cultural influences	X	X		X	X		F	X	X	
Organizational influences	F		X		F	F	F	F	X	X
Workforce/skills	X			X		X	X		X	X
Knowledge management and information access	X	F	F		X	X	X	X	X	
Industry and competitiveness	X			F			X		X	
Vendor and third-party support	X					X			F	X
Legal and regulatory influences	X					X		X		
Resources and funding	F		X		X	X	X			F

Note. An "X" indicates the literature discussed this influence within the published work, either as part of a literature review, study finding, or concluding remark of some significance. An "F" indicates that the influence was presented with significant focus or was a primary finding of the study or review; "F" marks are bolded for clarity within the table.

Appendix B: Quantitative Survey Questionnaire

About this Survey and the Study
Examining Leadership Factors for Implementing Cyber Resiliency
You are invited to take part in this research study. The information in this form is meant to help you decide whether or not to take part. If you have any questions, please ask.

The purpose of this study is to better understand the innovation-decision process for cyber resiliency, and what influences affect adoption or rejection of cyber resiliency innovations at the organizational leadership level. Participants in this study should be senior information security professionals with experience in organizational cyber resiliency.

How does this study define cyber resiliency? The study adopts the definition presented within the U.S. National Institute for Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 2, defined as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources" (U.S. National Institute for Standards and Technology [NIST], 2021, p. 60).

What techniques comprise this definition of cyber resiliency? Appendix D of NIST SP 800-160 Vol. 2 describes a number of techniques that correspond to various technologies and processes comprising "cyber resilient" capabilities, including: adaptive response, analytic monitoring, contextual awareness, coordinated protection, deception, diversity of modes, dynamic positioning, non-persistence, privilege restriction, realignment, redundancy, segmentation, substantiated integrity, and unpredictability (NIST, 2021, pp. 89-91). A system is considered cyber resilient when it "provides a degree of cyber resiliency commensurate with the system's criticality" to the organization (NIST, 2021, p. 3).

What will be done during this research study? You will be asked to complete the following online survey sections, which should take approximately 13-22 minutes to complete.

- Complete the Informed Consent question at the bottom of this section that will indicate that you consent to participate in this study.
- Complete "Part I: Demographics" (2-3 minutes)
- Complete "Part II: Innovation and Structural Characteristics" (3-5 minutes)
- Complete "Part III: Limiting Influences on the Cyber Resiliency Innovation-Decision Process" (3-5 minutes)
- Complete "Part IV: Enabling Influences on the Cyber Resiliency Innovation-Decision Process" (3-5 minutes)
- Complete "Part V: The Innovation-Decision" (2-4 minutes)
- Opt-in or opt-out of the follow-on qualitative portion of the study (interviews)

What are the possible risks of being in this research study? There are no known risks to you for participating in the online survey. Should you opt-in to the qualitative portion of the study that involves experiential interviews, your views on your organization's innovation-decision process and cyber resiliency adoption will be discussed and pseudonyms shall be used to protect participant identities.

What are the possible benefits to you? You are not expected to receive any direct benefits or compensation from participating in this research study.

What are the benefits to others? This research study will contribute to the body of knowledge of the field of cybersecurity leadership, in particular cyber resiliency adoption within United States. To date, a study of this design has not been conducted that focuses on influences upon adopting or rejecting cyber resiliency as an innovation. This study has significance within national cyber defense and national security, particularly for those organizations operating with the 16 critical infrastructure sectors identified by the Department of Homeland Security. The data and results of this study will help shape future research on this topic and may influence public policy-makers to adjust approaches to encouraging cyber resiliency adoption, such as through public-private partnership programs or media campaigns.

What will participation in this research study cost you? There is no cost to you to be in this research study

How will information about you be protected? All data collected in this study is anonymous. This means no identifying information will be collected that would allow anybody to contact the participant, or attribute their answers to their personal identity or that of their organization.

What will happen if you decide not to be in this study or if you decide to stop participation during the study? Participation in this study is completely voluntary. If you choose to participate, you may stop participation at any time without penalty and without losing any benefits that are a part of this study.

