AN ANALYSIS OF U.S. STATE LEVEL CYBERSECURITY PLANS AND POLICIES

by

Mesut Karakoç

A dissertation submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Urban Affairs and Public Policy.

Summer 2022

© 2022 Mesut Karakoç
All Rights Reserved

AN ANALYSIS OF U.S. STATE LEVEL

CYBERSECURITY PLANS AND POLICIES

by

Mesut Karakoç

Approved: _____

Sarah Bruch, Ph.D.
Program Director of the Doctoral Program in Urban Affairs and Public Policy

Approved: _____

Maria P. Aristigueta, D.P.A
Dean of the Joseph R. Biden School of Public Policy and Administration

Approved: _____

Louis F. Rossi, Ph.D.
Vice Provost for Graduate and Professional Education and
Dean of the Graduate College

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Daniel Rich, Ph.D.
Professor in charge of dissertation

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Minion K.C. Morrison, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Jerome R. Lewis, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Nii Attoh-Okine, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Stephen Viña, J.D.
Member of dissertation committee

ACKNOWLEDGMENTS

It feels great to achieve a goal that I dreamed about over ten years ago. It was a long challenging journey with many ups and downs. I would like to thank all the people who encouraged me during this journey.

No words of gratitude can summarize the thankfulness that I owe to my academic father, Dr. Daniel Rich, who has always been a power source for me. I could never finish this project without his immeasurable help. I will always appreciate his kindness, generosity, and understanding. I would also like to thank my mentor, Dr. Minion K. C. Morrison, for his contribution to my intellectual progress in addition to his genuine friendship. I have already missed our humorous and rich conversations on our way to teaching UAPP225. I am also grateful to Dr. Jerome Lewis for his continuous encouragement and support from the days of my MPA program. Thank you for keeping your office doors open and available for all the times when I needed it. Many thanks also to other committee members, Stephen Viña and Dr. Nii Attoh-Okine, for their feedback and discussion. Their ideas from different perspectives have always been valuable to me.

I am grateful to the Republic of Turkey, the Ministry of National Education for the financial support. I would not have had a chance to study at the University of Delaware without their fellowship. I also want to thank Biden School for providing me teaching and research experience.

I would also like to thank my parents and my sister, Tuncer, Nermin, and Gamze. Words cannot express how grateful I am to them for all of the support and sacrifices that they have made on my behalf.

The writing sessions and friendship of Kelsey Edmond have kept me motivated and on track. Her witnessing of all my life events means a lot to me.

Lastly, I am eternally grateful to Büşra, who is the first reviewer of all my work, and my loving and supportive wife. Now, I understand she was right by saying "You are almost done! You will be okay!" every time when I struggle with something during this Ph.D. journey. I am sure I could not even see the light at the end of the tunnel without her support.

Thank you!

TABLE OF CONTENTS

LIST OF TABLES xi
LIST OF FIGURES xiii
ABSTRACT xiv

Chapter

1 INTRODUCTION 1

1.1 Research Problem 1
1.2 Purpose of the Research 4
1.3 Cybersecurity Terminology Discussion 6
1.4 Significance of the Research 10
1.5 Research Questions 14
1.6 Organization of the Research 16

2 LITERATURE REVIEW 19

2.1 Importance of Cybersecurity Planning and Policymaking 19
2.2 U.S. Federalism and Cybersecurity 22
2.3 National-level Cybersecurity 26
2.4 Local-level Cybersecurity 30

2.4.1 Barriers in Local-level Cybersecurity 31

2.4.1.1 Insufficient Budget 31
2.4.1.2 Lack of Expertise 33
2.4.1.3 Lack of Adequately Trained Personnel 34
2.4.1.4 (Un)awareness of Being Under Attack 35

2.4.2 Proposals for Improving Local-Level Cybersecurity 35

2.4.2.1 Funding 35
2.4.2.2 Training 36
2.4.2.3 Better Equipment 36
2.4.2.4 Better Coordination and Communication 37
2.4.2.5 Culture 37

2.5 State-level Cybersecurity 38
2.5.1 Barriers and Challenges 40
2.5.1.1 Lack of Sufficient Funding 40
2.5.1.2 Increasing Sophistication of Threats 41
2.5.1.3 Inadequate Availability of Cybersecurity Professionals 41
2.5.1.4 Lack of Adequate Cybersecurity Planning 43
2.5.2 Proposals for Improving State-Level Cybersecurity 44
2.6 Summary 46
3 CONCEPTUALIZATION AND RESEARCH DESIGN 48
3.1 Concepts 48
3.1.1 Cybersecurity Planning Documents 48
3.1.2 Cybersecurity-related Policies 50
3.1.3 The Best Practices 50
3.1.3.1 NIST Cybersecurity Framework 51
3.1.3.1.1 The Framework Core 54
3.1.3.2 Criteria from the Literature 61
3.2 Research Questions and Methodology 64
3.3 Data collection 68
3.3.1 Cybersecurity Planning Documents 68
3.3.2 Cybersecurity-related Policies 68
3.4 Data Analysis 69
3.4.1 Document Analysis of the State Cybersecurity Planning Documents and Policies 69
3.4.2 Sample Selection 71
3.5 Summary 74
4 AN ANALYSIS OF 50 STATES' CYBERSECURITY PLANNING DOCUMENTS 75

4.1 Introduction 75
4.2 The State of Cybersecurity Planning of the States 76
4.3 Key Themes of Cybersecurity Plans 82

4.3.1 Training 82
4.3.2 Partnership 84
4.3.3 Coordination and Communication 86
4.3.4 Developing Awareness & Culture for Cybersecurity 87
4.3.5 Better Equipment 89
4.3.6 Leadership 90
4.3.7 Funding 92
4.3.8 National Security 93

4.4 Cross-state Analyses 95

4.4.1 Level of Depth 95
4.4.2 Level of Coverage 102

4.5 Conclusion 108

5 INCORPORATION OF NIST CYBERSECURITY STANDARDS 111

5.1 Conceptualization Of NIST Cybersecurity Framework Functions 111
5.2 Operationalization of NIST Cybersecurity Framework Functions 113
5.3 Incorporation of NIST Cybersecurity Standards 114
5.4 Cross-state Analysis of Cybersecurity Planning documents in terms of NIST Cybersecurity Framework Functions 120
5.5 State Model of the Best Cybersecurity Planning Practices 127

5.5.1 Rhode Island 127
5.5.2 Connecticut 131
5.5.3 Virginia 132

5.6 Conclusion 135

6 AN ANALYSIS OF SAMPLE STATES' CYBERSECURITY-RELATED LEGISLATED POLICIES 137

6.1 Introduction 137
6.2 The Landscape of Sample States' Cybersecurity-related Legislated Policies 138
6.3 Key Themes of Cybersecurity-related Policies 142

6.3.1 Coordination and Communication 143

6.3.2 Funding 144
6.3.3 Leadership 145
6.3.4 Better Equipment 146
6.3.5 Partnership 147
6.3.6 Developing Awareness & Culture for Cybersecurity 148
6.3.7 Training 149
6.3.8 National Security 149

6.4 A Cross-state Analysis of the Correspondence of Cybersecurity-related Policies and Plans of Sample States 150

6.4.1 Policy-Planning Correspondence Based on the Scholarly Criteria 150
6.4.2 Policy-Planning Correspondence Based on the NIST Cybersecurity Framework Functions 155

6.5 Categorization of Sample States Based on Their Cybersecurity-related Policies 158

6.5.1 States of California-Maryland-Montana 158
6.5.2 States of Florida-Virginia 161
6.5.3 States of Delaware-New York-Wyoming 162

6.6 Conclusion 164

7 CONCLUSION 167

7.1 Research Findings and Conclusions 167
7.2 Research Contributions 173
7.3 Research Implications for State Cybersecurity Planning and Policy 175
7.4 Limitations 179
7.5 Future Research 180

REFERENCES 183

Appendix

LINEAR REGRESSION ANALYSIS OF THE COVERAGE OF SCHOLARLY THEMES 201

LIST OF TABLES

Table 3.1 Function and Category Unique Identifiers 57

Table 3.2 NIST Cybersecurity Framework Functions, Categories, and Descriptions 58

Table 4.1 Characteristics of State Plans 76

Table 4.2 Number of States that Cover Each Theme 83

Table 4.3 Examples from Planning Documents 95

Table 4.4 States categorized based on level of coverage. 103

Table 4.5 Correlation Among the Coverage of Eight Scholarly Themes 107

Table 5.1 Coding NIST Cybersecurity Framework Functions. 114

Table 5.2 The Correlation Table of NIST Cybersecurity Functions 119

Table 5.3 Binary Code of State Cybersecurity Planning Documents' Incorporation of NIST Cybersecurity Framework Functions 120

Table 5.4 Cross-state Analysis based on NIST Cybersecurity Framework 122

Table 5.5 Allocation of States Based on the NIST Cybersecurity Framework Functions 124

Table 5.6 Evolution of Rhode Island's Cybersecurity 130

Table 6.1 Number of Enacted, Fail to Enact, and Pending Cybersecurity-related Policies of Sample States 140

Table 6.2 Legislative Activities, Political Cultures, and Regions of Sample States 141

Table 6.3 The Scholarly Themes and the Sample States that Cover the Themes in Cybersecurity-related Policies 143

Table 6.4 A Comparison of Planning Documents and Cybersecurity-related Policies based on Scholarly Themes of Sample States 152

Table 6.5 A Comparison of Planning Documents and Cybersecurity-related Policies based on NIST Functions of Sample States..... 156

LIST OF FIGURES

Figure 1.1 Google Trends of Security 2004-2019. 7

Figure 2.1 Main challenges to achieving a strong cybersecurity posture within Federal, State, and local government organizations 33

Figure 2.2 Top three barriers in addressing cybersecurity challenges. 42

Figure 3.1 NIST Cybersecurity Framework Core Functions. 55

Figure 3.2 Steps of Qualitative Data Analysis 70

Figure 3.3 Sample Selection. 73

Figure 4.1 Centralized versus Decentralized System. 79

Figure 4.2 Scatter plot analysis of States based on scholarly themes and political culture. 105

Figure 5.1 The percentages of States that cover each NIST Cybersecurity Framework Function. 118

Figure 5.2 Fitted Regression Analysis of NIST Compliances Based on the Scholarly Themes. 126

Figure 5.3 Screenshot from Rhode Island State Cybersecurity Strategy 128

Figure 5.4 2016-2018 Critical Controls Comparison. 132

Figure 5.5 Virginia's Cyber Security Resources. 134

ABSTRACT

While technological developments and interconnected information networks have improved many aspects of individuals' lives and increased the effectiveness of public and private services, they also have created cybersecurity challenges. To address these challenges, governments at federal, state, and local levels have started to plan and make policies that improve their cybersecurity posture. This research explores U.S. state governments' cybersecurity planning documents and cybersecurity-related policies. Through the use of document analyses methods, the research reveals the landscape of 50 states' cybersecurity planning documents and sample states' cybersecurity-related legislative policies. In addition, this study combines issue-area specific criteria gained from the state and local government cybersecurity scholarship with overall guidelines from the 2018 NIST Cybersecurity Framework. By doing so, this research contributes to a Best Practices Framework, which is the most complete set of assessment criteria for state cybersecurity planning and policymaking. The research offers a categorization of states based on how well their planning documents and policies incorporate the Best Practices Framework. Findings show that while all states engage in cybersecurity planning and policy making to some extent, there is significant variation across states' level of incorporation of the Best Practices Framework.

For the sample states with high cyberattack figures, the research conducts a correspondence assessment between their planning documents and policies. The assessment finds that the majority of sample states present a high correspondence level

between planning and legislative policy, and their policies incorporate the Best Practices Framework better than their plans. Overall, the research findings lead to the conclusion that cybersecurity policies often lead planning rather than the other way around. Besides contributing one of the first academic endeavors that systematically research state level cybersecurity governance, the research findings and conclusions offer lessons for state cybersecurity planners and policy makers. The research significance stems from the exploration of an emerging and understudied issue area for state governments, the development of an original framework for the assessment of cybersecurity planning documents and policies, and the generation of options for improving cybersecurity posture for state governments.

Chapter 1

INTRODUCTION

This research focuses on cybersecurity planning documents and cybersecurity-related policies of state governments. It explores the landscape of cybersecurity planning documents adopted by state governments as of December 2021. The research also analyzes the extent to which cybersecurity planning documents of states incorporate the best practices as defined by the 2018 NIST Cybersecurity Framework and scholarly criteria. After exploring all the planning documents, the research focuses on sample states that are selected based largely on cyberattack figures, cybersecurity job supply, and political culture of the states. With a closer examination of the sample states' cybersecurity legislative policies enacted from 2015 to 2021, the research reveals whether they adopt the NIST Cybersecurity Framework and scholarly themes. Most importantly, this research analyzes if and the ways in which cybersecurity-related policies correspond to cybersecurity planning documents.

1.1 Research Problem

In the United States, the state governments collect sensitive data and store the information in many databases to provide a range of public services to their residents. For instance, elections are run by state and local governments. Across many state governments, elections use different types of voting equipment, with some making use of electronic devices and others using paper ballots to record votes. Whether the actual mechanism of voting is electronic or not, all state and local governments have a voter

database that contains voter information. In addition, the collection of tax revenues requires states to collect data from residents.

One of the known examples of the election security failures is the 2016 United States presidential election. Some state-sponsored hackers hit election systems in 39 States. One of these 39 States was Illinois. In July 2016, according to the general counsel for the Illinois board of elections, the state's networks were breached, allowing the unauthorized access and exfiltration of data. The hackers accessed the state's voter database, which contained sensitive information of 15 million people (Bruer & Perez, 2016; Goudie & Tressel, 2020; Riley & Robertson, 2017). This case created the public perception that citizens were manipulated regarding their voting behavior.

State infrastructures, databases, and electronic devices that state government agencies use for public services are significant targets for cyber attackers. For instance, in 2009, a hacker breached one of the health websites of Virginia government and accessed to 8.3 million people's patient records and prescriptions (Goodin, 2009; Merrill, 2009; WikiLeaks, 2009). In 2011, the personal information of 3.5 million people who live in Texas were disclosed as a result of the Texas comptroller's office data breach. The office spent $1.8 million on this data breach (Kerschberg, 2011; Liebowitz, 2011). In 2012, the South Carolina Department of Revenue announced that 3.6 million tax returns from as far back as 1998 were hacked, and this cost $12 million to the agency (CBS News, 2012; Knell, 2012). In 2015, the Georgia Secretary of State announced that 6.2 million voters' sensitive information was breached. Meanwhile, before the breach, the Georgia State Secretary had rejected

help from the U.S. Department of Homeland Security to protect the election systems in the 2016 election (Devine & Griffin, 2018; Torres, 2015).

Besides the databases that contain citizen sensitive information, the state governments also have critical infrastructure systems such as aviation, transportation, dams, and ports. Ninety percent of critical infrastructure is privately owned; however, in order to prevent cyber incidents, state governments have become more responsible for coordinating security efforts. Without collaboration between the public and private sectors, the efforts to mitigate cyber incidents fall short (Spidalieri, 2015). The USA Patriot Act defines critical infrastructure as:

> systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (USA Patriot Act-107-56, 2001).

There are several ways to prevent or mitigate the impact of cyberattacks for state governments. Increasing funding for cybersecurity, better training of the state officials, and public-private partnerships for a multi stakeholder approach are some of the most discussed strategies in the scholarship (Goodyear et al., 2010; Harknett & Stever, 2009; Karakoç, 2017; Norris et al., 2019; Spidalieri, 2015).

States' legal involvement in addressing cyber risk traditionally focused more on privacy and consumer protection and dates back to at least 2003. In 2003, California passed the data privacy and breach notification law which requires that any company that has citizen information and falls victim to a security breach has to disclose the specifics about the security breach. Following California, 45 additional states also enacted data privacy and breach notification laws by 2010 (Glennon, 2012). More recently, this legal involvement expanded from data privacy and breach

notification laws that aim to protect consumers to laws that regulate the security practices of businesses. For instance, in 2011, both Maryland and Michigan launched their cybersecurity initiatives named the Maryland Commission on Cybersecurity Innovation and Excellence and the Michigan Cyber Initiative, respectively. Both commissions aim to protect states from cyber incidents and create a comprehensive response mechanism. In the following years, California, Idaho, North Dakota, Rhode Island, Virginia, and Texas also established their cybersecurity commissions, councils, or task forces to improve their cybersecurity posture (Spidalieri, 2015). As of 2022, cybersecurity has become one of the most prominent issues for the state legislators and governors. For instance, National Governors Associations (NGA) stated that governors increasingly acknowledge their role in cybersecurity resilience to protect "critical business and continuity of government, homeland security and workforce development" (National Governors Association, 2020).

While states have been developing cybersecurity planning documents and making cybersecurity-related policies, there is not a systematic analysis that examines the correspondence between these documents and policies. Thus, whether states take advantage of their planning documents in crafting cybersecurity policies remains a puzzle. The next section describes the purpose of this research in tackling with the research puzzle.

1.2 Purpose of the Research

This research examines state cybersecurity planning documents as of December 2021 and cybersecurity-related policies passed between 2015 and 2021 legislative sessions. The research has four main goals; (1) exploring the key areas of cybersecurity planning documents adopted by state governments as of December

2021, (2) examining in what ways cybersecurity planning documents of states incorporate the best practices, (3) exploring the key areas of the cybersecurity-related policies in states that have high cyberattack figures, and (4) analyzing the ways in which cybersecurity-related policies correspond to cybersecurity planning documents.

First, each state has different cybersecurity planning characteristics. This research aims to explore the variations in American state governments' cybersecurity planning. A text analysis reveals the common themes and patterns of the state governments' cybersecurity planning documents. Furthermore, the research analyzes the common and differential features of cybersecurity planning documents for each state.

Second, the states differ in the ways they incorporate the best practices into their planning documents. This dissertation defines best practices based on the 2018 NIST Cybersecurity Framework and recommendations of the scholarship. With the Best Practices Framework, the research analyzes how states' cybersecurity planning documents incorporate the suggested practices by the NIST and academic literature.

Third, this dissertation explores states' cybersecurity-related policies passed from 2015 to 2021 and the issues involved in them. It examines cybersecurity-related legislative policies of a sample of states with high cyber-attack figures. This investigation creates a cybersecurity-related policy inventory for these sample states and analyze the variation in components of cybersecurity-related policies amongst the sample states.

Last, the policy inventory enables an analysis of the extent to which the policies correspond to the state cybersecurity planning documents as of December 2021. In doing so, the findings of this project provides a means to measure the

correspondences between cybersecurity planning documents and cybersecurity-related policies. Thus, it will help policy makers and cybersecurity planners to bridge any potential gaps. In addition, the results will help cybersecurity planners and policy makers to plan, implement, and manage cybersecurity in state government agencies, and also to create cybersecurity planning documents that follow the best practices.

1.3 Cybersecurity Terminology Discussion

At the beginning of the twenty-first century, cybersecurity was being accepted under the terms "computer security" and "information security" because most of the scholars were accepting that cyberspace can only be protected with technical solutions. However, after 2014, the use of the terms "cybersecurity" or "cyber security" started to become increasingly popular (Schatz et al., 2017). As shown in Figure 1.1, google search of the terms "cybersecurity" and "cyber security" have dramatically increased after 2014. The only peak before 2014 is because of Obama's speech about the importance of cybersecurity for the nation in 2009.

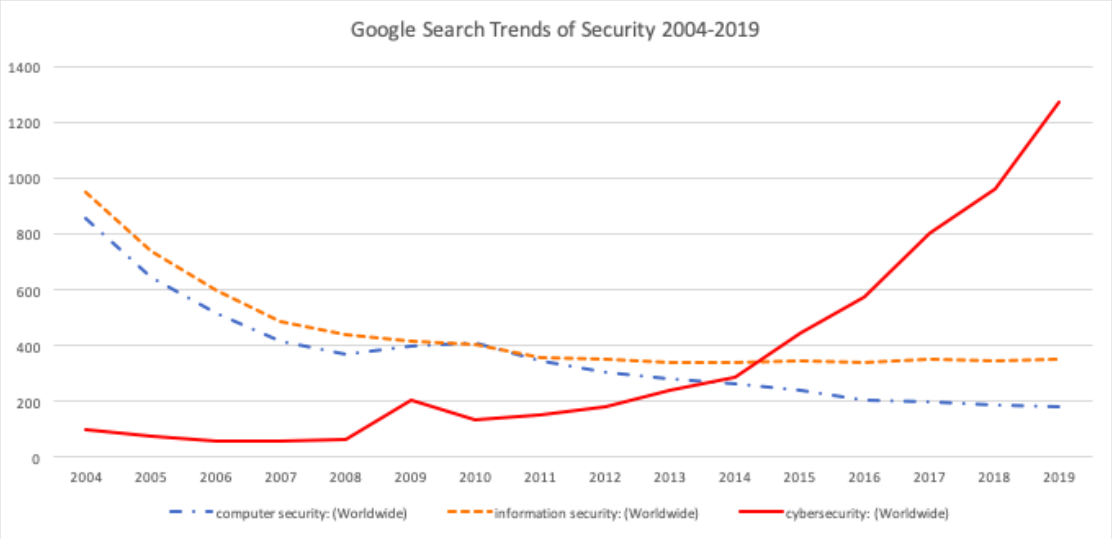

Figure 1.1 Google Trends of Security 2004-2019. Note: The cybersecurity search is done with both “cybersecurity” and “cyber security” terms.

Scholars have not agreed with how to write the term. Some scholars use the term as "cyber security" (Bayuk et al., 2012; von Solms & van Niekerk, 2013), whereas others use it as a single word, "cybersecurity" (Andreasson, 2012; Davis et al., 2016; Garcia et al., 2017), or "cyber-security" (Cavelty, 2015; Clark & Hakim, 2017). This variety shows the recency of the issue and the lack of standardization in academic and practical usage of the term. This dissertation uses the single word version, “cybersecurity”, of the term because “it has become the norm in Washington D.C. in government circles – including the White House, Washington Post, and other news outlets. Even foreign conventions are starting to combine cyber words" (Lohrmann, 2012). More importantly, the term cybersecurity is used as a single word in the documents released by NIST. For this reason, this dissertation focuses more on the meaning and definition of the term “cybersecurity” instead of the etymological and spelling discussions of it.

In the literature, there is also no single definition of cybersecurity that most scholars agree upon. As Schatz et al. (2017) stated, there is a "... lack of a uniformly accepted definition of cyber security..." in the private sector use (Barzilay, 2013; Stubley, 2013; Walls et al., 2013), the public sector use (Falessi el al., 2012; Government of Montenegro, 2013; Wamala, 2011), and in scholarly work (Baylon, 2014; Giles & Hagestad, 2013). In another research conducted on 19 countries' national cybersecurity strategies, the lack of a common or harmonized cybersecurity definition was stressed (Luiijf and Besseling, 2013). The most obvious explanation for the variety of cybersecurity definitions comes from the nature of the issue. Because cyberspace is a very dynamic and evolving place, the definitions of cybersecurity also evolve and grow based on increasing dimensions it acquires.

The word "cyberspace" first appeared in a science fiction novel, Neuromancer (1984), by William Gibson. Ever since, the term has been used by a wide range of people from government officials to businesspeople to academics. From a hypothetical and utopic use, the term has evolved into a practical and specific concept. For instance, in 2010, Public Safety Canada defined cyberspace as "the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where... people are linked together to exchange ideas, services and friendship" (quoted from Craigen et al., 2014, p. 14).

In attempts to secure cyberspace, some scholars in the burgeoning period of the cybersecurity literature accepted only the technical and engineering solutions (Alibasic et al., 2016; von Solms & van Niekerk, 2013). Other scholars oppose the idea of a purely technical approach to cybersecurity (Craigen et al., 2014; Shoemaker et al., 2019). The underlying reason for their opposition to a purely technical definition is the

organizational, economic, social, political, and other human dimensions that are inseparably linked to cybersecurity efforts (Goodall et al., 2009; Buckland et al., 2015; Deibert, 2012).

To broaden the definition of cybersecurity, Craigen and his colleagues (2014) identified "five dominant themes of cybersecurity: i) technological solutions; ii) events; iii) strategies, processes, and methods; iv) human engagement; and v) referent objects (of security)" (p. 15). These different dominant themes demonstrate the need for an interdisciplinary perspective and a comprehensive conceptualization. Through content analysis on extant literature, they problematized the subjective and uninformative use of the term. To overcome these problems, they suggested that deconstruction of the term cybersecurity is helpful to provide a more holistic, inclusive, and practical definition and meaning for organizations. Finally, they proposed a new definition of cybersecurity:

> Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights (Craigen et al., 2014, p. 17).

Schatz and his colleagues (2017) cited this definition as one of the valid definitions of cybersecurity used in the scholarly literature. Nevertheless, they proposed to synthesize all of the definitions in the literature to create a more systematic, comprehensive, and inclusive definition. To do this, they conducted a semi-systematic literature review and analyzed the major sources defining the cybersecurity term. After that, they conducted various lexical and semantic analysis techniques to understand the scope and context of the definitions. Finally, they propose a new, improved, and inclusive definition of the term based on this analysis. They define cybersecurity as:

> The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyberspace. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users (Schatz et al., 2017, p. 66).

Although these definitions of the cybersecurity term are comprehensive, they might be vague for cybersecurity planners and policy makers. Because cybersecurity concerns everyone in an organization, and not just the IT experts (Williams, 2008; Wylder, 2003), it should be framed in a way that serves the security needs of people as well as the state (Liaropoulos, 2015). In order to have an accessible definition of the term, there is a need for a multidimensional and practical conceptualization. Scholars cited above have debated the definition of cybersecurity not in the context of the State government policy-making or planning, but more broadly. Thus, the planning aspect of the term is neglected. Schatz et al. (2017)'s definition considers the policy dimensions; however, it only includes the national and organizational levels of the concept. Likewise, Craigen et al. (2014) conceptualize cybersecurity in relation to de jure and de facto property rights; however, they also exclude the State level planning and policy aspects. Including planning and policy perspectives into the term is crucial for making it more holistic, inclusive, and practical for state-level cybersecurity planning and policymaking.

The next section discusses the significance of this research for academics, public administrators, and policy makers.

1.4 Significance of the Research

> Every American depends — directly or indirectly — on our system of information networks. They are increasingly the backbone of our economy and our infrastructure; our national security and our personal

> well-being … As President, I'll make cyber security the top priority that it should be in the 21st century (Barack Obama quoted from Jose, 2008).

A year after the 2008 Summit on Confronting New Threats, President Barack Obama announced the strategy of the US government against cyberattacks. On May 29 in 2009, he stated that transparency, accountability, and new ways to participate in democracy would not be possible without America's digital infrastructure. He also noted that the revolutions in communication and information technology had given birth to a virtual world called "cyberspace" (Obama, 2009).

Obama detailed the threats that make the cyberspace vulnerable. For instance, he gives an example that cyber thieves stole millions of dollars in just 30 mins by using stolen credit card information. In addition to economic effects, Obama pointed out, because we bank on computer networks to deliver our oil and gas, our power, and our water; for public transportation and air traffic control, this is also a public safety and national security issue. As a result, it is clear that cyber threats are the most serious economic and national security challenges (Obama, 2009).

Many years after Obama's speech, it is even more clear that most American's lives depend increasingly on the utilization of cyberspace technologies. Organizations in all sectors of the economy also increasingly depend on cyberspace technologies for virtually all aspects of their operations and services. Some of the cybersecurity policy scholars believe that government and business reliance on the Internet will continue to increase (Spidalieri, 2015). As Obama noted, the local networks in schools, hospitals, businesses, and the power grids are simple examples of this interconnectivity. Individuals across the globe increasingly rely on the Internet, which makes the current global population more interconnected than at any time in human history to pay bills,

to make financial transactions, to shop, to file taxes, to organize virtual meetings, to take classes, and to socialize (Rainie & Wellman, 2012).[1]

Increased interconnectivity poses a challenge for state governments as well. It has been clear that the United States' state governments have a problem with securing cyberspace. For instance, in recent years, US states have faced an increasing number of cyber threats such as data breaches, ransomware attacks, political manipulation, and tax refund frauds (Deloitte and National Association of State Chief Information Officers (NASCIO), 2012, 2014, 2016, 2018). As illustrated in the first section of this chapter, for example, Illinois, Georgia, South Carolina, Texas, and Virginia have lost a significant amount of data on voter, patients, and tax records since 2009. These states paid millions of dollars to address these data breaches (Bruer & Perez, 2016; CBS News, 2012; Devine & Griffin, 2018; Goodin, 2009; Kerschberg, 2011).

States have responded to these attacks in various ways. For instance, California Department of Technology set up the California Cybersecurity Task Force in order to enhance cyber preparedness and response in 2013 (Wood, 2013). Similarly, in 2019, the Department of Management Services of Florida established the Florida Cybersecurity Task Force that is in charge of analyzing the current cyber attacks and improving the state's cybersecurity posture (Department of Management Services of Florida, n.d.).

States have also formed partnerships with businesses and other institutions. For instance, Georgia Technology Authority (GTA) created partnerships with several university institutions such as the Augusta University Cyber Institute, University

---

[1] This individual connectivity skyrocketed because of COVID-19 pandemic.

System of Georgia, the Technical College System of Georgia. Furthermore, they cooperated with public institutions such as the Georgia National Guard, Georgia Bureau of Investigation (GBI) and federal agencies. Similarly, North Carolina National Guard also work in a "wide range of state, national and international industries and corporations" (Devivo, 2014, para.6). Lastly, they allied with the private corporations to promote cybersecurity workforce across sectors (U.S. Department of Homeland Security and National Association of State Chief Information Officers (NASCIO), 2017).

Many states have issued cybersecurity planning documents and passed relevant policies to improve cybersecurity atmosphere. For example, in 2017, State of New Jersey's information and technology leaders issued cyber incident response policy and plan, organized cybersecurity roles and responsibilities, and required state agencies to adopt IT policies (U.S. Department of Homeland Security and NASCIO, 2017).

Despite all these efforts from state governments, some scholars claim that state governments are getting worse at protecting cyberspace (Shoemaker, Kohnke, & Sigler, 2019). Furthermore, state cybersecurity planning documents and policies have not been systematically analyzed yet. This research is significant because it analyzes the characteristics of cybersecurity planning documents and cybersecurity-related policies. In addition, it is one of the first academic research that examines the correspondence between the planning documents and the policies. In doing so, it shows whether there is a gap between states' planning and policy making as attempts to protect their cyberspace.

The next section describes the four main research questions that guide this dissertation.

1.5 Research Questions

Four interrelated research questions guide this research.

RQ1: What are the characteristics of cybersecurity planning documents of 50 states adopted as of December 2021?

This research, first, explores the nature of state governments' cybersecurity planning documents and analyzes the major commonalities and differences. The research focuses on the latest cybersecurity planning document adopted as of December 2021. Chapter 3 explains what constitutes a cybersecurity planning document and discusses the characteristics.

RQ2: In what ways do cybersecurity planning documents of 50 states incorporate the best practices defined by the scholarship and the 2018 NIST Cybersecurity Framework?

This research examines 50 states' cybersecurity planning documents based on the criteria proposed by the literature (leadership, national security, partnerships, funding, training, better equipment, developing awareness and cybersecurity culture, and coordination and communication) and 2018 NIST Cybersecurity Framework standards. The scholarly criteria and the NIST Framework are collectively referred as the Best Practices Framework (BPF). The NIST Framework is commonly used to evaluate cybersecurity planning documents in different sectors. Chapter 3 further justifies the use of NIST Cybersecurity Framework standards in this research and discusses the criteria proposed by the literature. By investigating this question, this research explores the convergences and divergences in cybersecurity planning documents across states based on the Best Practices Framework.

RQ3: In what ways do cybersecurity policies adopted between 2015 and 2021 legislative sessions of states with high cyberattack figures incorporate

the best practices as defined by the scholarly criteria and the 2018 NIST Cybersecurity Framework?

This research creates a cybersecurity-related policy inventory for the sample states and applies the Best Practices Framework to state cybersecurity policies. The policies are found with the help of the National Conference of State Legislatures' (NCSL) list of cybersecurity legislations for the legislative years since 2015. Furthermore, the NexisUni database is used to complement the compilation of policies listed in the NCSL's website. NexisUni allows a full text search of State Bills. The following keywords are used to find cybersecurity-related policies in the database: "cyber security", "cybersecurity", "cyber-security", "data-breach", "network security", "hacking", "information security", "data security", and "data privacy".

RQ4: In what ways do the cybersecurity policies in the sample states correspond to their latest cybersecurity planning documents as of the end of the 2021 legislative session?

In the last part, this research analyzes if and to what extend the policies passed from 2015 to 2021 correspond to the latest state cybersecurity planning documents as of the end of the 2021. The correspondence is searched between the adoption of the BPF by the planning documents and policies. This way, the research demonstrates (1) whether cybersecurity planning documents were implemented and (2) whether the policies were shaped in accordance with the planning documents, or not.

To investigate these research questions, this study benefits from the literature on national-state-local level cybersecurity, strategic planning, information technology and homeland security, cybersecurity planning, state-level policy making, and cybersecurity policies.

The next section outlines the organization of this dissertation.

1.6 Organization of the Research

The dissertation is divided into seven chapters: (1) Introduction, (2) Literature Review, (3) Research Design and Methodology, (4) An Analysis of 50 States' Cybersecurity Planning Documents, (5) Incorporation of NIST Cybersecurity Standards, (6) An Analysis of Cybersecurity-related Policies of Sample States, and (7) Conclusion.

Chapter 2 is a literature review of the four primary areas of scholarship related to this dissertation. First, it discusses the terminology of cybersecurity and reveals the lack of planning perspective in the existing cybersecurity definitions. Second, it focuses on the importance of national-level cybersecurity, and reviews the scholarship on the determinants of successful national cybersecurity including cybersecurity capacity, critical infrastructure and planning, developing a cybersecurity culture, and decentralization of cybersecurity management. Third, it reviews the literature on local and state government cybersecurity. It first focused on the barriers that local governments have been facing and some proposals to strengthen the practices of cybersecurity at the local level. It then considers the state government cybersecurity literature with a specific focus on (1) the barriers that state governments have been facing, (2) some proposals to strengthen the practices of cybersecurity, and (3) state-level cybersecurity planning.

Chapter 3 describes the key concepts and methodology for this research. The chapter consists of five parts: (1) Concepts, (2) Research Questions and Methodology (3) Data Collection, (4) Data Analysis, and (5) Data Limitations. The first part of this chapter provides definitions of key concepts that are used in this dissertation. The

NIST Cybersecurity Framework standards and scholarly recommended themes, which are used to examine the states' cybersecurity planning documents and policies, are also discussed and explained in the first part of Chapter 3. The second part discusses the research questions and their importance in addition to methodology. The third part explains how the cybersecurity planning documents and policies are collected. The fourth part discusses methods for data analysis and interpretation as well as method justification. The last part discusses the research limitations.

Chapter 4 addresses the results of the analysis with regard to first two research questions. First, it explores the nature of state cybersecurity planning as of December 2021 through an analysis of the characteristics of latest cybersecurity planning documents of 50 states. This analysis of planning documents helps to lay out the landscape of state level cybersecurity planning. Second, it examines the extent to which state plans align with best practices defined by scholarly literature. This is done through a review of the extent and ways in which states' cybersecurity planning documents incorporate the best practices defined by the scholarly literature.

Chapter 5 addresses the latter part of the second research question. It analyzes the extent to which cybersecurity planning documents of states incorporate the best practices as defined by the 2018 NIST Cybersecurity Framework. This chapter first defines each NIST function and then describes how these functions are coded in the analysis of state planning documents. The chapter reports the results of a text analysis of the incorporation of NIST Cybersecurity Framework functions within the cybersecurity planning documents of the states. The analysis continues with an examination of cross-state variations in terms of incorporation of NIST Cybersecurity

Framework functions. Finally, it discusses the most common best practices of model states.

Chapter 6 addresses the third and fourth research questions. It, first, explores the landscape of sample states' cybersecurity-related policies that are enacted from 2015 to 2021. Second, it analyzes the level of incorporation of the Best Practices Framework, which combines the scholarly themes and the NIST Cybersecurity Framework functions, for each sample state. Third, it examines the correspondence between the planning documents and cybersecurity-related policies of sample states. For each sample state, the correspondence analysis reveals whether planning documents' alignment with the Best Practices Framework matches with cybersecurity-related policies' alignment with the Best Practices Framework.