What should you do if you have any questions or concerns about this research study? If you have any questions or concerns during or after this study, you may contact the Principal Investigator, Travis D. Howard at tdhoward@captech.edu. You can also contact the faculty advisor, Dr. Chris Mitchell, at cmitchell@captechu.edu.

Who can you contact if you have questions about your rights as a participant? You can speak to the Principal Researcher or you can contact the Capitol Technology University (CTU) Institutional Review Board (IRB) at irb@captechu.edu; additional information about CTU's IRB purpose, authority, responsibilities, and procedures can be found on this webpage: https://www.captechu.edu/about-capitol/leadership/institutional-review-board.

Informed Consent

I understand that this survey is completely voluntary and I can opt-out at any time by closing the form before submitting answers at the end of the survey. I have read the information disclosed by the researcher in the "About" section of the survey. By clicking "I Agree to Participate", I understand that my answers will be recorded at the end of the survey and used for statistical analysis.
I agree to participate
I do not wish to participate (exit)

Part I: Demographics

What is your current career level within the information security field?
Internship / Student
Entry
Associate
Mid-Senior
Director
Executive

How many years of experience have you had in the field of information security?
0-5 years
5-10 years
10-20 years
Over 20 years

What SPECIALTY AREA(S) have you worked within during your career? (select all that apply)
(Note: derived from the Workforce Framework for Cybersecurity, NICE Framework, https://niccs.cisa.gov/about-niccs/workforce-framework-cybersecurity-nice-framework-work-roles)
Risk Management
Software Development
Systems Architecture
Technology R&D
Systems Requirements Planning
Test and Evaluation
Systems Development
Database Administration
Knowledge Management
Customer Service and Technical Support
Network Services
System Administration
Systems Analysis
Legal Advice and Advocacy
Training, Education, and Awareness
Cybersecurity Management

Strategic Planning and Policy
Executive Cyber Leadership
Acquisition and Program/Project Management
Cyber Defense Infrastructure
Incident Response
Vulnerability Assessment and Management
Threat Analysis
Exploitation Analysis
All-Source Analysis
Targets
Language Analysis
Collection Operations
Cyber Operational Planning
Cyber Operations
Cyber Investigation
Digital Forensics
Other (Please Specify)

Are you a veteran of the U.S. Armed Forces?
Yes/No

Do you now, or have you ever, worked within one of the 16 critical infrastructure sectors designated by the Department of Homeland Security?
(Reference: https://www.cisa.gov/critical-infrastructure-sectors)
Yes/No

If yes, what CRITICAL INFRASTRUCTURE SECTOR(S) have you worked within? (select all that apply)
Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials, and Waste
Transportation Systems
Water and Wastewater Systems

During the period of time in which you experienced cyber resiliency decision-making in your organization, were you the decision-maker and/or responsible for governance and implementation of the cyber resiliency solution?
Yes/No

Part II: Organizational Characteristics
The following questions ask about the organizational structure and general innovativeness of your organization. In all questions "your organization" means the organization in which you experienced a cyber resiliency adoption decision.

In your organization, how significant was the executive leadership's positive attitude towards change influential in decision-making?
Not at all significant
Somewhat significant
Greatly significant

In your organization, to what extent has the role of an "innovation champion" (formalized or informal) at the executive or director level influenced decision making?
Not at all
To some extent
To a great extent

In your organization, to what extent have EXTERNAL NETWORKS, such as partnerships, vendor agreements, and consultancies influenced decision-makers?
Not at all
To some extent
To a great extent

In your organization, to what degree is decision-making CENTRALIZED within the organizational structure?
Not at all
To some extent
To a great extent

In your organization, to what degree is the employed workforce COMPLEX by possessing high levels of knowledge, expertise, and a wide range of occupational specialties?
Not at all
To some extent
To a great extent

In your organization, to what degree are rules FORMALIZED through documented policies and procedures?
Not at all
To some extent
To a great extent

In your organization, to what degree are internal departments and divisions INTERCONNECTED through informal or formal practices, such as social circles or working groups?
Not at all
To some extent
To a great extent

In your organization, to what degree are UNCOMMITED RESOURCES, such as funding or people, available for use in new projects in a short amount of time?
Not at all
To some extent
To a great extent