Chapter 7, which is the concluding chapter, summarizes the findings of this dissertation with regard to the research questions. It discusses the research significance and the implications of the findings for academics as well as practitioners. It also reviews the overall research contributions to the state-level cybersecurity planning and policy scholarship and discusses the future research agenda that is built on this dissertation project.

Chapter 2

LITERATURE REVIEW

Cybersecurity planning and policy making have been considered as one of the most important tools for state governments to enhance their cybersecurity posture (Caruson et al., 2012; Coulson et al., 2018; Dawson & Desouza, 2015). Because of the federalism structure in the US, the role and responsibility of state governments in addressing cybersecurity issues are rarely shaped with regards to local and national governments. Thus, this chapter reviews the literature on cybersecurity planning and policy making at the local, state, and federal levels. The major focus of the scholarship is on challenges of cybersecurity planning and policy making and proposals to address these challenges (Caruson et al., 2012; Deloitte and National Association of State Chief Information Officers (NASCIO), 2012, 2014, 2016, 2018; Lewis et al., 2016; Norris et al., 2018, 2020). The next section reviews the literature on the importance of cybersecurity planning and policymaking.

2.1 Importance of Cybersecurity Planning and Policymaking

Planning is not a brand-new term for public administrators and policy makers. In 1937, Luther Gulick published one of the preliminary articles of the public administration field titled “Notes on the Theory of Organization”. To point out major elements of an organized executive function, Gulick made up a word: POSDCORB (Planning, Organizing, Staffing, Directing, Coordinating, Reporting, and Budgeting) which is still widely used in the field of management and public administration that

reflects the classic view of the organizational theory. His acronym starts with "P" which represents "planning".

Kemp (2010) also notes that planning is the first step of preparedness for emergency response. He states that analyzing "organizational and departmental weaknesses and shortcomings" (p. 10) is essential for disaster preparedness. In addition, Caruson et al. (2012) claim that "disaster preparedness is contingent upon good planning".

An organization's cybersecurity planning is critical to protect its data (Coulson et al., 2018; Khouzani et al., 2016; Richardson et al., 2020). According to the Privacy Rights Clearinghouse (2018), attacks factored into an organization's cybersecurity planning only constitute 29% of total attacks. Besides the classic technology-based attacks, state-level planning should address the physical and human attack domain as they constitute 71% of annual data losses (Shoemaker, 2019).

Scholars and private companies have suggested improving state-level cybersecurity planning to make it more comprehensive. The plans should be more precise, and strategies and goals should be clearly identified for the planning to be effective. For this purpose, some of the scholars proposed holistic cybersecurity implementation frameworks (Atoum et al., 2014; Garcia et al., 2017) and planning guides (Federal Communications Commission, 2012) for private companies, government organizations, and national governments. The common purposes of these frameworks and guides are (1) detecting of threats and mitigate risks related to information systems and infrastructures, (2) enabling decision-makers to take necessary actions once needed, and (3) including different stakeholders such as private

companies, government agencies, and citizens to implement effective security solutions (Atoum et al., 2014).

Regarding state level planning trends, U.S. Department of Homeland Security and NASCIO collaboratively published a report that identifies three major strategy and planning trends in 2017. Firstly, locating the authority to set cybersecurity strategy by laws and policies is common because of the need for leadership. Secondly, putting formal mechanisms in place to evolve and address changing conditions under the guidance of strategic plans is also common because it is the most efficient way decision-makers adjust key initiatives. Lastly, enabling collaborations in the development of strategy between the public and private sectors is a common trend because cybersecurity is an interconnected issue (U.S. Department of Homeland Security and National Association of State Chief Information Officers (NASCIO), 2017).

Strategic planning method is the way to apply these three major strategies and planning trends (Bryson et al., 2010). It has been a frequently used method in U.S. government agencies and nonprofit organizations. It can be also successfully used by public agencies and departments (Bryson, 2011; Steiss, 2003), general purpose governments like states (Hendrick, 2003; Kissler et al., 1998), and purpose-driven organizations in the public sector for emergency services (Choi, 2008; Nelson & French, 2002).

Strategic planning is a systematic process for managing organizations' future directions and their relationships with their environment (Berry & Wechsler, 1995). There is a large number of studies that proof its applicability at state level (Berry, 1994; Berry & Wechsler, 1995; Bryson et al., 2010; Kissler et al., 1998). This

approach improves decision making; enhances organizational effectiveness, responsiveness, and resilience; promote strategic thinking, acting, and learning; and improves organizational legitimacy (Berry & Wechsler, 1995; Bryson, 2010). As the cybersecurity paradigm becomes more sophisticated (Deloitte and National Association of State Chief Information Officers (NASCIO), 2012, 2014, 2016, 2018; McQuade, 2006; Van Dine et al., 2017), cybersecurity and IT strategic planning is vital for state governments.

The lack of planning in cybersecurity demonstrates the underdevelopment of the literature on state-level cybersecurity planning. In other words, because cybersecurity planning documents are understudied, leading cybersecurity strategic frameworks and practices are still deficient in planning perspectives. This dissertation project contributes to the state-level cybersecurity scholarship by focusing on the planning aspect of cybersecurity. Most of the scholarship on cybersecurity comes from national-level studies that concern the federal government policies as well as international aspects. Before reviewing the literature on cybersecurity at the national level, the next section briefly addresses the issue of cybersecurity from the vantage point of U.S. federalism. Understanding the U.S. federal system is critical to explore the division of cybersecurity responsibilities between the federal government and state governments.

2.2 U.S. Federalism and Cybersecurity

The U.S. Constitution creates a division of responsibilities between the states and the federal government. Some of the provisions in the Constitution expand the federal government's power whereas others protect states' right. For instance, "each state retains its sovereignty, freedom, and independence, and every power,

jurisdiction, and right, which is not... expressly delegated to the United States, in Congress assembled" (U.S. Const. art. II). However, the federal government triumphs in cases of conflicting state actions. This law is known as 'The Supremacy Clause of the Constitution' (U.S. Const. art. VI, para. 2).

The current cyber policies presume a significant authority of the federal government in creating and influencing cybersecurity policies in the country. There are three main reasons for the federal government's significant authority. The first is the aforementioned Supremacy Clause (Rosner, 2017). In addressing cyber challenges, state governments are aware that any of their investments can be potentially usurped with a new federal legislation. While the clause applies to all policy areas, it can be paralyzing in the issue of cybersecurity due to lack of clear boundaries. The second reason is the historically gradual evolution of cybersecurity policies. Because cybersecurity firstly acknowledged as a national security issue against international threats, the federal government presumed primary responsibility (Glennon, 2012). Therefore, laws prohibiting fraud by wire, radio, or television, and unsolicited commercial emails (CAN-SPAM Act-108-187, 2003), and the Computer Fraud and Abuse Act are all drafted at the federal level. The third reason is the Commerce Clause, which attributes the power to regulate interstate commerce to Congress (U.S. Const. art. I, sec. 8, cla. 3). Internet allows of interstate commerce and thus cyber activities inherently traverses state lines. Thus, especially, economic activities in the cyber space arguably invokes the commerce clause and the federal authorities assume the power to regulate.

Because cyber-attacks are getting more localized, sophisticated, and individualistic, broad federal policies and precautions are not enough to protect

citizens and critical infrastructure. This shift led states and local governments to notice that they are the new targets of cyber attacks (Karakoç, 2017). For instance, government agencies have lost more than 94 million citizens' records from 2009 to 2013 due to cyber attacks directly targeting state and local governments. The loss represents a cost of $194 for each case (Center for Digital Government, 2014). Because of this void, states have step into the cybersecurity planning and policy making area. As Ostrom (1991) advocates for poly-centric approaches to the governance problems, the state governments have started to share the cybersecurity responsibilities. Thus, the understanding of Federalism as "not just a form of government; (but) a method for solving problems, a way of life" is crucial for cybersecurity management (Ostrom, 1991, p. 247). With the poly-centric problem solution method, states have adopted various cybersecurity policies and plans. States' legal involvement in cybersecurity planning and policy making area begins with the California data privacy and breach notification law of 2003 (Glennon, 2012). Ever since 2003, all States adopted varying degrees of cybersecurity planning and legislations.

Political cultures of states have affected these cybersecurity plans and legislations. To identify major political cultures in the United States, Elazar (1991) created three ideal types based on ethnic and religious groups' migration and settlement patterns. These three dominant political subcultures in the American states are moralistic, individualistic, and traditionalistic cultures. The moralistic culture refers to progressive communitarian values exist in New England, the Northern Plains, and West Coast area. This culture is a product of Puritan and Scandinavian immigrants settling in these areas. The individualist culture refers to a minimalistic approach to

the government and priority of marketplace in arranging social affairs. Immigrants from the non-Puritan England and the interior Northern European countries created this culture in the middle and western U.S. Lastly, the traditionalistic culture refers to protecting the hierarchy and elite based status quo in the government. The southern states, which relied on the agricultural system of slavery under the control of large landowners, carry the traditionalistic culture (Elazar, 1991; Marquis & Battilana, 2009).

Elazar (1994) integrated two other dimensions of location in his theory in addition to space: time and culture. He argues that understanding the three-dimensional location (space, time, and culture) is the beginning of understanding a government and its political system. According to Elazar, "location in time and culture structure to no less a degree that does location in space, and that their structure can be understood to be systematic or at least sufficient systematic to be mapped." Elazar explains this three-dimensional location with generational change. The American political landscape is formed by the collective evolution of space, time, and culture. Thus, the geographical and temporal aspects of the location determine the rhythm of the generations. Each of the four generations in the US, according to Elazar, face a new frontier shaped by the geo-historical conditions. The first generation faced rural-land frontier, the second faced urban-industrial frontier, the third generation faced metropolitan-technological frontier, and the current generation is facing the ongoing rurban-cybernetic frontier. This frontier that the last generation lives in is marked by the developments in the cyber space and the intertwined rural and urban areas. This research considers the implications of this frontier when analyzing the variation in state level cybersecurity planning and policy making. The next three sections review

the literature on cybersecurity at the (1) national level, (2) local level, and (3) state level.

2.3 National-level Cybersecurity

Because the state-level cybersecurity scholarship benefits from the national-level cybersecurity literature, this dissertation briefly reviews the latter body of literature as well. This section specifically focuses on the importance of national-level cybersecurity, and reviews the scholarship on the determinants of successful national cybersecurity. The determinants include cybersecurity capacity, critical infrastructure and planning, developing a cybersecurity culture, and decentralization of cybersecurity management.

Although the majority of scholars approach national-level cybersecurity as a recent problem (Alexander et al., 2020; Asllani et al., 2013; Atoum et al., 2014; Ghernouti-Hélie, 2010; Schatz et al., 2017; Srinivas et al., 2019; Veiga, 2016), the 'cyber' issue is not new (Geers, 2009; Warner, 2012). Warner (2012) finds that computer systems were susceptible to leaks since the 1960s. They also were sensitive to attacks and data breaches since the 1970s. Thus, cybersecurity has been a critical national security issue for more than a half-century.

Nevertheless, the significance of cyber threats as serious economic and national security challenges has increased dramatically in the last decade. Almost a year later from the Summit on Confronting New Threats, Barack Obama announced the strategy of the US government against cyberattacks on May 29 in 2009. He stated that transparency, accountability, and new ways to participate in democracy would not be possible without America's digital infrastructure. He also noted that the revolutions in communication and information technology had created a virtual world called

cyberspace. As Obama mentioned, because we depend on computer networks, this is also a public safety and national security issue (Obama, 2009). Even though the private sector runs most of the critical infrastructures, they lease these services to the government as well as to commercial entities (Geers, 2009).

To develop successful national-level cybersecurity mechanisms, the first attempt should focus on clarifying what cybersecurity is, as the previous section mentioned. Cavelty (2015) states that for effective national and supranational cybersecurity policies, we first need to understand what constitutes cybersecurity and a common definition of the term. Even though national-level cybersecurity scholarship is not a mature field yet, the literature is steadily growing.

Another important requirement of national-level cybersecurity is to build cybersecurity capacity. There are many determinants of cybersecurity capacity including the wealth of nations, the size of nations, the scale of Internet use, and the centrality of Internet use (Dutton et al., 2019). Through a cross-national analysis on national cybersecurity capacity, Dutton et al. (2019) showed capacity building covers "the domains of policy and strategy; cultural and societal norms and behavior; cybersecurity education training and skills; legal and regulatory frameworks; standards, organizational arrangements, and technologies" (p. 281). The authors also found a strong negative relationship between a higher percentage of people online and end-user cybersecurity problems. In addition, the authors demonstrated that the higher a nation's cybersecurity capacity the lower the end-user cybersecurity problems in that nation. Although this research links cybersecurity capacity and end-user experiences, it underemphasizes the planning aspect of capacity building.

The planning aspect of national-level cybersecurity is more highlighted in the scholarly debate on the protection of critical national infrastructure. Because international cyber attacks are more threatening to countries than ever before making investment plans for network security, incident response, technical training, and international collaboration is vital. To mitigate security threats and protect national critical infrastructure, Geers (2009) suggests that national security planners at least should focus on three major questions (1) how much the national critical infrastructure is dependent on IT, (2) the degree of IT connected to the Internet, and (3) the worst-case scenario against this infrastructure in terms of cybersecurity. Based on these three national characteristics, there is a need for a comprehensive national cybersecurity policy; however, this topic is beyond the scope of this dissertation.

Beside the scholarship that focuses on national cybersecurity capacity building and developing policy frameworks, there are other scholars who emphasize the human factor and creating a cybersecurity culture to implement a successful national cybersecurity strategy (Ghernouti-Hélie, 2010; Liaropoulos, 2015; Veiga, 2016; Whitmer, 2007). The major reason for stressing the human factor is that the human aspect remains the weakest link in relation to cybersecurity (Ghernouti-Hélie, 2010; Huang & Pearlson, 2019; Veiga, 2016). It is crucial to strengthen the human factors in order to support successful cybersecurity strategies. Also, the cybersecurity strategy needs to be specific to the values related to different organizations, individuals, or states belonging to the same region (Ghernouti-Hélie, 2010). For this reason, they focus more on defining the cybersecurity culture and measuring the level of it. For instance, Veiga (2016) defined the cybersecurity culture at international, national, organizational, and individual levels. Through her "Cybersecurity culture research

methodology (CSeCRM)", she developed a valid and reliable cybersecurity culture measuring instrument applicable to all of these four levels.

Because the national level cybersecurity is mostly enhanced through outsourcing and leasing; the organizational level cybersecurity awareness and culture are vital for national cybersecurity (Harknett and Stever, 2009). At the organizational level, a multiperspective definition of cybersecurity culture, which is shaped with organizational, national, and informational culture, was developed by Huang and Pearlson (2019). They define organizational cybersecurity culture as "the beliefs, values, and attitudes that drive employee behaviors to protect and defend the organization from cyber attacks" (Huang & Pearlson, 2019, p. 6399).

Analyzing employee behaviors, as an important component of organizational cybersecurity culture, is also applied to the public sector. Employee behavior, in the US Government, is empirically examined with regards to similarities and differences in cybersecurity perception and behavior between cybersecurity experts and non-experts (Theofanos et. al., 2017). The authors found that US Government cybersecurity experts are proactive in their online security practices whereas non-experts are not. Experts generally believe they have a plan to mitigate or recover from potential cybersecurity problems; however, non-experts do not have plans in advance to protect themselves or to overcome potential cybersecurity problems. Thus, the cybersecurity culture and awareness can be at different levels amongst the same sector employees based on their expertise area. This confirms the need for an individual level analysis built into the cybersecurity culture framework (Veiga 2016).

Lastly, even though it requires a change in laws, some scholars have suggested decentralizing cybersecurity. Reorganization of responsibility and governance of

cybersecurity is necessary rather than centralizing the federal government for cybersecurity. Harknett and Stever (2009) propose a cybersecurity triad that rests on three legs of core institutional and process relationships including intergovernmental, public-private, and general population. The first is defined as relationships both between federal agencies, and between federal, state, and local governments. The second, public-private leg, is defined in terms of government to private business and critical infrastructure relations. The third leg is integrating the general population into this framework. A resilient model is possible with a balanced triad of intergovernmental relations, private corporate involvement, and active cyber citizenship that can manage the complexity of the current cybersecurity environment.

In line with the decentralization of the cybersecurity research agenda, this project focuses on the state-level cybersecurity plans and cybersecurity policies. Before reviewing state-level cybersecurity literature, the next section focuses on the local-level cybersecurity scholarship because their role contributes to the complexity of the responsibilities of the states.

2.4 Local-level Cybersecurity

Local governments increasingly provide critical services and online transactions. Also, they use "share(d) data with state and federal government programs" (Newcombe, 2011, p. 50). However, there are few scholarly works focused on local government cybersecurity. Because of the lack of the scholarly literature at the local level, scholars mostly benefited from publicly available studies and reports from consulting firms, centers and institutions, professional associations, private IT and cybersecurity companies, and professional organizations (Norris et al., 2017, 2018, 2019, 2020). Furthermore, in this burgeoning period, scholars mostly focus on

barriers and challenges for the protection of cyberspace (Caruson et al. 2012; (Karakoç, 2017; MacManus et al., 2013; Norris et al., 2019; Pfeiffer, 2015; Wolff and Lehr, 2018) and variations in the perspectives of local officials (Caruson et al., 2012; Ponemon Institute, 2015; Reddick, 2010; MacManus et al., 2013). The first, identifying the barriers that local governments face in managing cybersecurity, is significant because these barriers prevent developing comprehensive cybersecurity planning documents at the local level (Caruson et al., 2012). The second, variations in the perspectives of local officials based on agency size and the type of position held can deter critical team-building and networking efforts (Caruson et al., 2012).

This section reviews the literature on local government cybersecurity with a specific focus on the barriers that local governments have been facing and some proposals to strengthen the practices of cybersecurity at the local level.