Part III: Limiting Influences on the Cyber Resiliency Innovation-Decision Process
For the following questions: During the period in which cyber resiliency measures were being considered, rate to what extent (greatly, somewhat, or not significant) the influence factor limited the decision of whether or not to adopt the cyber resiliency measure.
Consider the following definitions when making your choices:
"Limiting" means preventing or posing as an obstacle to overcome prior to the decision being made
For a factor to be "not significant" means it had no appreciable negative influence on the decision-making process

TECHNICAL FACTORS such as network topology, implementation frameworks, engineering designs, and digital tool selection.
Not significantly limiting
Somewhat limiting
Greatly limiting

CULTURAL FACTORS such as awareness and agency of cybersecurity, adaptability to change, and work culture conducive to new ideas and learning.
Not significantly limiting
Somewhat limiting
Greatly limiting

ORGANIZATIONAL INFLUENCES such as governance models, management of risks, leadership or board buy-in, innovativeness, and/or established policies and procedures.
Not significantly limiting
Somewhat limiting
Greatly limiting

WORKFORCE AND SKILLS such as mix of specialty area and work roles within the organization, or availability of specialized skills (such as skills with a specific technology or innovation type).
Not significantly limiting

Somewhat limiting
Greatly limiting

KNOWLEDGE MANAGEMENT AND INFORMATION ACCESS including access to internal and external information necessary for decision-making, and how the organization categorizes, organizes, and shares knowledge inter-organizationally.
Not significantly limiting
Somewhat limiting
Greatly limiting

INDUSTRY AND COMPETITIVENESS such as how the organization views and maintains their competitive advantage, communicates value to customers, and the general characteristics of the business and market.
Not significantly limiting
Somewhat limiting
Greatly limiting

VENDOR AND THIRD-PARTY SUPPORT such as how the organization's technology infrastructure is supported through vendor contracts, managed services, and other third-party offerings.
Not significantly limiting
Somewhat limiting
Greatly limiting

LEGAL AND REGULATORY INFLUENCES to include international, national, state, and/or local laws and regulations affecting the organization, marketplace, or industry sector.
Not significantly limiting
Somewhat limiting
Greatly limiting

RESOURCES AND FUNDING such as spending power of the organization, access to funding, budgetary management, and access to adequate material resources.
Not significantly limiting
Somewhat limiting
Greatly limiting

Part IV: Enabling Influences on the Cyber Resiliency Innovation-Decision Process
For the following questions: During the period in which cyber resiliency measures were being considered, rate to what extent (greatly, somewhat, or not significant) the influence factor enabled the decision of whether or not to adopt the cyber resiliency measure. Consider the following definitions when making your choices:
"Enabling" means a helpful or positive influence on the decision-making process or overall outcome
For a factor to be "not significant" means it had no appreciable positive influence on the decision-making process

TECHNICAL FACTORS such as network topology, implementation frameworks, engineering designs, and digital tool selection.
Not significantly enabling
Somewhat enabling
Greatly enabling

CULTURAL FACTORS such as awareness and agency of cybersecurity, adaptability to change, and work culture conducive to new ideas and learning.
Not significantly enabling
Somewhat enabling
Greatly enabling

ORGANIZATIONAL INFLUENCES such as governance models, management of risks, leadership or board buy-in, innovativeness, and/or established policies and procedures.
Not significantly enabling
Somewhat enabling
Greatly enabling

WORKFORCE AND SKILLS such as mix of specialty area and work roles within the organization, or availability of specialized skills (such as skills with a specific technology or innovation type).
Not significantly enabling
Somewhat enabling
Greatly enabling

KNOWLEDGE MANAGEMENT AND INFORMATION ACCESS including access to internal and external information necessary for decision-making, and how the organization categorizes, organizes, and shares knowledge inter-organizationally.
Greatly enabling
Somewhat enabling
Not significantly enabling

INDUSTRY AND COMPETITIVENESS such as how the organization views and maintains their competitive advantage, communicates value to customers, and the general characteristics of the business and market.
Not significantly enabling
Somewhat enabling
Greatly enabling

VENDOR AND THIRD-PARTY SUPPORT such as how the organization's technology infrastructure is supported through vendor contracts, managed services, and other third-party offerings.
Not significantly enabling
Somewhat enabling
Greatly enabling