2.4.1 Barriers in Local-level Cybersecurity

There are several survey research that reveal the most important barriers for the protection of cyberspace at the local level. The findings of these research mostly overlap (Norris 2019). The common barriers that were found in these research include (1) insufficient budget, (2) lack of expertise, (3) lack of adequately trained personnel, and (4) (un)awareness of being under attack (Caruson et al., 2012; Karakoç, 2017; MacManus et al., 2013; Newcombe, 2011; Norris et al., 2019; Pfeiffer, 2015; Ponemon Institute, 2009; Reddick, 2010; Wolff and Lehr, 2018).

2.4.1.1 Insufficient Budget

Insufficient funding to overcome cybersecurity issues is not a brand-new problem at local, state and federal organizations. However, a research report titled

"State of Cybersecurity in Local, State & Federal Government" published by Ponemon Institute (2015) demonstrates that budgetary issues constitute a much more important concern at the local and state level compared to the federal level (see Figure 2.1). Local government officials report that a lack of insufficient budget is always an issue to manage cybersecurity in their agencies (Ponemon Institute, 2015; Norris, 2017, 2018, 2019; Caruson et al., 2012). It is also very important to know how to efficiently use the budget because it is limited (Lohrmann, 2017). Every single security update or exploit requires updated technology and more money because the fields of technology and security progress incredibly fast. Because the budget is limited, it's not effortless to successfully deploy and maintain all the required components for a secure cyberspace in an ordinary local government agency.

Furthermore, the budget is the core of other barriers local governments face in protecting their cyberspace as well. For instance, lack of expertise and lack of training, which is be discussed as separate barriers below, mostly originate from the insufficient budget. Local governments are not able to pay competitive salaries to cybersecurity employees which causes a lack of expertise among the staff (Norris, 2019).

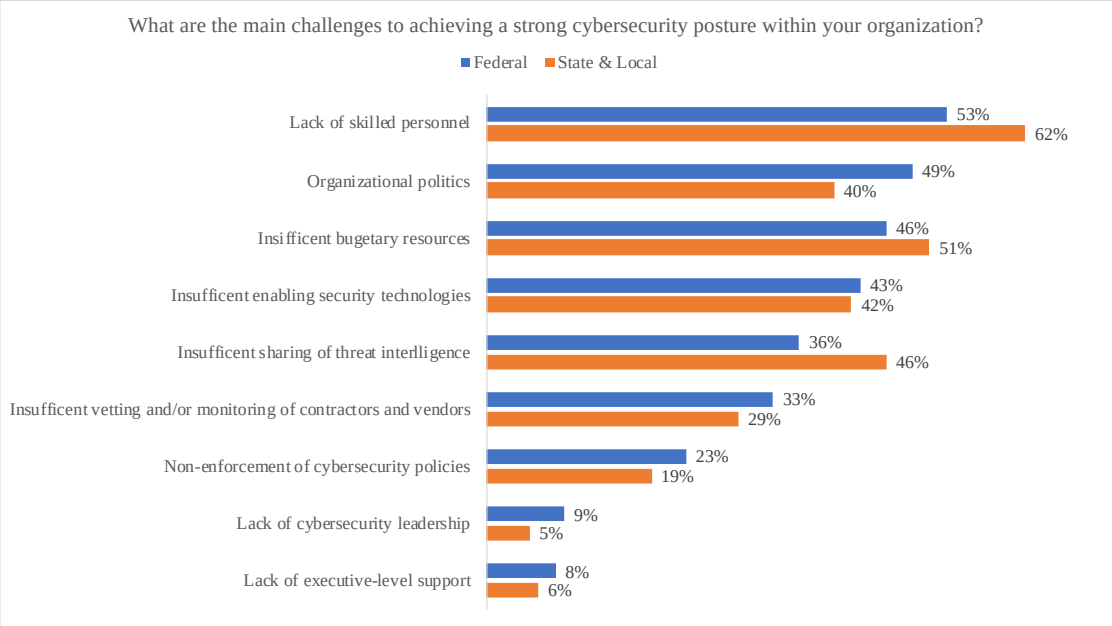

Figure 2.1 Main challenges to achieving a strong cybersecurity posture within Federal, State, and local government organizations (Ponemon Institute, 2015, p. 8).

2.4.1.2 Lack of Expertise

Organizations with more expertise and skilled personnel achieve better cybersecurity management. However, a lack of expertise is a major challenge, as shown in Figure 2.1, at the local (Caruson et al., 2012; Norris, 2019), state (Delliotte-NASCIO, 2010, 2012, 2014, 2016, 2018) and federal level (Ponemon Institute, 2015). According to the Ponemon Institute research report, 62 percent of state and local government officers state that a lack of skilled personnel is the major challenge for their agencies. This issue has always been a problem for local governments because of a limited budget and infrastructure. Local government agencies struggle to compete with the private sector because the private sector offers higher salaries to cybersecurity employees than the public sector (NASCIO, 2015; Stone, 2014).

In addition to the insufficient budget issue, the scarcity of cybersecurity professionals available to be employed by local governments also contributes to the problem. Although the cybersecurity job sector is dramatically growing, the supply of cybersecurity experts is very limited due to the few numbers of colleges offering dedicated cybersecurity programs and training. For instance, the first cybersecurity undergraduate program was launched at the University of Maryland as late as 2013 (Feiman, 2019).

2.4.1.3 Lack of Adequately Trained Personnel

Training and educating employees on up-to-date cybersecurity practices are crucial to mitigate and recognize sophisticated cyber threats. Verizon (2019) reports that 34% of cyberattacks involved internal actors such as employees and stakeholders in 2018.

Training is necessary for regular employees more than IT and cybersecurity professionals because there is a knowledge gap between IT professionals and other public administrators (Caruson et al., 2012). This gap is even wider at the local level than at the federal and state levels (Caruson et al., 2012; Ponemon Institute, 2015). It causes a vulnerability in terms of cybersecurity. Despite the significance of employee preparedness, a recent study demonstrated that "thirty percent of local government agencies provided no training, twenty-one percent provided initial training on hiring, twenty-six percent provided annual training of some kind, and twenty-four percent did not respond" (Pfeiffer, 2015, p.29). These findings are consistent with the findings from other research results that show there is a lack of cybersecurity training in local governments (Norris et al., 2019; Caruson et al., 2012).

2.4.1.4 (Un)awareness of Being Under Attack

Detection of cyber attacks are extremely difficult because most of the time they are done by invisible and silent attackers who might not want victims to know they attacked. For example, a black-hat hacker might want to steal the personal information of a government agency. In most of the cases, the hacker does not want the agency to notice they were breached. Norris (2019) found that one-third of the local government agencies do not know whether they were under attack, and nearly two-third of them do not know whether their information systems have been breached, or not. The problem of unawareness of being under attack causes the local governments to remain inactive in managing cybersecurity.

2.4.2 Proposals for Improving Local-Level Cybersecurity

A majority of scholars agree that local governments should lead on protecting their cyberspace. The literature identifies five basic ways to improve local level cybersecurity practices.

2.4.2.1 Funding

As discussed above, insufficient budget is the most known barrier in local-level cybersecurity management. Since the funding is always an issue to manage cybersecurity in local governments (Ponemon Institute, 2015; Norris, 2017, 2018, 2019; Caruson et al., 2015; Lohrmann, 2017), scholars call the Federal government and state governments for increasing the budget for cybersecurity. Local governments should also be careful on how they use their budget because it can be just important how to allocate budget resources than how much money is spent (Karakoç, 2017).

2.4.2.2 Training

All of the employees who have access to a local government computer system should be periodically trained on cybersecurity. Providing continuing IT security training is cost-effective because a large data breach caused by an employee may cost the local government millions in resources and diminish citizens' trust in their government (Whitmer, 2007). A lack of adequately trained personnel is also due to limited budget because it costs money to the local governments to hire or train personnel (Norris et al., 2019). For this reason, Norris and his colleagues propose that local governments should be careful on allocating their budget to provide money for personnel training.

2.4.2.3 Better Equipment

Local governments use electronic devices to provide more efficient and quick public service. The systems and software should be updated in a timely period (Federal Communications Commission, 2012). These updates should include security patches, firmware upgrades, and, if necessary, hardware upgrades. Using automatic updating services and continually scanning and testing systems (Norris et al., 2018) helps to keep local government IT services updated sufficiently. Wolff and Lehr state that "… local governments should invest in protection mechanisms that emphasize computer system resilience, network segmentation, and regular, automated back-ups to allow for rebooting in the event of a ransomware attack" (2018, p. 71). In addition, Norris et al. (2018) recommend local government administrators use two factor authentication and authorization to access their administrator accounts (Norris et al., 2018). This prevents potential cyberattacks that might cause data breaches.

2.4.2.4 Better Coordination and Communication

Local governments with limited resources and cybersecurity expertise have difficulty in managing cybersecurity. Establishing a cybersecurity team is not cost efficient for many local governments. Norris et al. (2018) suggest local governments should be in communication with officials from the state and federal government to cooperatively work on cybersecurity policies and procedures, and methods for implementation. Instead of centralization, an expanded coordination should be the kickoff of intergovernmental and public-private relation reform. (Harknett & Stever, 2009). Similarly, Wolff and Lehr (2018) suggest partnerships among government agencies and "national top-down leadership with bottom-up cooperation and coordination" (p. 74). Better communication and coordination among local government agencies also help to manage cybersecurity efficiently.

2.4.2.5 Culture

Creating a culture of cybersecurity for American local governments improves the local-level practice of cybersecurity (Caruson et al., 2012; Harknett & Stever, 2009; Norris et al., 2018, 2019, 2017; Theofanos et al., 2017). In addition, as Norris et. al. (2018) discovered from their focus group research, practitioners (local government officers) believe that it is necessary for local governments to create a culture for cybersecurity. To create this culture, there is a need for perception change among non-IT public administrators (Caruson et al., 2012; Theofanos et al., 2017). Because this is an overarching proposal, it might come true with more education, better equipment, better communication, technical how-know, and more funds. Norris et al. (2018) propose that "this would be a culture in which all parties, especially end-users, but also elected officials and top managers, would understand and embrace the need for

high levels of cybersecurity, would be well trained in appropriate cybersecurity policies and techniques, would practice cybersecurity, and would be held accountable for their actions regarding cybersecurity" (p. 10).

Cultural change is necessary to ensure that government officials and contractors know their IT security responsibilities and understand that they are crucial (Whitmer, 2007).

Many of these important issues on the local cybersecurity front also appear at the state-level cybersecurity posture. For instance, insufficient budget has always been an issue for both local and state governments (Deloitte and National Association of State Chief Information Officers (NASCIO), 2012, 2014, 2016, 2018; Norris et al., 2017; Ponemon Institute, 2015). A lack of trained personnel and inadequate availability of cybersecurity professionals are also common barriers for both types of governments. As a result, the big portion of the barriers state and local governments face overlap. The next section reviews the literature at state level. In addition to proving a state government perspective on the barriers that both types of governments face, the next section also introduces additional barriers that are mostly faced by state governments. Furthermore, it discusses proposals for addressing cybersecurity barriers at the state level.

2.5 State-level Cybersecurity

State governments hold sensitive collections of personally identifiable information (PII) of its residents including health and driving records, educational and criminal records, professional licenses and tax information, etc. For this reason, cybercriminals have increasingly targeted the state governments. Some scholars believe that cyberattacks to States are inevitable (Karakoç, 2017; Norris et al., 2019)

and these intrusions will always continue (Glennon, 2012). For this reason, the state governments have a critical role to mitigate and respond to malicious cyber activities. These cyberattacks are not only damaging the critical infrastructure, information systems, and data of the states, but also the nation's ability to fight crime (Janairo, 2002). Thus, the individual state governments have a responsibility to protect "critical infrastructure as well as the data that has been entrusted to them by their citizens" and "ensure that their citizens can rely on safe and secure Internet connectivity." (Spidalieri 2015 p. 13).

Each year NASCIO conducts a survey to identify and prioritize the top policy and technology issues facing state governments. The state CIOs are the responders of these surveys. Survey results have been used as input to NASCIO's programs, planning for conference sessions, and publications. According to these survey results, cybersecurity has been the state CIOs' top priority since 2014 (Deloitte and National Association of State Chief Information Officers (NASCIO), 2014, 2016, 2018). Because of the importance of the cybersecurity issue, NASCIO admits that cybersecurity is not only an IT function but also has a multidimensional aspect. Janairo (2002) also believes that cybersecurity must be considered from a statewide perspective rather than only the responsibility of a technical department.

This section reviews the literature on state government cybersecurity with a specific focus on (1) the barriers that state governments have been facing, (2) some proposals to strengthen the practices of cybersecurity, and (3) state-level cybersecurity strategic planning.

2.5.1 Barriers and Challenges

State CIOs identified three major barriers (See Figure 2.2) that challenge state governments in addressing cybersecurity since 2010 (Deloitte and National Association of State Chief Information Officers (NASCIO), 2012, 2014, 2016, 2018): (1) a lack of sufficient funding, (2) an increasing sophistication of threats, and (3) an inadequate availability of cybersecurity professionals. These barriers pose constraints on cybersecurity plans and policies. They also correspond to the literature findings and mostly similar to barriers local governments face that were discussed in the previous section. In this section, these three major barriers that challenge state governments are briefly reviewed.

2.5.1.1 Lack of Sufficient Funding

Dan Lohrmann (2017), the former chief information security officer (CISO) of the state of Michigan, states that funding for cybersecurity has always been a problem for state governments. Mark Raymond, the state of Connecticut's CIO, states that the state allocates only 1 percent of its IT budget for cybersecurity (Bergal, 2017).

NASCIO-Deloitte Cybersecurity Survey (2018) also clearly shows that State's IT leaders often lack the funding to maintain their cybersecurity. The survey results demonstrate almost fifty percent of states do not have a separate cybersecurity budget. More than one third of the other half of the states have had static or reduced budgets over time even though they have a separate cybersecurity budget. The survey results also match up with Mark Raymond's statement that the majority of states spend 1 to 2 percent of their IT budgets on cybersecurity whereas federal agencies spend 5-10 percent of their IT budgets for cybersecurity. As Figure 2.2 shows, a lack of budget has been the most significant issue of state government CISOs every year.

In addition to these findings from the practitioners, scholarly works also show that US State governments often struggle with lack of sufficient funds to deal with the cybersecurity threats they face (Wolff & Lehr, 2018).

2.5.1.2 Increasing Sophistication of Threats

Tools and techniques used by cyber attackers are immensely complex and utilize a broad range of technologies. Thus, cyberthreats are steadily becoming more sophisticated. Expanding nature of sophistication of cyberthreats puts state governments behind the eight ball. Van Dine et al. (2017) argue that growing sophistication of cyber threats injures the capabilities of governments. Moreover, according to the 2018 Deloitte-NASCIO Cybersecurity Study (2018), 48 percent of state CIO's indicated there was an increasing sophistication of cyberthreats.

Cyberattacks are becoming sophisticated in two ways: (1) philosophically and (2) technically (Karakoç, 2017). On the one hand, improvements in social engineering techniques, the act of manipulating people into performing actions (McQuade (2006), makes cyberthreats more sophisticated. On the other hand, cyber attackers always improve their strategies by using new tools and technological improvements which create new cyberattack techniques that are harder to detect.

2.5.1.3 Inadequate Availability of Cybersecurity Professionals

In addition to budgetary and sophistication concerns, state governments face a serious shortage of cybersecurity professionals. Two third of state governments' IT initiatives are hindered by a lack of qualified candidates. Furthermore, 85 percent of States struggle with finding the available positions. In addition, approximately 92 percent of states admit that this shortage results because of low salary rates and pay

grade structures. For government agencies, it is not easy to compete with the private sector in terms of IT professionals' salary. For instance, Michigan State officials report that salaries of their cybersecurity professionals are 20 percent below the market rate. Private sector companies are able to offer salaries $25.000 higher than state government agencies (Karakoç, 2017; NASCIO, 2015; Stone, 2014).

According to the Deloitte-NASCIO Cybersecurity studies (2010, 2014, 2016, 2018), as Figure 2.2 shows, almost half of the state CIO's surveyed indicated that there is an inadequate availability of cybersecurity professionals since 2010. The size of this shortage positively correlates with the cyber attacks and data breaches because States are likely to spend more money when they challenge cybersecurity problems, rather than preemptively. Wolff and Lehr (2018), in their scholarly research, found out that state governments struggle with finding technical expertise to deal with the cybersecurity threats they face.

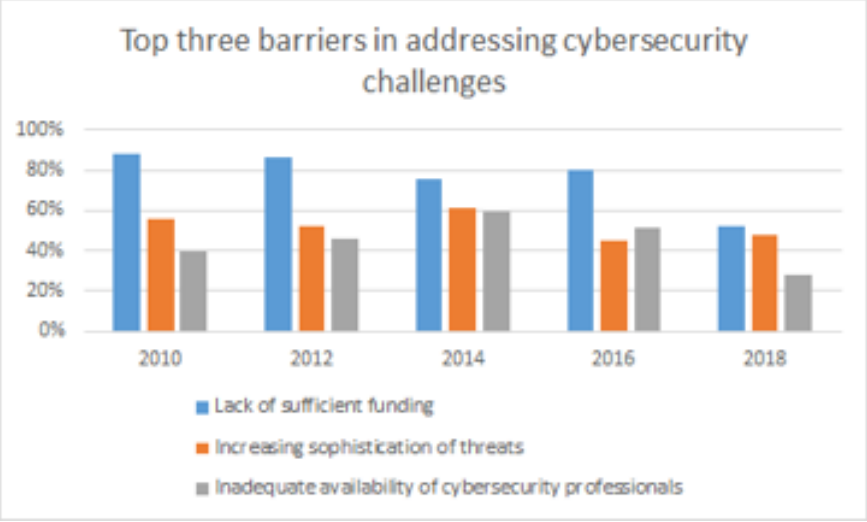

Figure 2.2 Top three barriers in addressing cybersecurity challenges. Source: Author's calculation from Deloitte-NASCIO Studies; 2010, 2012, 2014, 2016, 2018.

In addition to these major barriers discussed above, there are other barriers such as undeveloped public-private cybersecurity (Eichensehr, 2016), weak cybersecurity legislation (Alexander et al., 2020; Glennon, 2012), and organizational politics (Ponemon Institute, 2015) among States. Knowing these barriers helps to define and identify cybersecurity managing problems which is necessary for planning cybersecurity in the States. The next section discusses assessment of cyber-readiness which evaluates how states are prepared for potential cyberattacks.