LEGAL AND REGULATORY INFLUENCES to include international, national, state, and/or local laws and regulations affecting the organization, marketplace, or industry sector.
Not significantly enabling
Somewhat enabling
Greatly enabling

RESOURCES AND FUNDING such as spending power of the organization, access to funding, budgetary management, and access to adequate material resources.
Not significantly enabling
Somewhat enabling
Greatly enabling

Part V: The Innovation-Decision

Are there other influence factors not listed here that were significant to the decision-making process to adopt or reject cyber resiliency measures within your organization?
Yes/No

If yes, please describe this influence, or influences, and how it affected the process
Short Answer: _____

What was the final decision in adopting or rejecting this cyber resiliency capability?
Adoption through trial program
Adoption through observing results of trial from others
Full adoption without trial
Rejection after consideration or trial
Rejection without consideration

Are there any other comments you would like to make in relation to the innovation-decision process you experienced that may be relevant to this study?
Short Answer: _____

Optional: Opt-in for Qualitative Component of this Study

The researcher is concurrently pursuing one-on-one interviews with participants to understand lived experiences with cyber resiliency, as part of a mixed-method study design. This involves an internet-based virtual interview session conducted through the Zoom conferencing platform; the use of Zoom is ideal to maintain anonymity of the participant and video is not required. The inclusion of qualitative, lived-experiential data will enrich the study through a correlational analysis of survey results (closed-ended questions) and interview narratives (open-ended questions).

Your participation is greatly valued and will add to the credibility of the study through triangulation and converging lines of inquiry.

Ideal Participant: The ideal participant for an experiential interview is a senior, director, or executive level professional who has had direct decision-making experience with cyber resiliency.

Session Details: The Zoom session would be scheduled for no more than one hour, with the potential for follow-up discussions if agreed upon by the participant and researcher. The session will be recorded and the researcher will take notes. There is a potential for the participant to be directly quoted in the published study. The recorded audio/video is kept confidential, used by the researcher for analysis purposes only, and will not be shared nor published as part of the study. The use of video during the zoom session is not required.

Information Collected: The information collected is strictly limited to the lived experience of how the participant navigated the innovation-decision process for cyber resiliency within their organization.

- No personally identifying information will be collected; identities of the participants will be masked with the use of pseudonyms and anonymized identifiers.
- No organizationally identifying information will be collected other than the sector or industry the organization operates within.

Email Contact and Next Steps: The researcher will contact you via an official university ".edu" email address associated with Capitol Technology University to set up a time and date that is convenient for you.

Attribution: By opting in to the interview process the participant will be attributing a chosen pseudonym and an email address, that they choose to provide, to their answers in this survey. The researcher may use this association in correlational analysis. Participants are directed through the survey instructions to mask their given name by providing a chosen name (pseudonym) instead, and to use an email address for correspondence that is not attributable to their real identity. The use of identity masking techniques will not affect the research results. These risk control instructions are included in the opt-in section of the survey and disclosed to potential interview participants.

Are you willing and able to participate in an interview about your experience with cyber resiliency implementation?
Yes, the researcher may contact me to schedule an interview, and I have read and understood the opt-in instructions
No, thank you

If yes, provide an identifier (pseudonym or chosen name) and email address for the researcher to contact you.
Name: _____
Email: _____

Appendix C: Qualitative Interview Questionnaire

Researcher Opening Statement and Informed Consent:

The purpose of this study is to better understand the innovation-decision process for cyber resiliency, and what influences affect adoption or rejection of cyber resiliency innovations at the organizational leadership level. Participants in this study should be senior, director, or executive level information security professionals with experience in organizational cyber resiliency.

This interview collects qualitative, lived-experiential data will enrich the study through a correlational analysis of survey results and interview narratives. Your participation is greatly valued and will add to the credibility of the study through triangulation and converging lines of inquiry.

This session's duration will not exceed one hour with the potential for follow-up discussions if agreed upon by the participant and researcher. The session will be recorded and the researcher will take notes. There is a potential for the participant to be directly quoted in the published study. The recorded audio/video is kept confidential, used by the researcher for analysis purposes only, and will not be shared nor published as part of the study.