2.5.1.4 Lack of Adequate Cybersecurity Planning

Three intertwined issues discussed above limit state government cybersecurity planning. Most scholars agree that states are far from cyber-ready (Bhaskar, 2006; Dawson and Desouza, 2015; Spidalieri, 2015). While it is challenging for the states to plan in advance because of the rapid changing nature of cyber attacks and for all the reasons mentioned above, there is still a large room for them to improve their cybersecurity posture. For instance, Bhaskar (2006) states that even though the national cybersecurity plan helps to increase the success rate in responding to cybersecurity incidents and reducing potential damage, the state governments are not successful in responding to these incidents because different agencies are responsible for different tasks and they do not necessarily coordinate.

Similarly, Spidalieri (2015) overviews the level of "cyber readiness" across different States. She uses Melissa Hataway's "Cyber Readiness Index" methodology to evaluate the current level of States' cybersecurity posture. In conclusion, Spidalieri (2015) claims that none of the States are ready in terms of cybersecurity.

Lastly, Dawson and Desouza (2015) conducted a content analysis of state government IT strategic plans. The authors analyzed the current state of cybersecurity

of each state. They used the NASCIO's security related concerns exhorted state CIOs in 2015. The authors found that there is little evidence of cybersecurity as an issue and none of the state IT strategic plans are strong enough for addressing cybersecurity as an issue. The authors claimed that States still have much work to do in order to consider and evaluate cybersecurity as a significant issue.

Although the lack of sufficient state-level cybersecurity planning discussed above creates a general picture of cyber-unreadiness, the differences amongst states must be considered. Because every state faces a unique set of challenges, no model will be ideal in all contexts. For this reason, some scholars believe that each state should craft its cybersecurity planning and legislation differently (Alexander et al., 2020; Cohen & Nussbaum, 2018). However, Cohen and Nussbaum claim that "... individual successful programs and approaches can collectively constitute a menu of options from which states can pick and choose those methods and techniques that fit their needs." (2018, p. 10). They provide three major models based on existing planning practices in the States of Arizona, New Jersey, and Washington. According to Cohen and Nussbaum (2018), these states represent three main approaches: (1) The Community Approach (Arizona), (2) The Bureaucratic Superstructure Approach (New Jersey), and (3) The Multidisciplinary Approach (Washington). This dissertation project uses a similar way of model building based on 2018 NIST cybersecurity standards that are discussed in Chapter 3.

2.5.2 Proposals for Improving State-Level Cybersecurity

Beside state-level cybersecurity challenges, there is also literature on proposals for state-level cybersecurity policy makers to help with design their programs. In order to improve their cybersecurity planning and combat cyber risks scholars argue that

States should carefully follow the latest security products, tools, and technology plans (Spidalieri, 2015) and adopt standards, policies, and procedures created by NIST (Dawson and Desouza, 2015). Clark and Hakim (2017) believe the separation of power between the Federal government and the States makes it very difficult to develop a holistic and unified cybersecurity strategy. For this reason, they claim that adopting public-private partnerships (PPPs) is a favorable solution to overcome constitutional and political barriers to developing unified cybersecurity strategies. Similarly, Cohen and Nussbaum (2018) state that state-level cybersecurity policy makers should consider the private sector as a vital part of the ecosystem.

Another major theme of proposals is collaboration. Both academy and policy practitioners agree that state-level cybersecurity practices could benefit a lot from collaboration amongst state governments as well as between local governments and state governments.

Particularly, state governments should be in charge of providing guidance to local government agencies. They also should be kept in touch with the federal government about best security practices. State governments also should communicate to the appropriate federal agencies for incident reporting (Wolff & Lehr, 2018).

More specifically, Goodyear et al. (2010) identified five areas for further collaboration: (1) increasing the use of collaboration and networks, (2) evaluating their formal and informal relationships with federal cybersecurity officials, (3) devoting increased attention to and receiving training in multidisciplinary problem solving, (4) receiving training in collaboration competencies and those competencies should be recognized and rewarded, and (5) devoting increased attention to data management. Through these measures a more multistakeholder approach to cybersecurity can be

developed, because they include many actors (public and private as well as state and local) to increase cyber resilience (Cohen & Nussbaum, 2018; Goodyear et al., 2010; Ward & Brunner, 2020).

2.6 Summary

This chapter reviewed the literature on local, state, and national level cybersecurity challenges and proposals. Because cybersecurity planning documents and policies of the state governments have not been studied by scholars, there are two major gaps in the relevant literature. First, all of the state governments have some kind of cybersecurity planning documents and implement different cybersecurity relate policies to manage their cybersecurity in state agencies; however, there is no research that systematically evaluates these planning documents. Second, state governments use different guidelines and frameworks to create cybersecurity planning documents and policies; however, there is no research about the extent to which States' cybersecurity policies correspond to their cybersecurity planning documents. Overall, this research addresses these two gaps in the literature in two ways.

First, this research analyzes the common and differential features of cybersecurity planning documents for each state, which reveals the characteristics of the state governments' cybersecurity planning documents. This typology of state cybersecurity planning documents is a unique contribution to the literature that shows common and diverging themes. Second, it creates a cybersecurity-related policy inventory for the sample states, which enables to examine if and to what extent the policies correspond to the best practices. In this way, the research examines whether cybersecurity plans were implemented, or not.

The next chapter lays out the research design, including research questions, conceptualization, data collection and analysis methods, and justification for the sample selection as well as the research limitations.

Chapter 3

CONCEPTUALIZATION AND RESEARCH DESIGN

This chapter explains the research design of this dissertation in five sections. First, it defines the major concepts such as cybersecurity planning documents, cybersecurity-related policies, the best practices framework, which includes the conceptualization of the NIST Cybersecurity Framework and scholarly themes. After the concept definitions, the chapter discusses the four research questions and the methodology. The data collection explains how planning documents and policies are accessed and collected. Data analysis includes the descriptive quantitative analysis for background information as well as qualitative document analysis to answer the four main research questions. Lastly, research limitations explain the factors that might limit the research.

3.1 Concepts

This section explains and defines the major concepts used throughout this dissertation. It defines what this dissertation considers as "cybersecurity planning documents", "cybersecurity-related policies", and "the best practices."

3.1.1 Cybersecurity Planning Documents

State governments and its agencies are under pressure to plan their cybersecurity for two reasons. First, cyberattacks to state governments are getting increasingly more sophisticated. Second, there is a lack of sufficient federal laws and regulations that are tailored for state governments. The present laws such as the Health

Insurance Portability and Accountability Act of 1996 (HIPPA) that mandates protection of sensitive health information of patients and Sarbanes-Oxley Act of 2002 that requires corporations to conduct certain practices in financial record keeping and reporting apply to all entities no matter where they are regulated. Even though states follow similar planning techniques and learn from each other, there are variations among state governments' cybersecurity planning methods. For this reason, types of cybersecurity planning documents could vary among states. For instance, some states (e.g., Alabama) prefer to give a place for their cybersecurity planning in their Information Technology plans whereas some others (e.g., Illinois and Indiana) create Cybersecurity Strategic Plans. Moreover, others (e.g., Connecticut and Michigan) plan their cybersecurity with multiple resources such as Cybersecurity Strategic plans, Cybersecurity Action Plans, Cyber Incident Response Plans, and Cyber Disruption Response Plans (Alabama OIT Cybersecurity, n.d.; Connecticut Cybersecurity Resource Page, n.d.; Indiana Cybersecurity, 2021; State of Illinois Cybersecurity Strategy - Securing the State, n.d.).

In this dissertation project, the "Cybersecurity Planning Documents" term is defined as state government released documents or sections of documents that engage with cybersecurity planning. These cybersecurity planning documents include state strategic plans, annual reports, information technology plans, and cybersecurity response plans. The documents that are about cybersecurity planning in their entirety, such as Cybersecurity Strategic Plans and Cyber Disruption Response Plan, are the subject of analysis. If a document only mentions a section for cybersecurity planning, such as Information Technology Strategic Plan and Statewide Technology plan, that relevant section is considered as a cybersecurity planning document. For states that do

not have such separate documents, but share cybersecurity planning information on their official websites, the websites themselves are considered as planning documents.

3.1.2 Cybersecurity-related Policies

In this dissertation, "cybersecurity-related policies" refers to state bills and resolutions related to cybersecurity. The research only examines enacted state legislations and excludes failed and pending ones. Resolutions refer to various initiatives that are not accepted as legislative activities. Besides these legislative actions, some states also make policies by giving authority to particular agencies or the Governor rather than approving each separate policy. While some agencies publish these executive and administrative policies on their websites, others are not willing to publicize them. Thus, this research does not cover the executive and administrative policies because of the lack of systemic data.

The majority of the sample states (ratio: 5/8) of this research are centralized which means they rarely engage in executive and administrative policy activities. Instead, they mostly pass legislation by approving each separate policy through normal legislative order. The other three sample states are hybrid. Thus, implications of excluding executive and administrative policies are minimal for this research.

3.1.3 The Best Practices

This dissertation conceptualizes the best practices for state governments in cybersecurity planning and policymaking based on two resources: (1) 2018 NIST Cybersecurity Framework standards and (2) the criteria gained from the state and local government scholarship. This combined structure simply adds the NIST standards to the criteria gained from the literature. When applying the best practices framework,

the research seeks out the presences of both the NIST standards and scholarly criteria. This structure is used as the best practices framework to evaluate cybersecurity planning documents and cybersecurity-related policies of state governments. Both NIST and a large number of scholars (Dawson & Desouza, 2015; Srinivas et al., 2019) recommend NIST Cybersecurity Framework to state governments that aim to improve their cybersecurity posture. However, the framework cannot be the only criteria to evaluate states' cybersecurity planning documents and policies because every state has different risk profiles. For this reason, other evaluation criteria based on cybersecurity scholarship at the state and local government level are included, which are: *leadership, partnership, funding, training, better equipment, developing awareness and culture for cybersecurity, coordination and communication*, and *national security*.

3.1.3.1 NIST Cybersecurity Framework

NIST developed the "Framework for Improving Critical Infrastructure Cybersecurity" in response to Obama's Executive order 13636 in 2014. In 2018, NIST revised the framework based on the feedback received from eight public workshops and thousands of direct interactions with stakeholders from various industry sectors in the United States and around the world (NIST, 2018). The framework is also known as NIST Cybersecurity Framework (CSF). CSF allows public and private organizations to manage and improve their cybersecurity posture in terms of preventing, detecting, and responding to cyber-attacks. It consists of standards and guidelines to mitigate and respond to cybersecurity-related risks. The main purpose of the CSF is to establish a set of standards and practices to help organizations address cybersecurity risks.

CSF is considered a guidance to improve the nation's critical infrastructure; however, it can also be adopted by any size of companies and organizations across

different sectors in addition to federal, state, and local governments (NIST, 2018, p. v). In addition to the NIST's recommendation for adaptation of CSF to different sectors, a number of scholars consider the CSF a useful guidance to state (Dawson & Desouza, 2015; Srinivas et al., 2019) and local (Ibrahim et al., 2018; Norris et al., 2018, 2020) governments to improve their cybersecurity posture.

Besides academics, policy practitioners also recommend the use of the Framework in state governments. For instance, National Governors Association (NGA) argues that it is vital for state governments to utilize the Framework in order "to determine their current level of cybersecurity, set goals for cybersecurity that are in sync with their business environment, and establish a plan for improving or maintaining their cybersecurity." According to Federal Cybersecurity Programs: A Resource Guide, "the cybersecurity framework also offers a methodology to protect privacy and civil liberties to help organizations incorporate those protections into a comprehensive cybersecurity program." (NGA, 2014 quoted from NIST, 2018).

Some state governments already use the five functions of the Framework as a guidance in planning their cybersecurity and developing strategic plans because the NIST standards create a common language across public agencies. For instance, "the State of Texas Agency Security Plan template developed by the Department of Information Resources uses … five concurrent and continuous functions, which are the same as the Cybersecurity Framework's functions." (Texas Department of Information Resource, 2020). By doing so, the State of Texas aims to benefit from the common language NIST provides. Consequently, it achieves a cost-effective way to manage cybersecurity risks without dealing with the expenditure of creating new regulatory requirements (Texas Department of Information Resource, 2020).

Similarly, the State of Illinois also adopted the NIST Cybersecurity Framework to develop their cybersecurity programs with the widely accepted roadmap and the consistent set of maturity measurement. As in the case of State of Texas, Illinois also refers to the expertise authority and prevalent acceptance of the NIST standards (Illinois Department of Innovation and Technology, 2017). Shoemaker (2019) explains this expertise authority of NIST by resembling to the role that the American Medical Association plays for doctors, the American Bar Association plays for lawyers, and the National Society of Professional Engineers plays for engineers. The expert authority of NIST is due to its identification of the most successful and applicable cybersecurity policies and practices.

Furthermore, the State of Minnesota utilizes the five core functions of the NIST CSF to create a scorecard that evaluates the cybersecurity posture across its agencies. This scorecard aims to provide an empirical assessment of the state agencies in service of the executives who might not be experts of cybersecurity (NIST, 2018).

There are other cybersecurity frameworks such as ISO IEC 27001/ISO 27002, IASME Governance, CIS v7, and FISMA. However, due to the reasons explained above, most state governments use the NIST CSF and so does this dissertation. Although the NIST CSF was designed for the critical infrastructure sector, the resemblance of the state governments cybersecurity needs allows the use of this Framework at the state level. Cybersecurity is an issue that requires basic standards for enhancing the protection of the cyberspace. Because of the nature of the issue, the planning needs between public and private agencies do not differ significantly.

Even though each state has different cybersecurity responsibilities, the NIST CSF provides a basic guideline that benefits all state governments. Thus, scholars,

policy makers, and NIST as an expert authority concur that the CSF, and the core five functions within the framework, are well-suited to assess state government cybersecurity planning.

The next section discusses the CSF's core 5 functions that are the first part of the best practices framework.

3.1.3.1.1 The Framework Core

The Framework Core is "a set of cybersecurity activities, desired outcomes, and applicable references ..." (p. V) that "... can be used by organizations in any sector or community" (NIST, 2018, p. 3). Standards and guidelines that the Framework Core presents allow all organizational levels for communication of cybersecurity activities and outcomes in the organization. It is used to examine the sample states' cybersecurity planning documents and cybersecurity-related policies. Figure 3.1 shows the five interrelated and continuous functions of the Framework Core: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover (NIST, 2018).

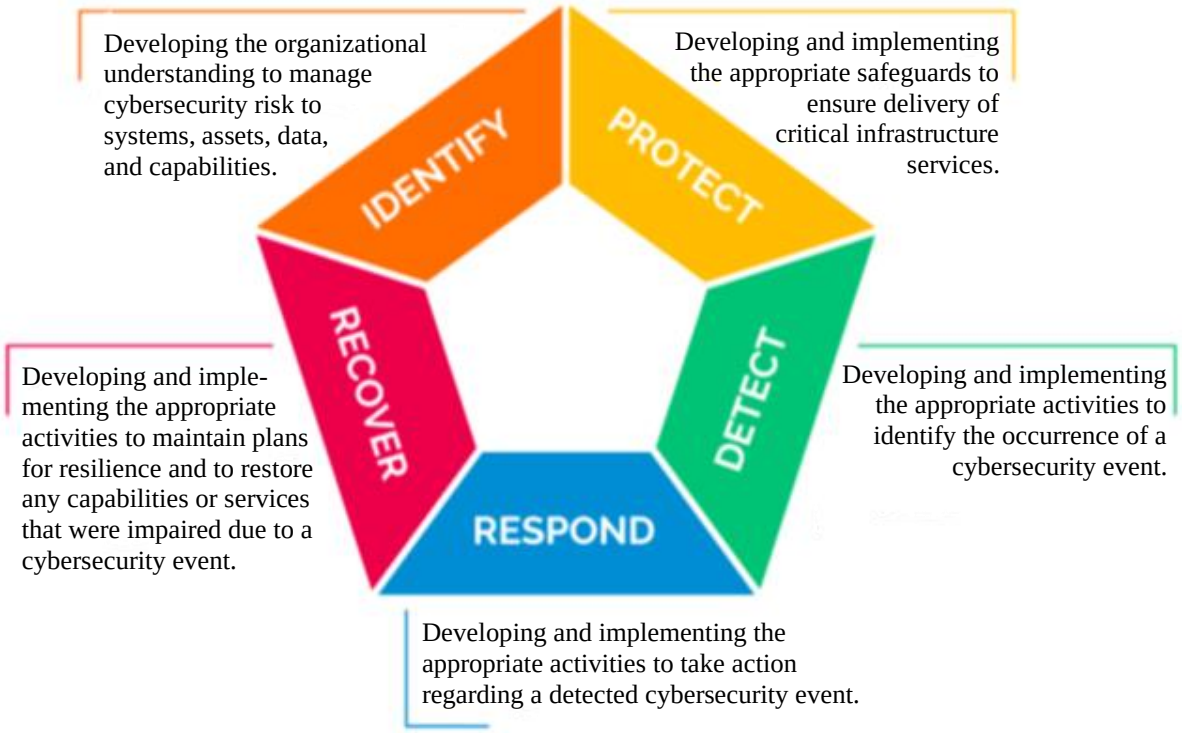

Figure 3.1 NIST Cybersecurity Framework Core Functions. Source: 2018 NIST Cybersecurity Framework

These functions produce a critical strategic view for an organization's cybersecurity risk management when they are considered collectively. Figure 3.1 also summarizes the descriptions of these functions.

Each Function has its own Categories. Table 3.1 shows the listing of the Functions and Categories under each Function in CSF. For example, under the "Identify" function, there are six different categories: (1) Asset Management (ID.AM), (2) Business Environment (ID.BE), (3) Governance (ID.GV), (4) Risk Assessment

(ID.RA), (5) Risk Management Strategy (ID.RM), and (6) Supply Chain Risk Management (ID.SC). The Best Practices Framework considers a function is addressed if any of the function's categories mentioned in the cybersecurity planning document and policies.

Table 3.1 Function and Category Unique Identifiers

Function	Category Unique Identifier	Category
Identify	ID.AM	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy
	ID.SC	Supply Chain Risk Management
Protect	PR.AC	Identity Management and Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection Processes and Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology
Detect	DE.AE	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes
Respond	RS.RP	Response Planning
	RS.CO	Communications
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements
Recover	RC.RP	Recovery Planning
	RC.IM	Improvements
	RC.CO	Communications

Source: NIST Cybersecurity Framework, 2018.