Do you consent to continue?
Yes/No

Interview Protocol
Project: *Examining Leadership Factors for Implementing Cyber Resiliency*

Time of Interview: _____

Date: _____

Location: _____

Interviewer: *Travis D. Howard*
Position of Interviewer: *Primary Investigator and PhD Candidate*

Participant: _____
Position of Participant (relevant to the study): _____

- **[ ] Mid-Senior Level**
- **[ ] Director Level**
- **[ ] Executive Level**

Questions:

1. What was the cyber resiliency capability that your organization considered implementing at the time of your experience?

2. Who were the most significant people, interorganizational group, or external groups that influenced the decision-making process?
3. How innovative is your organization? Why or why not?
4. What was your experience with limiting factors in cyber resiliency implementation?
5. What was your experience with enabling, or positive, factors in cyber resiliency implementation?
6. What was the ultimate decision in implementing or rejecting the capability and how did it affect the organization?
7. Do you feel the right decision was made? Why or why not?

Thank the individual for participating in the interview, assure confidentiality of the responses, and discuss potential for a follow-up interview.

Appendix D: Data Tables

Table 8

Frequency Table for Survey Questions 2, 3, 4, 5, 6, 7, and 8

Variable	*n*	*%*
What is your current career level within the information security field?		
Mid-Senior	35	50.72
Director	19	27.54
Executive	15	21.74
Missing	0	0.00
How many years of experience have you had in the field of information security?		
5-10 years	16	23.19
10-20 years	25	36.23
Over 20 years	28	40.58
Missing	0	0.00
What SPECIALTY AREA(S) have you worked within during your career?		
Risk Management	58	84.06
Software Development	24	34.78
Systems Architecture	33	47.83
Technology R&D	20	28.99
Systems Requirements Planning	33	47.83
Test and Evaluation	30	43.48
Systems Development	30	43.48
Database Administration	12	17.39
Knowledge Management	33	47.83
Customer Service and Technical Support	31	44.93
Network Services	31	44.93
Systems Analysis	21	30.43
Legal Advice and Advocacy	8	11.59
Training, Education, and Awareness	45	65.22
Cybersecurity Management	62	89.86
Strategic Planning and Policy	43	62.32
Executive Cyber Leadership	28	40.58
Acquisition and Program/Project Management	31	44.93
Cyber Defense Infrastructure	33	47.83
Incident Response	39	56.52
Vulnerability Assessment and Management	48	69.57

Variable	*n*	*%*
Threat Analysis	36	52.17
Exploitation Analysis	17	24.64
All-Source Analysis	14	20.29
Targets	6	8.70
Language Analysis	2	2.90
Collection Operations	7	10.14
Cyber Operational Planning	24	34.78
Cyber Operations	32	46.38
Cyber Investigation	27	39.13
Digital Forensics	18	26.09
Other (please specify)	3	4.35
Are you a veteran of the U.S. Armed Forces?		
Yes	32	46.38
No	37	53.62
Missing	0	0.00
Do you now, or have you ever, worked within one of the 16 critical infrastructure sectors		
Yes	61	88.41
No	8	11.59
Missing	0	0.00
If yes, what CRITICAL INFRASTRUCTURE SECTOR(S) have you worked within?		
None of the above	4	5.80
Chemical	1	1.45
Commercial Facilities	2	2.90
Communications	17	24.64
Critical Manufacturing	2	2.90
Defense Industrial Base	27	39.13
Emergency Services	2	2.90
Energy	8	11.59
Financial Services	7	10.14
Food and Agriculture	2	2.90
Government Facilities	26	37.68
Healthcare and Public Health	10	14.49
Information Technology	40	57.97
Nuclear Reactors, Materials, and Waste	5	7.25
Transportation Systems	3	4.35
Water and Wastewater Systems	5	7.25
During the period in which you experienced cyber resiliency decision-making in your organization, were you		

Variable	*n*	*%*
the decision-maker and/or responsible for governance and implementation of the cyber resiliency solution?		
Yes	44	63.77
No	25	36.23
Missing	0	0.00

Note. Due to rounding errors, percentages may not equal 100%.