Each Category has its own Subcategories, and every Subcategory also has its Informative References which are specific sections of a variety of information security

standards. The Framework Core matches the Informative References such as existing standards, guidelines, and practices with each Subcategory.

NIST CSF is originally created for critical infrastructures; for this reason, it is very detailed in terms of subcategories and informative resources. However, as NIST suggested, this framework can be used by organizations in any sector or community. State level cybersecurity planning documents and policies are not detailed enough to evaluate on the bases of Subcategories and Informative References.[2] Thus, this dissertation examines cybersecurity planning documents and policies based on the CSF Functions and their Categories. 0 describes each Category of the Functions. Because Subcategories and Informative References are not used as evaluation criteria, this dissertation does not describe them in detail.

Table 3.2 NIST Cybersecurity Framework Functions, Categories, and Descriptions

Function	Category	Description
IDENTIFY	**Asset Management**	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

[2] This implies the immaturity of state and local level cybersecurity planning documents. CSF provides the roadmap for State and local governments to mature and address various cyber risks by providing detailed guidelines.

	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
	Supply Chain Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
PROTECT	**Identity Management, Authentication and Access Control**	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
	Awareness and Training	The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

	Maintenance	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
	Protective Technology	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
DETECT	**Anomalies and Events**	Anomalous activity is detected and the potential impact of events is understood.
	Security Continuous Monitoring	The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
RESPOND	**Response Planning**	Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
	Communications	Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
	Analysis	Analysis is conducted to ensure effective response and support recovery activities.
	Mitigation	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
	Improvements	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RECOVER	**Recovery Planning**	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
	Improvements	Recovery planning and processes are improved by incorporating lessons learned into future activities.

	Communications	Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

Sources: 2018 NIST Cybersecurity Framework

Overall, organizations use these five Functions and Categories to find relevant answers for fundamental questions such as "how well are we doing" in terms of cybersecurity management. Because each state has different cybersecurity planning and policy needs, addressing one category will be considered as a sufficient function. For this reason, the Best Practices Framework considers a function addressed if any of the function's categories are mentioned in the cybersecurity planning document and policies.

In addition to the NIST Cybersecurity Framework, the scholarly criteria are used when analyzing planning documents and cybersecurity-related policies. The next section discusses the scholarly criteria in further detail.[3]

3.1.3.2 Criteria from the Literature

The local and state level cybersecurity literature recommends cybersecurity planning documents and policies to improve the material structure such as *funding* and *better equipment* (Caruson et al., 2012; Federal Communications Commission, 2012.; Norris et al., 2018, 2019). Furthermore, the personnel aspect of better planning and

[3] The CSF functions and the scholarly criteria are not mutually exclusive and can be supportive of one another. For instance, the CSF's risk assessment enables states to tell where they are deficient and thus help support funding allocations. For research feasibility, they are considered as two complimentary parts of the Best Practices Framework.

policy making requires *leadership* and *training* (Deloitte and National Association of State Chief Information Officers (NASCIO), 2012, 2014, 2016, 2018; Whitmer, 2007). Similarly, cooperation both across the stakeholders such as *partnerships* and within the government agencies through *coordination and communication* are found to be critical (Harknett & Stever, 2009). Also, the informative context such as *developing awareness and a cybersecurity culture* and proving a *national security* context are significant factors in effective cybersecurity planning documents and policies (Ghernouti-Hélie, 2010; Veiga, 2016).

Funding: In cybersecurity planning and policy making, the discussion of how to allocate the budget and how to increase funding are amongst the most significant issues to improve cybersecurity posture. In the text analysis, the keywords "budget", "funding", "money", "cost", "fund(s)", "expenses", "finance", and "resources" are considered as acknowledgement of the funding concept in the cybersecurity planning documents and policies.

Better equipment: The physical infrastructure also constitutes a key point in cybersecurity planning documents and policies. In the text analysis, the keywords "equipment", "material", "hardware", "software", "update", "upgrade", "security patches", and "firmware upgrades" are considered as acknowledgement of the better equipment concept in the cybersecurity planning documents and policies.

Leadership: Administrative structure and authority allocation are significant to clarify the management mechanisms of the organization. State governments with a proactive cybersecurity leadership are more likely to be efficient in managing cybersecurity. In the text analysis, the keywords "leader", "leadership", "hierarchy", "top-down", "bottom-up", "directing", "authority", "manager", "management",

"proactive", and "motivation" are considered as acknowledgement of the leadership concept in the cybersecurity planning documents and policies.

Training: Because cybersecurity is a constantly changing planning and policy area, and the cyberattack are getting more sophisticated, state governments benefit from training their employees. In the text analysis, the keywords "training", "practice", "guidance", "guide", "workshop", "seminar", and "education" are considered as acknowledgement of the training concept in the cybersecurity planning documents and policies.

Partnerships: The private sector is leading the technological innovations as well as security mechanisms for these innovations. So, partnerships with firms, companies, universities, and research institutes have incredible potential of improving state level cybersecurity posture. In the text analysis, the keywords "PPPs", "public private partnership", "university", "institute", "company", "firm", "collaboration", "cooperation", "business", "alliance", "partner", and "corporation" are considered as acknowledgement of the *partnership* concept in the cybersecurity planning documents and policies.

Coordination and communication: Communication between state government agencies facilitate effective translation of newly drafted planning documents and polices. Furthermore, communication is essential for effective coordination between organizations as well as employees. In the text analysis, the keywords "coordination", "communication", "intergovernmental", "contact", "correspondence", "conversation", "report", "publicity", "disclosure", and "briefing" are considered as acknowledgement of the coordination and communication concept in the cybersecurity planning documents and policies.

Developing awareness and cybersecurity culture: Sophistication of cybersecurity threats requires all state government employees and citizens to be alert and informed about the importance of cybersecurity and potential risks. In the text analysis, the keywords “culture”, “awareness”, “knowledge”, “perception”, “consciousness”, “citizen”, “information”, “recognition”, “attention”, and “alertness” are considered as acknowledgement of developing a cybersecurity culture concept in the cybersecurity planning documents and policies.

National security: Past experiences and cases show that foreign cyberattack can target state governments’ cyberspace. For instance, election data stored by the state governments were breached by foreign state sponsored cyber-attacks. For this reason, state governments include the national security context in their planning documents and policies. In the text analysis, the keywords “nation”, “federal”, “national-security”, “country”, “international”, “foreign”, “Russia”, “China”, and “defense” are considered as acknowledgement of the national security concept in the cybersecurity planning documents and policies.

3.2 Research Questions and Methodology

There are two major gaps in the relevant literature. First, all of the state governments have some kind of cybersecurity planning documents to manage their cybersecurity in state agencies; however, there is no research that systematically evaluates these planning documents. Second, state governments use different guidelines and frameworks to create cybersecurity planning documents and policies; however, there is no research about the extent to which States’ cybersecurity policies correspond to their cybersecurity planning documents. Overall, this research addresses these two gaps in the literature.

In order to address the lack of scholarship at state-level cybersecurity planning documents and policies, this dissertation provides a baseline understanding of the state-level cybersecurity planning and policy atmosphere.

RQ1: What are the characteristics of cybersecurity planning documents of 50 states adopted as of December 2021?

To examine this research question, this dissertation evaluates the common and differential features of cybersecurity planning documents for each state. The research uses publicly available cybersecurity planning documents such as state strategic plans, annual reports, information technology plans, response plans, and states' official websites. With a text analysis, this research reveals the characteristics of the state governments' cybersecurity planning documents with a focus on the type of the documents, whether the cybersecurity planning is centralized, and what groups are targeted in the documents. The types of documents show if a state plans its cybersecurity with a cybersecurity-specific consolidated plan or a section in its IT strategic/master plan or its official website. The characteristic of centralized, hybrid, or decentralized planning show how state governments approach cybersecurity planning. This reveals the variation in the authorities who handle cybersecurity planning and the specific advantages and disadvantages of all three approaches. Through iterative skimming, reading, and interpretation techniques (Bowen, 2009), this research question also points out the targeted groups of state cybersecurity planning documents and shows whether citizens, the public sector, or the private sector are targeted in the documents. The variation and commonalities in these characteristics of planning documents draw the landscape of 50 states' cybersecurity planning.

RQ2: In what ways do cybersecurity planning documents of 50 states incorporate the best practices defined by the scholarly criteria and the 2018 NIST Cybersecurity Framework?

In the second phase, state cybersecurity planning documents are examined based on criteria of best practices developed from the literature and the 2018 NIST Cybersecurity Framework standards. The 2018 NIST Cybersecurity Framework standards and criteria from the state and local government scholarship constitute the Best Practices Framework (BPF). This combined structure is the framework used to evaluate cybersecurity planning documents of state governments.

Both NIST and a large number of scholars (Dawson & Desouza, 2015; Srinivas et al., 2019) recommend NIST Cybersecurity Framework to state governments that aim to improve their cybersecurity posture. Thus, Chapter 5 evaluates cybersecurity planning documents of 50 states based on the NIST Cybersecurity Framework. However, the NIST Cybersecurity Framework standards cannot be the only criteria to evaluate states' cybersecurity planning documents because the Framework is not inclusive enough. For this reason, Chapter 4 evaluates states' cybersecurity planning documents based on the cybersecurity scholarship at the state and local government level. The criteria from the local level literature are included due to the insufficient cybersecurity scholarship at the state level. The evaluation criteria based on the literature are: *leadership, partnerships, funding, training, better equipment, developing awareness and cybersecurity culture, coordination and communication,* and the context of *national security.* The research analyzes whether the 50 states' cybersecurity planning documents contain these desirable key themes. A content analysis examines the frequency of adoption of these

key themes for each state. The analysis, then, differentiates if the themes are just acknowledged or addressed in-depth with an action plan. This differentiation categorizes states' planning documents based on how many themes they address in-depth. The cross-state analysis also points out model states to show a model plan of best practices.

RQ3: In what ways do cybersecurity policies adopted between 2015 and 2021 legislative sessions of states with high cyberattack figures incorporate the best practices as defined by the scholarly criteria and the 2018 NIST Cybersecurity Framework?

In Chapter 6, this research identifies cybersecurity related policies of eight sample states. This investigation creates a cybersecurity-related policy inventory for the sample states. Similar to the second research question, the cybersecurity-related policies are analyzed based on the Best Practice Framework. The 2015 legislative session is selected because the first version of NIST Cybersecurity Framework was released in 2014. Thus, analyzing the policies crafted prior to 2015 based on the 2014 NIST Cybersecurity Framework standards would be anachronistic.

RQ4: In what ways do the cybersecurity policies in the sample states correspond to their latest cybersecurity planning documents as of the end of the 2021 legislative session?

Chapter 6 also analyzes if and to what extent the adoption of the BPF by the state cybersecurity planning documents correspond to the adoption of the BPF by the policies. For instance, if a cybersecurity planning document of Delaware in 2018 mentions cybersecurity training for its employees, the analysis checks whether the policies from 2015 to 2021 also include a policy on training. Similarly, if there is a

policy on increasing funding, the analysis shows whether that was mentioned in the latest planning documents. This way, the research demonstrates (1) whether cybersecurity planning documents were implemented and (2) whether the policies were shaped in accordance with the planning documents, or not.

3.3 Data collection

There are two main data sources used for this dissertation: planning documents and cybersecurity-related policies. Data collection for this dissertation project contains two stages.

3.3.1 Cybersecurity Planning Documents

To investigate the first and second research questions, publicly available cybersecurity planning documents are being acquired such as state strategic plans, annual reports, information technology plans, and response plans. These documents are collected from the official websites of state governments and their agencies. The corresponding state agencies are emailed to make sure if there are other publicly accessible documents that are not on their websites. Some of the documents are not entirely related to cybersecurity planning. So that, if a document only includes a section for cybersecurity planning, such as Information Technology Strategic Plan and Statewide Technology plan, that relevant section is extracted for the analysis.

3.3.2 Cybersecurity-related Policies

National Conference of State Legislatures (NCSL) has listed cybersecurity-related legislation for each state since 2015. That data for the years from 2015 to 2021 is compiled to create a spreadsheet for the analysis.

The NexisUni database is also used to complement the compilation of policies listed in the NCSL's website. NexisUni allows a full text search of State Bills.

Some of the states have lists on their websites that include cybersecurity-related policies and these are reviewed if there are additional cybersecurity-related policies that are not in the NCSL's list and NexisUni.

3.4 Data Analysis

The data is analyzed in two steps.

3.4.1 Document Analysis of the State Cybersecurity Planning Documents and Policies

Among qualitative methods, document analysis technique is adopted to mark the characteristics of the state governments' cybersecurity planning documents and policies. The document analysis of 50 states' cybersecurity planning documents and policies applies the predetermined themes that are explained in the best practices framework section. The predetermined themes, created by the NIST Cybersecurity Framework standards and scholarly criteria, provide a lens to analyze the planning documents and policies. Thus, the analysis is examined how the data fits to the predetermined themes (Creswell & Creswell, 2018). The document analysis with predetermined themes is used to answer all four research questions. This analysis finds the variation in adoption of the predetermined themes in planning documents and policies. It also shows if the planning documents and policies correspond with one another in terms of adopting the predetermined themes.

The data analysis follows the general steps of qualitative data analysis described by Creswell and Creswell (2018). The cybersecurity planning documents and policies constitute the raw data, which is the first step in the figure below. After

collection, the raw data is organized and prepared for data analysis by keeping the relevant parts for the analysis. Then, relevant sections are read through to understand the general meaning of the data.

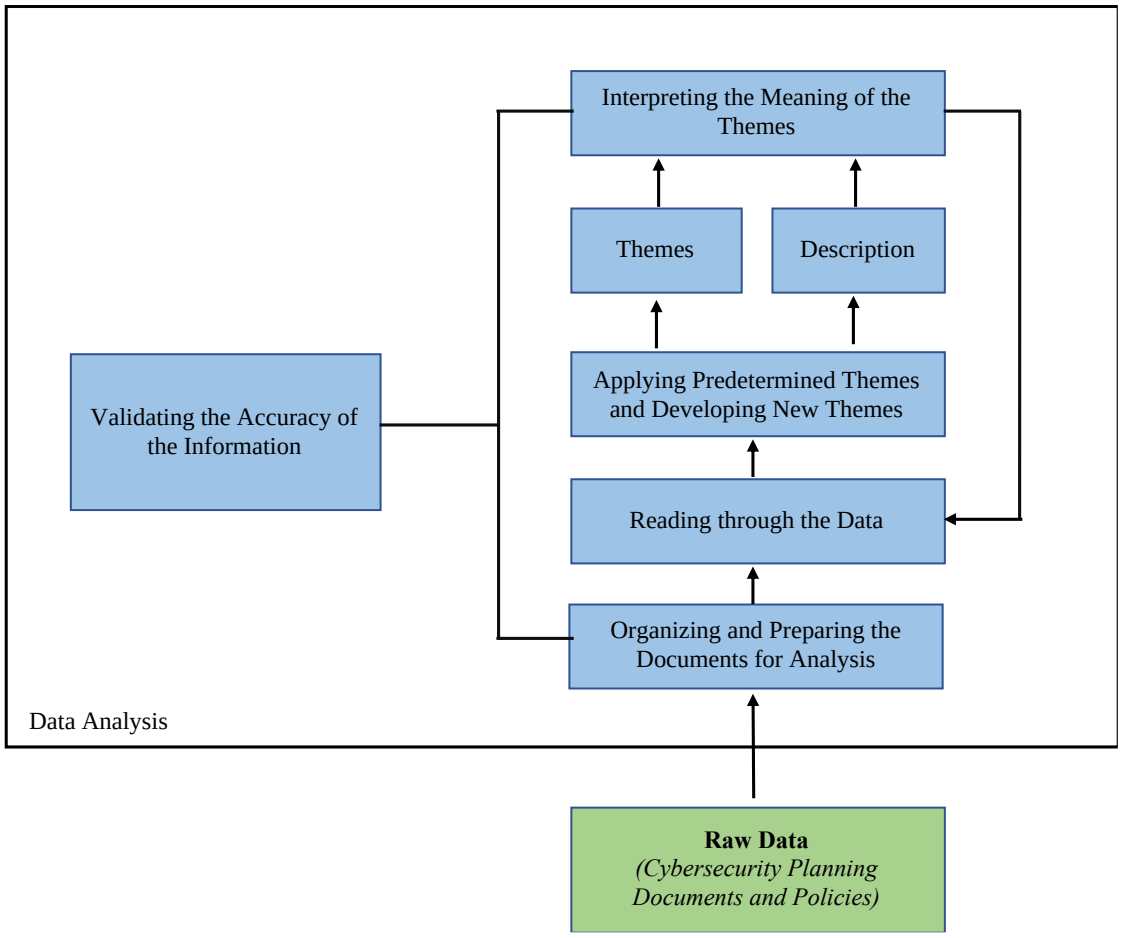

Figure 3.2 Steps of Qualitative Data Analysis (adapted from Creswell & Creswell, 2018, p.194).

The research describes each document and policy in terms of their document type (e.g., IT strategic plan, cybersecurity strategic plan, enacted policy, and pending

policy), the approach to cybersecurity planning (e.g., centralized, decentralized, and hybrid) the target groups (e.g., the public sector, the private sector, and citizens), and year of the publication of the planning documents. After each document is organized, the research applies predetermined themes to the planning documents and policies.

The themes then are interpreted in relation with the descriptions. Because document analyses require iterative skimming, reading, and interpretation (Bowen, 2009), the interpretation step includes going back to the reading stages. As Creswell and Creswell (2018) acknowledges, in reality, the qualitative analysis doesn't necessarily follow this structure strictly. Thus, through all these steps and their repetitions and adjustments, the validation of the accuracy of the research findings occurs.

3.4.2 Sample Selection

This research uses purposeful sampling in case selection which is defined as, "selecting information-rich cases to study, cases that by their nature and substance will illuminate the inquiry question being investigated" (Patton, 2015, p. 401). The sample selection considers the victim loss index and the cybersecurity job supply index as two main dimensions. I assume the states with high victim loss and high cybersecurity job supply are also the ones that focus on cybersecurity in their planning documents and policies because these states are the most at risk from cyberattacks.