Table 9

Frequency Table for Characteristics of Organizational Innovativeness (Survey Questions 9, 10, 11, 12, 13, 14, 15, and 16).

Variable	*n*	*%*
In your organization, how significant was the executive leadership's positive attitude towards change influential in decision-making?		
Somewhat significant	19	27.54
Greatly significant	50	72.46
Missing	0	0.00
In your organization, to what extent has the role of an "innovation champion" (formalized or informal) at the executive or director level influenced decision making?		
Not at all	14	20.29
To some extent	26	37.68
To a great extent	29	42.03
Missing	0	0.00
In your organization, to what extent have EXTERNAL NETWORKS, such as partnerships, vendor agreements, and consultancies influenced decision-makers?		
Not at all	6	8.70
To some extent	49	71.01
To a great extent	14	20.29
Missing	0	0.00
In your organization, to what degree is decision-making CENTRALIZED within the organizational structure?		
Not at all	7	10.14
To some extent	43	62.32

Variable	*n*	*%*
To a great extent	19	27.54
Missing	0	0.00
In your organization, to what degree is the employed workforce COMPLEX by possessing high levels of knowledge, expertise, and a wide range of occupational specialties?		
Not at all	2	2.90
To some extent	27	39.13
To a great extent	40	57.97
Missing	0	0.00
In your organization, to what degree are rules FORMALIZED through documented policies and procedures?		
Not at all	1	1.45
To some extent	28	40.58
To a great extent	40	57.97
Missing	0	0.00
In your organization, to what degree are UNCOMMITED RESOURCES, such as funding or people, available for use in new projects in a short amount of time?		
Not at all	18	26.09
To some extent	45	65.22
To a great extent	6	8.70
Missing	0	0.00

Note. Due to rounding errors, percentages may not equal 100%.

Table 10

Frequency Table for Outcome Variable

Variable	*n*	*%*
Organization Decision		
Adoption through trial program	36	52.17
Adoption through observing results of trial from others	19	27.54
Full adoption without trial	8	11.59
Rejection after consideration or trial	1	1.45
Rejection without consideration	5	7.25
Missing	0	0.00

Variable	*n*	*%*
Organization Decision- dichotomous		
Adoption	63	91.30
Rejection	6	8.70
Missing	0	0.00

Note. Due to rounding errors, percentages may not equal 100%.

Table 11

Frequency Table for Limiting Factors

Variable	*n*	*%*
Technical Factors		
Not significantly limiting	15	21.74
Somewhat limiting	35	50.72
Greatly limiting	19	27.54
Missing	0	0.00
Cultural Factors		
Not significantly limiting	11	15.94
Somewhat limiting	30	43.48
Greatly limiting	28	40.58
Missing	0	0.00
Organizational Influences		
Not significantly limiting	10	14.49
Somewhat limiting	34	49.28
Greatly limiting	25	36.23
Missing	0	0.00
Workforce and Skills		
Not significantly limiting	16	23.19
Somewhat limiting	30	43.48
Greatly limiting	23	33.33
Missing	0	0.00
Knowledge Management and Information Access		
Not significantly limiting	17	24.64
Somewhat limiting	38	55.07
Greatly limiting	14	20.29
Missing	0	0.00
Industry and Competitiveness		

Variable	*n*	*%*
Not significantly limiting	40	57.97
Somewhat limiting	21	30.43
Greatly limiting	8	11.59
Missing	0	0.00
Vendor and Third-party Support		
Not significantly limiting	16	23.19
Somewhat limiting	41	59.42
Greatly limiting	12	17.39
Missing	0	0.00
Legal and Regulatory Influences		
Not significantly limiting	22	31.88
Somewhat limiting	26	37.68
Greatly limiting	21	30.43
Missing	0	0.00
Resources and Funding		
Not significantly limiting	9	13.04
Somewhat limiting	25	36.23
Greatly limiting	35	50.72
Missing	0	0.00

Note. Due to rounding errors, percentages may not equal 100%.

Table 12

Frequency Table for Enabling Variables

Variable	*n*	*%*
Technical Factors		
Not significantly enabling	10	14.49
Somewhat enabling	41	59.42
Greatly enabling	18	26.09
Missing	0	0.00
Cultural Influences		
Not significantly enabling	15	21.74
Somewhat enabling	31	44.93
Greatly enabling	23	33.33
Missing	0	0.00
Organizational Influences		

Variable	*n*	*%*
Not significantly enabling	11	15.94
Somewhat enabling	37	53.62
Greatly enabling	21	30.43
Missing	0	0.00
Workforce and Skills		
Not significantly enabling	12	17.39
Somewhat enabling	41	59.42
Greatly enabling	16	23.19
Missing	0	0.00
Knowledge Management and Information Access		
Not significantly enabling	18	26.09
Somewhat enabling	39	56.52
Greatly enabling	12	17.39
Missing	0	0.00
Industry and Competitiveness		
Not significantly enabling	31	44.93
Somewhat enabling	32	46.38
Greatly enabling	6	8.70
Missing	0	0.00
Vendor and Third-party Support		
Not significantly enabling	20	28.99
Somewhat enabling	35	50.72
Greatly enabling	14	20.29
Missing	0	0.00
Legal and Regulatory Influences		
Not significantly enabling	27	39.13
Somewhat enabling	28	40.58
Greatly enabling	14	20.29
Missing	0	0.00
Resources and Funding		
Not significantly enabling	18	26.09
Somewhat enabling	36	52.17
Greatly enabling	15	21.74
Missing	0	0.00

Note. Due to rounding errors, percentages may not equal 100%.

Table 13

Variance Inflation Factors for technical factors, cultural factors, workforce and skills, knowledge management, organizational influences, industry and competition, vendor third-party support, legal regulatory, and resources and funding

Variable	VIF
Technical factors	1.52
Cultural factors	1.67
Workforce and skills	4.62
Knowledge management	2.91
Organizational influences	1.86
Industry and competition	1.50
Vendor third-party support	2.47
Legal regulatory	1.62
Resources and funding	1.56

Table 14

Logistic Regression Results with enabling factors: technical factors, cultural factors, workforce and skills, knowledge management, organizational influences, industry and competition, vendor third-party support, legal regulatory, and resources and funding Predicting organization decision.

Variable	*B*	*SE*	χ^2	*p*	*OR*	95.00% CI
(Intercept)	-1.69	2.32	0.53	.467	-	-
Technical factors	1.63	1.07	2.32	.128	5.12	[0.63, 41.89]
Cultural factors	0.33	0.88	0.14	.705	1.40	[0.25, 7.90]
Workforce and skills	1.65	1.77	0.87	.352	5.20	[0.16, 167.34]
Knowledge management	-2.24	1.36	2.70	.100	0.11	[0.007, 1.54]

Organizational influences	0.52	1.01	0.27	.605	1.69	[0.23, 12.25]
Industry and competition	0.83	1.05	0.64	.425	2.30	[0.30, 17.93]
Vendor third-party support	-0.85	1.01	0.71	.399	0.43	[0.06, 3.09]
Legal regulatory	-0.53	0.84	0.41	.524	0.59	[0.11, 3.04]
Resources and funding	1.15	1.05	1.20	.274	3.16	[0.40, 24.86]

Note. $\chi^2(9) = 14.77$, $p = .097$, McFadden $R^2 = 0.36$.

Table 15

Variance Inflation Factors for technical factors, cultural factors, workforce and skills, knowledge management, organizational influences, industry and competition, vendor third-party support, legal regulatory, and resources and funding

Variable	**VIF**
Technical factors	1.46
Cultural factors	1.79
Organizational influences	2.18
Workforce and skills	1.74
Knowledge management	1.58
Industry and competition	1.47
Vendor third-party support	1.85
Legal regulatory	2.08

Table 16

Logistic Regression Results with limiting factors: technical factors, cultural factors, workforce and skills, knowledge management, organizational influences, industry and

competition, vendor third-party support, legal regulatory, and resources and funding

Predicting organization decision.