To create the victim loss index, this research uses the victim loss variable that measures the financial loss of individuals and businesses that have been the victims of online fraud. The FBI's Internet Crime Complaint Center (IC3) releases the data with victim loss variable in its official website; however, there is no direct way to download the data. So that, Python is used to scrap the data and create a spreadsheet for the

2014-2019 years. Then, the data is imported into Stata and examined from the previous 5 years to create an average victim loss divided by the 5 years average state population. Due to a large variation and standard deviation, the research takes natural logarithm of this variable and thus creates the cybersecurity victim loss index. The index is the X axis of Figure 3.3 Sample Selection.

After creating the victim loss index, the research uses the supply of the cybersecurity workers in the public sector data from the CyberSeek project. The cross-state data covers from October 2018 through September 2019 and contains the estimated number of cybersecurity workers in the public sector. The cybersecurity workers refer to the employees mainly working for cybersecurity jobs such as cybersecurity analysts. They also refer to the workers who need cybersecurity-related skills and certifications as part of their job descriptions. Thus, the data captures the full cybersecurity workforce in the public sector. This data is imported into Stata and divided by average population of each corresponding state. Due to a large variation and standard deviation, the research takes natural logarithm of this number and thus creates the cybersecurity job supply index. This index is the Y axis of Figure 3.3 Sample Selection.

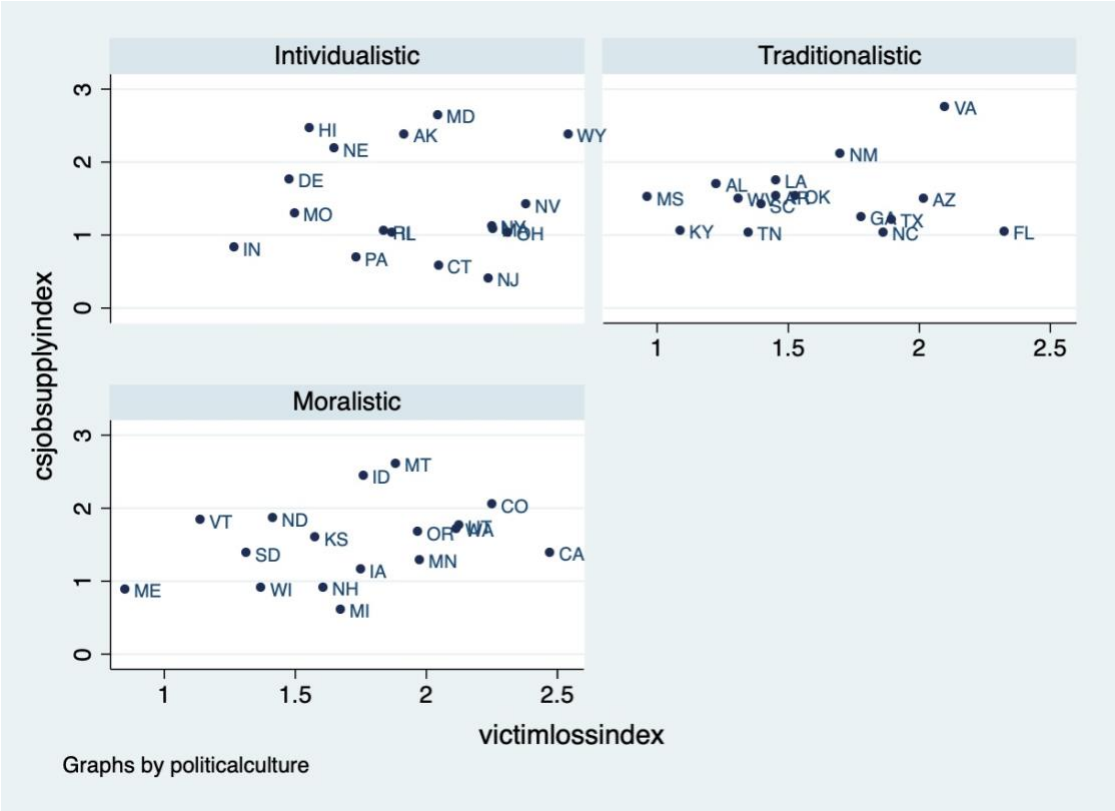

Figure 3.3 Sample Selection.

Finally, this research also uses Daniel Elazar's theory on political culture to create a theoretical background for the sample selection. This theory divides all states into three groups namely, *individualistic*, *traditionalistic*, and *moralistic* states (Elazar, 1991; 1994). Figure 3.3 above illustrates the distribution of states based on higher supply of the cybersecurity workers in the public sector and victim loss for each political culture. The research selects the states with the highest cybersecurity job supply index in each political culture group. According to this selection, the state with the highest supply of the cybersecurity workers amongst *individualistic* states is Maryland, in *traditionalistic* states is Virginia, and in *moralistic* states is Montana.

Then, the research selects the states with highest victim loss index in each political culture group. The highest victim loss amongst *individualistic* states is Wyoming, in *traditionalistic* states is Florida, and lastly in *moralistic* states is California. In addition, due to their strategic importance with regards to financial services requiring high cyberspace protection, the research includes the state of Delaware and New York to the selected cases.

The eight sample states are California, Delaware, Florida, Maryland, Montana, New York, Virginia, and Wyoming. These sample states vary significantly across many state characteristics such as region, size, budget, GDP per capita, etc. Thus, the eight states provide a wide range of states that are relatively representative. However, each state is unique and despite the variation in the sample states, the generalizability of the results of these states to 50 states is still debatable. Future research might use other theories and methods in their sample selection to create a more representative sample. In our case, the purposeful sampling deliberately attempts to select states for whom cybersecurity matters the most.

3.5 Summary

In conclusion, this research adopts a mixed method approach in analyzing state level cybersecurity planning documents and policies. The qualitative analysis answers all four research questions by applying predetermined themes i.e., the Best Practices Framework, to the planning documents and policies. It also examines the correspondence by matching the planning documents and policies for each sample state. The quantitative analysis is adopted for sample selection of this research.

Chapter 4

AN ANALYSIS OF 50 STATES' CYBERSECURITY PLANNING DOCUMENTS

4.1 Introduction

This chapter addresses the results of the analysis with regard to first two research questions. First, it explores the nature of state cybersecurity planning as of December 2021 through an analysis of the key areas of latest cybersecurity planning documents of 50 states. This analysis of planning documents helps to lay out the landscape of state level cybersecurity planning. Second, it examines the extent to which state plans align with best practices defined by scholarly literature. This is done through a review of the extent and ways in which states' cybersecurity planning documents incorporate the best practices as defined by the scholarly literature.[4]

The next section explores the nature of cybersecurity planning documents and describes the striking variations across the 50 states. The following section focuses on the key themes of the state cybersecurity plans, and the patterns, differences, and similarities among the states based on the key themes included in their documents. Then, the chapter does a cross-state analysis that categorizes states based on their in-depth coverage of the themes. Finally, the chapter offers an account on some themes that pair in the cybersecurity planning documents.

---

[4] Incorporation of the best practices defined by NIST is examined in Chapter 5.

4.2 The State of Cybersecurity Planning of the States

Through an analysis of 50 States' cybersecurity planning documents, this research finds that there is a lack of uniformity amongst cybersecurity planning documents across the states.

First and foremost, the types of planning documents differ in their construction, organization as well as content. While some states have comprehensive, consolidated, specific plans for cybersecurity (e.g., Rhode Island, Indiana, New Jersey), others spare a section in their IT strategic/master plans (e.g., Mississippi, New Mexico, North Carolina), yet some others plan their cybersecurity only in their official websites (e.g., South Dakota, Alaska)[5]. Table 4.1 below demonstrates the variation in document type, centralization of the planning, and targeted groups.

Table 4.1 Characteristics of State Plans

State	Type of Planning Document	Centralized / Decentralized (2018)	Targeted Groups
Alabama	A section in IT Plan	Hybrid	Public Sector
Alaska	Website	Centralized	Public Sector
Arizona	A section in IT Plan	Centralized	Public Sector
Arkansas	Website	Hybrid	Public Sector, Private Sector
California	Cybersecurity Specific	Hybrid	Public Sector, Private Sector, Citizens

[5] The lack of standardization of the document types also causes a variation in the format of states' cybersecurity planning documents. For instance, the length of the documents ranges from one page to over hundred pages. Some states have only one planning document, others have multiple, and a few of them do not even have a publicly available document. Finally, some plans cover only a year whereas others are for 5 years.

Colorado	A section in IT Plan	Centralized	Public Sector
Connecticut	Cybersecurity Specific	Centralized	Public Sector, Private Sector, Citizens
Delaware	A section in IT Plan	Centralized	Public Sector, Private Sector
Florida	Cybersecurity Specific	Hybrid	Public Sector, Private Sector
Georgia	A section in IT Plan	Hybrid	Public Sector, Private Sector
Hawaii	Cybersecurity Specific	Hybrid	Public Sector
Idaho	A section in IT Plan	Hybrid	Public Sector
Illinois	Cybersecurity Specific	Centralized	Public Sector, Private Sector
Indiana	Cybersecurity Specific	Centralized	Public Sector, Private Sector
Iowa	Cybersecurity Specific	Hybrid	Public Sector, Private Sector, Citizens
Kansas	Cybersecurity Specific	Hybrid	Public Sector, Private Sector, Citizens
Kentucky	A section in IT Plan	Hybrid	Public Sector
Louisiana	Cybersecurity Specific	Centralized	Public Sector, Private Sector
Maine	Website	Centralized	Public Sector
Maryland	A section in IT Plan	Centralized	Public Sector, Private Sector
Massachusetts	Website	Hybrid	Public Sector, Private Sector, Citizens
Michigan	Cybersecurity Specific	Centralized	Public Sector, Private Sector, Citizens
Minnesota	A section in IT Plan	Centralized	Public Sector, Private Sector
Mississippi	A section in IT Plan	Hybrid	Public Sector, Private Sector
Missouri	Cybersecurity Specific	Centralized	Public Sector
Montana	A section in IT Plan	Hybrid	Public Sector, Private Sector, Citizens
Nebraska	Website	Centralized	Public Sector
Nevada	A section in IT Plan	Hybrid	Public Sector, Private Sector
New Hampshire	A section in IT Plan	Centralized	Public Sector, Private Sector
New Jersey	Cybersecurity Specific	Hybrid	Public Sector, Private Sector, Citizens
New Mexico	Cybersecurity Specific	Centralized	Public Sector

New York	Cybersecurity Specific	Centralized	Public Sector, Private Sector
North Carolina	A section in IT Plan	Centralized	Public Sector, Private Sector
North Dakota	A section in IT Plan	Centralized	Public Sector, Private Sector, Citizens
Ohio	A section in IT Plan	Centralized	Public Sector
Oklahoma	A section in IT Plan	Centralized	Public Sector
Oregon	Cybersecurity Specific	Decentralized	Public Sector, Private Sector
Pennsylvania	Website	Centralized	Public Sector, Private Sector, Citizens
Rhode Island	Cybersecurity Specific	Centralized	Public Sector, Private Sector, Citizens
South Carolina	A section in IT Plan	Hybrid	Public Sector
South Dakota	Website	Centralized	Public Sector, Citizens
Tennessee	Website	Centralized	Public Sector, Private Sector, Citizens
Texas	A section in IT Plan	Decentralized	Public Sector, Private Sector
Utah	Website	Centralized	Public Sector, Citizens
Vermont	A section in IT Plan	Centralized	Public Sector
Virginia	Cybersecurity Specific	Centralized	Public Sector, Private Sector, Citizens
Washington	A section in IT Plan	Centralized	Public Sector
West Virginia	Cybersecurity Specific	Centralized	Public Sector
Wisconsin	Cybersecurity Specific	Centralized	Public Sector, Private Sector
Wyoming	Website	Centralized	Public Sector, Private Sector

Source: Author calculation and Blomquist, 2020.

As Table shows, the variety is not limited to the document type. The second variation occurs in how state governments approach cybersecurity planning. Traditionally, there are two major approaches: (1) Centralized and (2) Decentralized. Based on whether the state is centralized or decentralized in terms of how they handle cybersecurity planning, the authorities who handle cybersecurity planning differ. In the centralized approach, the state cybersecurity planning is handled by either the

governor's office or state agencies, such as Department of Information and Technology and Department of Administrative Services. In the decentralized approach, the planning responsibility is delegated to local governments and the state governments play only a coordinative role. As shown in Figure 4.1, the centralized approach has a core authority whereas the decentralized approach does not have a core authority (Blomquist, 2020).

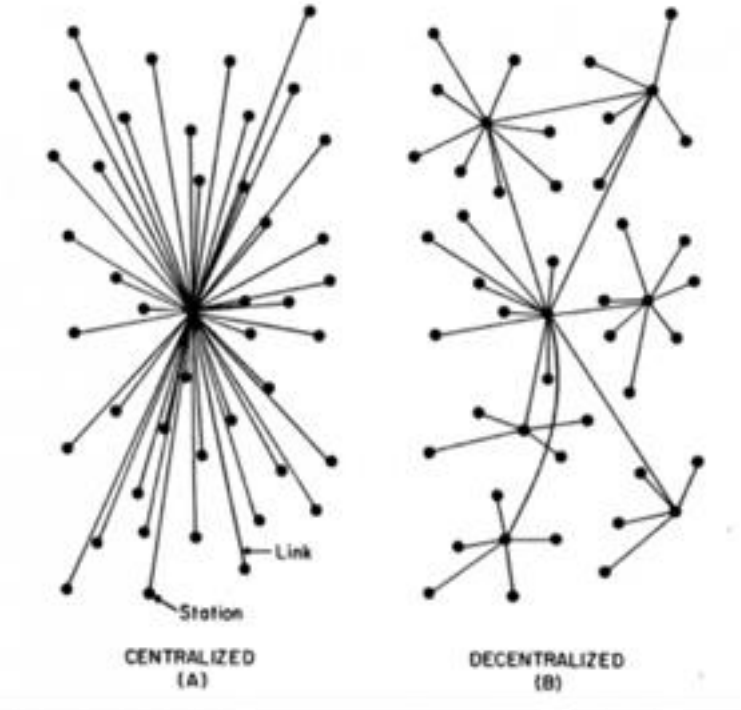

Figure 4.1 Centralized versus Decentralized System. Source: Truong et al., 2016.

There are advantages to both centralized and decentralized approaches. The centralized approach enables uniform control by establishing state-wide security standards, data access policies, and a comprehensive view of cyber threats (Blomquist,

2020; Liu et al, 2019; Center for Digital Government, 2018; Truong et al., 2016). Furthermore, centralizing cybersecurity planning advances implementation of centralized practices such as bring your own device policy, which asks employees to use their own electronic devices for their work, use of virtual private network (VPN) with more secure connections, and centralized cloud security (Blomquist, 2020; Center for Internet Security, 2020).

On the other hand, the states with the decentralized approach in both their cybersecurity planning and cybersecurity handling in general eliminate single point of failure (SPOF). In other words, the decentralized approach increases the number of required points of failure in a system crash. Thus, it significantly reduces the likelihood of entire system compromised. While agencies are still vulnerable to breaches, the states especially large ones are better protected from the spread of malicious attacks. With regards to planning specifically, the decentralized approach also allows for a more tailored cybersecurity planning that is responsive to specific local needs.

There are also disadvantages to both approaches. The centralized approach is not flexible enough to accommodate local agencies' needs and suffers from a SPOF. The decentralized approach requires a much better coordination and communication amongst agencies because each step of the planning process happens within subordinate groups. Also, the fact that there are many authorities who plan cybersecurity may result in a lack of synthesis of cybersecurity planning at the state level, leaving the cybersecurity planning at the state level fragmented, dispersed, and scattered. Thus, there is a trade-off between synthesized, uniform planning and fragmented but more responsive planning. States that combine these two approaches

are classified as *Hybrid* in Table , Column 2. The distribution among centralized, hybrid, and decentralized states show that states overwhelmingly prefer the centralized approach in handling cybersecurity planning. In contrast, only Texas and Oregon adopt the decentralized approach in handling cybersecurity planning (Blomquist, 2020).

Third, the states' cybersecurity plans target the issues of different groups. Cybersecurity at the state level is important for various actors such as citizens, private sector, local governments, and state government agencies. Hence, while some states' cybersecurity planning documents target the needs of all these groups (e.g., California, Connecticut, and Virginia), others target only a subset of them (e.g., Ohio, West Virginia, and Utah). The unique characteristics of the states determine which groups' interests and needs are addressed in the cybersecurity planning documents. Table shows the distribution of the targeted groups.

To sum up, this research has found that the data itself, i.e., state cybersecurity planning documents, varies. The document types, the responsible authorities for cybersecurity planning, and the target audiences strikingly vary amongst 50 states' cybersecurity plans. On the one hand, considering the U.S. federal system and immense differences of State cybersecurity needs, this lack of uniformity is not completely surprising. It's actually beneficial for the states to have autonomy on tailoring their cybersecurity plans specifically to their needs. On the other hand, it creates challenges in coordination of state level cybersecurity. The very existence of NIST Cybersecurity Framework is a proof of a federal effort to assist states in creating not only comprehensive cybersecurity plans, but also uniformity in state level

cybersecurity planning (NIST, 2018). Chapter 5 discusses incorporation of NIST Cybersecurity Framework in further detail.

4.3 Key Themes of Cybersecurity Plans

This research uses two main dimensions to analyze state cybersecurity planning documents. This chapter analyzes the plans based on eight themes derived from the local and state level cybersecurity literature. These themes are *funding, better equipment, leadership, training, partnership, coordination and communication, developing awareness & culture,* and *national security.*[6] Against these themes, each states' plans are examined to point out which themes they cover and in what detail they cover it. In addition to this analysis, Chapter 5 examines the plans based on criteria of the 2018 NIST Cybersecurity Framework standards, namely *identify, protect, detect, respond,* and *recover*. The next section explains each scholarly theme and their incorporation by the states' plans.

4.3.1 Training

The scholarship discusses the training theme as the education of state employees on the issues of cybersecurity conducted by the state governments or external sources such as private companies. This research operationalizes the training theme by conducting a text analysis with the following keywords: "training", "practice", "guidance", "guide", "workshop", "seminar", and "education".