Variable	*B*	*SE*	χ^2	*p*	*OR*	95.0 0% CI
(Intercept)	4.02	2.58	2.43	.119	-	-
Technical factors	-0.90	0.80	1.27	.261	0.41	[0.09, 1.95]
Cultural factors	0.11	0.82	0.02	.895	1.11	[0.22, 5.58]
Organizational influences	-1.82	1.11	2.67	.102	0.16	[0.02, 1.44]
Workforce and skills	0.42	0.86	0.24	.623	1.53	[0.28, 8.27]
Knowledge management	0.38	0.86	0.20	.658	1.46	[0.27, 7.95]
Industry and competition	1.50	0.98	2.33	.127	4.46	[0.65, 30.54]
Vendor third-party support	-0.95	0.99	0.91	.340	0.39	[0.06, 2.72]
Legal regulatory	1.29	0.81	2.53	.112	3.64	[0.74, 17.93]

Note. $\chi^2(8) = 6.88$, $p = .550$, McFadden $R^2 = 0.17$.

Table 17

Significant Statements on Cyber Resiliency Adoption Influences

Significant Statement	**Formulated Meaning**
Organizational politics greatly influenced and affected the process in all (secure) IT lifecycle stages.	Organizational factors were highly influential both positively and negatively.
Response to an adverse event. We had a small program that was moving slowly. Once we had a major cyber event, we	Real-world cyber events that negatively affected the organization were

Significant Statement	Formulated Meaning
gained substantial executive support that lasted for 5+ years.	significant enablers to creating positive organizational influences.
Many stovepipes throughout the organization, each trying to do their own thing. Makes resiliency almost impossible to attain across the board. Locally perhaps, but for the full organization, not a chance.	Adverse organizational factors prevented enterprise-wide cyber resiliency efforts.
In general, the fundamental enabler/disabler for developing resilient/survivable warfighting systems is the ability or inability of the govt program office to fully incorporate cybersecurity into the defense acquisition system and System Engineering processes.	For cyber resiliency programs within the U.S. federal government, a combination of legal and regulatory, technical, and Organizational factors are highly influential in implementing resiliency capabilities.
Most of our leaders want cybersecurity....but having a strong boss/leader, a smart CEO, a supportive BoD, and a security-minded IT team enables cybersecurity growth.	Organizational factors, specifically leadership buy-in, was significantly enabling to cyber resiliency efforts.
This is a leadership thing [prioritizing], this is what leaders are support [sic] to do.	Organizational factors, specifically leadership buy-in, was significantly enabling to cyber resiliency efforts.
There is no accountability.	Negative organizational factors, specifically leadership's ability to deflect responsibility for adverse cyber effects as a result of their decisions, can create the perception of a lack of accountability.

Table 18

Significant Statements on Cyber Resiliency or Cybersecurity in General

Significant Statement	Formulated Meaning
We talk it to death, then it becomes obsolete or overcome by events.	Cultural resistance to change prevented cyber resiliency adoption.

Significant Statement	Formulated Meaning
Get politics out of cyber security. Let us do our job.	Participant experienced significant cultural and organizational factors that negatively affected work performance.
Executive level buy-in is key obviously. Having someone engaged, knowledgeable and championing security at the Executive level made things much easier for us.	Organizational factors, specifically leadership buy-in, was significantly enabling for all cybersecurity efforts.
Cyber security was seen as a "must have" to protect (recover) our reputation first. It became a competitive differentiator ("look how good we are!") after years of investment and effort.	Leadership buy-in started as a risk reduction and incident response necessity, but changed to view cybersecurity as a marketplace differentiator and strategic advantage for the organization.
Investing in cyber is more important than buying another [asset].	Investing in cyber capabilities for existing assets over investing in more assets without (or reduced) cyber capabilities is viewed by this participant as holding higher strategic value for the organization.

Table 19

Observed Themes and Frequency

Observed Theme	Frequency of Mention (n)	%
Perception that the organization is innovative	4	5.48
Flawed implementation or decision-making was a key limiting factor	7	9.59
Leadership buy-in/support as significantly influential	10	13.70
Cultural resistance to change as a key limiting factor	14	19.18
Security apathy/lack of awareness as a key limiting factor	5	6.85

Past incidents or events as enabling factor or accelerator	8	10.96
Commitment of resources as most significant	8	10.96
Engineering/Technical feasibility of the innovation as a limiting factor	4	5.48
Organizational policies, procedures, strategies, or legal requirements as a key driver	13	17.81