The training theme is the most frequently addressed criteria with 38 states out of 50 addressing the issue in their planning documents (See Table 4.2 below). This

---

[6] Each of these themes is defined in Chapter 3.

finding is consistent with National Conference of State Legislatures (NCSL)'s website that points out: "Almost every state offers cybersecurity training for executive branch state employees. In most states, this training is voluntary." 31 of these 38 states cover the theme in detail whereas four states just acknowledge it. States that just acknowledge the importance of the theme, namely Louisiana, Washington, Minnesota, and Arizona, mention the need for training cyber experts of tomorrow, educating private and public sector employees, and strengthening privacy capacity in state government. For instance, Louisiana Cybersecurity Commission's Strategy Map just mentions that there is a need to "grow Louisiana's cybersecurity workforce and educate the public/private sectors about cybersecurity." (Louisiana Cybersecurity Commission Strategy Map, 2018, p. 1). On the other hand, 31 states pointedly plan the theme in their documents. For example, State of Illinois plans to "create and maintain comprehensive information/cyber security awareness and privacy training programs" in addition to "effective training and assist(ing) employees in obtaining applicable information security certifications." (State of Illinois Cybersecurity Strategy, 2017, p. 13).

Table 4.2 Number of States that Cover Each Theme

Theme	# of States that Address the Theme	# of States with In-depth Analysis	# of States that Acknowledge	# of States that do not Address the Theme
Training	38	31	7	12
Partnership	32	29	3	18
Coordination and Communication	31	27	4	19
Awareness & Culture	31	22	9	19
Better Equipment	27	20	7	23

Leadership	23	18	5	27
Funding	20	13	7	30
National Security	11	6	5	39

There are two major reasons for the training theme to be the most addressed criteria in states' cybersecurity plans. First, training is relatively easy and cost effective for state governments to implement. Even with simple online activities and tools, state governments can train their employees. Indeed, most of the states already provide voluntary and/or mandatory cybersecurity training for their employees.[7] However, our research demonstrates that a sizable portion of the states do not plan these trainings in their planning documents. Second, the Federal Government provides a lot of sources for state government cybersecurity training. For instance, Cybersecurity & Infrastructure Security Agency (CISA) provides resources for state governments cybersecurity training and workforce development on its website (https://www.cisa.gov/). In addition, DHS and NGA also provide resources for state cybersecurity training. These kind of resources makes states' job easier to train their employees and develop workforce with a little cost.

4.3.2 Partnership

The partnership theme refers to collaborations and cooperation with both governmental organizations such as FBI and Department of Homeland Security, and non-governmental organizations such as firms, companies, universities, and research institutes in different capacities. Partnership with the public sector, mostly at the federal level, provides guidelines, encourages better planning, and helps initiating new techniques and solutions to ever changing cybersecurity issues. Similarly, as the

[7] See the list: https://www.ncsl.org/documents/statefed/state_cybertraining_Final.pdf

private sector leads the technological innovations and their security mechanisms, creating partnerships with them is an emphasized theme in state-level cybersecurity scholarship. This research operationalizes the partnership theme by conducting a text analysis with the following keywords: “PPPs”, “public private partnership”, “university”, “institute”, “company”, “firm”, “collaboration”, “cooperation”, “business”, “alliance”, “partner”, and “corporation”.

The partnership theme is the second most frequently addressed one in state governments’ planning documents after the training theme. 32 out of 50 states covered the theme. Only three of these states (Minnesota, New Hampshire, and West Virginia) acknowledge it by identifying the venues for partnership. For instance, West Virginia’s Office of Technology Strategic Plan states a simple and broad plan for the partnership theme for cybersecurity. The plan suggests to “Strengthen working relationships with internal and external partners (MS-ISAC, Fusion Center, NASCIO, FBI, State Police, Department of Homeland Security, etc.).” (West Virginia Office of Technology, 2014, p. 6). On the other hand, the other 29 states include details about not only the institutions to cooperate with, but also cooperation areas and practices. For example, the state of Montana in its Information Technology Strategic Plan plans to “Protect information systems across the state by leveraging the public-private partnerships established by MT-ISAC to enhance information sharing, outreach, and risk awareness.” (Montana State Information Technology Services Division, 2018, p. 5.1). This quotation shows that Montana clarifies the benefits that it plans to gain with this partnership. Similarly, Mississippi plans to “maintain a partnership with a third-party forensics firm” to assist its resources “in reducing the timeframe required to

respond in the event of a major cybersecurity incident." (Mississippi Department of Information Technology Services, 2019, p. 8).

Among the states that include the partnership theme in their plans, a majority identify Federal security related organizations such as FBI, DHS, and CISA. A smaller portion of states mention potential cooperation with private security companies. And then, even smaller portion of the states plan for partnerships with education institutions such as universities, colleges, and K-12 schools. Disappointingly, a small number of states that plan for partnership with academia contradicts with the strong emphasis in the state-level cybersecurity scholarship on partnerships with academia.

4.3.3 Coordination and Communication

The coordination and communication theme refers to effective conversation and correspondence on cybersecurity planning within the state agencies, across the state agencies, and amongst local, state, and federal agencies. Thus, coordination and communication between state government agencies facilitate effective translation of newly drafted planning documents and polices. Furthermore, they are essential for effective information transmission between organizations as well as employees. This research operationalizes the coordination and communication theme by conducting a text analysis with the following keywords: "coordination", "communication", "intergovernmental", "contact", "correspondence", "conversation", "report", "publicity", "disclosure", and "briefing".

31 out of 50 States address on the coordination and communication theme in their cybersecurity plans. Four States, namely Minnesota, Missouri, New York, and West Virginia mention the importance of coordination and communication for cybersecurity without an in-depth planning for the theme. For instance, Minnesota's

Information Security Strategic Plan states that "solid relationships and ongoing communication can also help security professionals respond to incidents faster." (Minnesota IT Services, 2018, p. 7). Contrarily to these four states, there are other 27 states that make an in-depth planning for the coordination and communication theme for cybersecurity. These states emphasize communication of breach incidents, having an information center to coordinate intelligence efforts, and coordination amongst federal, regional and state institutions. As mentioned in the literature review section, creating and developing a common terminology is fundamental for effective communication and coordination. The state of Connecticut acknowledges and plans for development of a common terminology in their cybersecurity planning documents:

> Common terminology, language, procedures and values among law enforcement agencies can serve to enhance effectiveness and public confidence. As Connecticut cybersecurity officers in a dedicated investigations unit work together and with other law enforcement entities, effective communication has the same effect as in any security operation: understanding problems, priorities and orders and facilitating speedy and effective action (State of Connecticut, 2018, p. 32).

Other states argue that it is also important to have a standardized language and format to communicate with the private sector as well. For example, Mississippi's Strategic Master Plan for Information Technology plans to "develop a standardized reporting format for consistently communicating an enterprise view of the state government cybersecurity posture to stakeholders." (Mississippi Department of Information Technology Services, 2020, p. 10).

4.3.4 Developing Awareness & Culture for Cybersecurity

Sophistication of cybersecurity threats requires all state government employees and citizens to be alert and informed about the importance of cybersecurity and

potential risks. Thus, state governments aim to create a cyber aware atmosphere in which the employees as well as the citizens are equipped with relevant information about potential cyber threats and safe practices. This research operationalizes the developing awareness and culture for cybersecurity theme by conducting a text analysis with the following keywords: “culture”, “awareness”, “knowledge”, “perception”, “consciousness”, “citizen”, “information”, “recognition”, “attention”, and “alertness”.

31 out of 43 states address the awareness and culture theme. These states aim to develop a cybersecurity culture by creating awareness. According to some scholars, this is a necessary step because cybersecurity is an integral part of the information society (Malyuk & Miloslavskaya, 2016). Nine of 31 states acknowledge the themes of this theme. These states mention the importance of the theme generally, but do not go further into details about their action plans. For instance, Kansas Cybersecurity Task Force Interim Report states that “each respective government and private sector organization has a need for increased cybersecurity awareness and defense” (Kansas Cybersecurity Task Force, 2021, p. 30) and “cybersecurity aware employees are one of the most important lines of defense against cyberattacks.” (p. 19). In addition to these nine states, 22 other states plan this theme in detail. For example, Indiana Cybersecurity Strategic Plan promises to support an awareness campaign:

> Supporting a statewide cybersecurity public relations and awareness campaign designed to nurture fundamental change in culture that will make not only citizens of Indiana safer in their personal endeavors, but also the places they work as good cyber hygiene is presented, understood, and employed over time. (Indiana Executive Council on Cybersecurity, 2018, p. 27).

One common feature of States with in-depth coverage of the awareness theme is that they have websites with relevant articles, posts, and announcements about current and potential cyber threats. For example, California Department of Technology has resources that contain information on how to create a cybersafe and secure culture for individuals, small businesses, government leaders, academia, and hybrid workplaces on its website. (State of California, n.d.).

4.3.5 Better Equipment

The physical infrastructure also constitutes a key point in cybersecurity planning documents. The better equipment theme refers to the improvement of states' hardware and software assets to prevent outdated equipment causing cyber vulnerabilities. This research operationalizes the better equipment theme by conducting a text analysis with the following keywords: "equipment", "material", "hardware", "software", "update", "upgrade", "security patches", and "firmware upgrades".

Out of the 50 States, 27 States address the better equipment theme in their planning documents. 7 of these States only acknowledge the importance of the theme. These States are simply aware of the need for better equipment to protect its cyberspace; however, they do not plan how they will update/upgrade their current equipment in their planning documents in detail. For instance, in its Cyber Disruption Response and Recovery plan, the State of Oregon refers to its Vulnerability Management Program. According to the plan (2021), the program "notifies members on a monthly basis about any outdated software that could pose a threat to assets." (p. 13). However, the plan does not point out how they should update these outdated software or install newly needed equipment. Contrary to the states that acknowledge

the importance of the better equipment theme, the other 20 States plan this theme thoroughly by giving details about how they overcome this issue. For example, New Mexico's Status of Cybersecurity Memorandum states that "the $6 million will be used to purchase and install new equipment" (Garcia, 2020, p. 6) by state agencies in consultation with DoIT.

Having an outdated software or out-of-date equipment may cause serious cybersecurity issues. Even though scholarly literature (Caruson et al., 2012; Karakoç, 2017; Macmanus et al., 2013; Spidalieri, 2015) and reliable reports from the private sector (Deloitte and National Association of State Chief Information Officers (NASCIO), 2012, 2014, 2016, 2018; Ponemon Institute, 2015) indicate that state government agencies need better equipment to fight against cyberattacks, our analysis shows that most of the States do not take action on this issue in their planning documents.

4.3.6 Leadership

Administrative structure and authority allocation are significant to clarify the management mechanisms of state government organizations. State governments with a proactive cybersecurity leadership are more likely to be efficient in managing cybersecurity. The leadership theme refers to both a clear identification of responsibility allocation and a determined commitment to improve states' cybersecurity posture with new initiatives, ideas, and partnerships. This research operationalizes the leadership theme by conducting a text analysis with the following keywords: "leader", "leadership", "hierarchy", "top-down", "bottom-up", "directing", "authority", "manager", "management", "proactive", and "motivation".

Leadership is one of the most emphasized themes in the cybersecurity literature at the State level. 23 out of 50 States focus on this theme in their planning documents. Five of these 23 States acknowledge the issue whereas 18 of them include a clear designation of leadership responsibilities for cybersecurity policies and programs in their plans. The 5 states explain the benefits of a top-down leadership approach and a cooperation between government and business leaders. They also mention the costs of a lack of an effective leadership on cybersecurity. For instance, in its Cybersecurity Plan (2020), the State of Missouri's Office of Administration acknowledges the importance of leadership by mentioning "without determined leadership, cyber security will continue to be perceived as a burden that is unnecessarily placed on state employees by IT staff that don't understand" (p. 6).

However, acknowledging the importance of the leadership theme in a plan is not the same as describing leadership responsibilities. One of the clearest examples of the in-depth coverage of leadership comes from Delaware. Delaware's Statewide Information Technology Strategic Plan explicitly identifies the Department of Technology and Information's pioneering role in promoting the state's cybersecurity: "The Delaware Department of Technology and Information will take a leadership role across the state to deliver programs and services by advancing new ideas and pursuing collaborative partnerships." (2016, p. 24).

One of the potential reasons for many of the states to not include the leadership theme in their plans is the lack of established practices in allocating cybersecurity responsibilities. While the departments of information and technology usually appear as the "leader" in leading cybersecurity efforts, in most of them, there are not further specifics about the hierarchical distribution of roles within and across the

department(s). An exception to this is Vermont's Agency of Digital Services (ADS) 2019 Strategic Plan which lays out the role and responsibilities of newly hired CISO: "the CISO will participate in ongoing cybersecurity initiatives, as well as develop new initiatives for statewide cybersecurity." (p. 14).

4.3.7 Funding

In cybersecurity planning, the discussion of how to allocate the budget and how to increase funding are amongst the most significant issues to improve cybersecurity posture. Thus, some states discuss cybersecurity cost analysis, investment plans, and allocation of the state budget on different cybersecurity related expenses. This research operationalizes the funding theme by conducting a text analysis with the following keywords: "budget", "funding", "money", "cost", "fund(s)", "expenses", "finance", and "resources".

Out of 50 states, 20 states address the issue of funding. Amongst these 20 states, 7 of them acknowledge the importance of funding while 13 of them also identify a specific action plan to improve cybersecurity funding. The acknowledgement of the theme either identifies future resources to contribute to cybersecurity spending or mentions a generic increase in the investment of cybersecurity (See Table). For instance, Vermont's cybersecurity planning document states that they will "continue to grow our (their) investment in cybersecurity." (Vermont Agency of Digital Services, 2021, p. 9). In contrast, the in-depth coverage specifies the ways in which the state government will increase funding for cybersecurity and/or promote efficient use of cybersecurity budget. For example, the State of Montana plans to "perform a cybersecurity cost analysis for the State of

Montana, including investment recommendations." (Montana State Information Technology Services Division, 2018, p. 5.1).

The relatively few numbers of states that address the funding theme in their plans is surprising because, as it reviewed in Chapter 2, the scholarly literature on state and local level cybersecurity primarily focuses on this issue. The low budget spared for cybersecurity has been identified as one of the key barriers in improving state-level cybersecurity posture (Caruson et al., 2012; Davis et al., 2016; Karakoç, 2017; Macmanus et al., 2013; Norris et al., 2019). For instance, Connecticut allocates as low as 1 percent of its IT budget to cybersecurity (Bergal, 2017). In Connecticut's 2018 Cybersecurity Update, they include a budget request from the Department of Administrative Services to fund a program of targeted improvements (Currey et al., 2018). Thus, a small portion of states including Connecticut actively seek ways to improve their funding in their planning documents. However, counter intuitively, the planning documents of the majority of the states do not address this issue in great detail.

4.3.8 National Security

Past experiences and cases show that foreign cyberattacks can target state governments' cyberspace. For instance, election data stored by the state governments were breached by foreign state sponsored cyber-attacks. For this reason, some state governments include the national security context in their planning documents. This research operationalizes the national security theme by conducting a text analysis with the following keywords: "nation", "federal", "national-security", "country", "international", "foreign", "Russia", "China", and "defense".

The national security theme is addressed by the fewest number of states, 11 out of 50. Amongst these 11 states, 6 of them simply acknowledge the relationship between state and national level cybersecurity. In contrast, other 5 States provide details of the issue, and explain their action plan in concrete and specified terms. For instance, West Virginia, in its Cybersecurity Workforce Strategic Initiative Report, acknowledges that cybersecurity has a national security aspect but does not go into details about how this national security aspect will play a role in their planning: "Cyber threats facing the United States come from several primary sources: international governments, criminal elements and individual hackers." (TechConnect, 2019, p. 13). The discussion of the national security aspect of the issue remains limited to this quote and it shows an approach by simply acknowledging potential international cyber threats. In contrast, Connecticut spares paragraphs to discuss several ways in which national security relates to this state governments' cybersecurity plans. For example, it discusses the issue of fake news and manipulation as a consequence of international cyber-attacks and defines an action plan:

> National security officials warn that an attack by a nation state on state systems or critical infrastructure would most likely include disinformation, rumors and messages to instill panic and thwart order. Governor must have considered, ahead of time, and perhaps already composed, messages to pre-empt "fake news" and/or reassure the public with instructions and updates (Malloy, 2017).

The low coverage of the national security theme in States' planning documents is not a surprise for many scholars because national security is mostly a federal government responsibility. However, states engage in this area when they operate in congruence with the federal government. Thus, state plans appropriately should address the interconnection of responsibilities.

4.4 Cross-state Analyses

After the theme-based analysis of states' cybersecurity planning documents, the next two sections of this chapter engage in cross-state analyses to categorize states based on their planning documents' level of coverage. This cross-state analysis reveals exemplary states with comprehensive and in-depth plans regarding the eight scholarly themes.

4.4.1 Level of Depth

The first step of the planning document analysis focuses on the depth of the plans in their discussion of the predetermined themes. A theme can be simply acknowledged in a planning document. This refers to the case where a state cybersecurity planning document recognizes the presence of the issue by mentioning the theme. Alternatively, a theme can also be discussed in a planning document with details of the issue, and an action plan in concrete and specified terms. If a planning document both acknowledges a theme and explains how it is going to be addressed, I consider that theme as analyzed in-depth. So, this research codes how state cybersecurity planning documents address the scholarly themes in two dimensions: (1) acknowledgement and (2) in-depth. Table provides examples to illustrate the logic of analysis.

Table 4.3 Examples from Planning Documents

Scholarly Theme	**Acknowledgement**	**In-Depth**

Funding	**Kansas:** Identify ways to pool cybersecurity funding to build on economies of scale and reduce duplicate efforts (Kansas Cybersecurity Task Force, 2021, p. 13)	**Rhode Island**: Work with RIEMA (Rhode Island Emergency Management Agency) to request more funding and assets to support cyber training within the state (State of Rhode Island, 2019, p. 23).
Better Equipment	**Oregon**: Vulnerability Management Program (VMP) - VMP notifies members on a monthly basis about any outdated software that could pose a threat to assets (State of Oregon Enterprise Information Services, 2021, p. 13).	**Iowa**: Review and remediate legacy software and develop future plans OCIO working with agency/county application teams will review and remediate legacy software for potential cybersecurity risk and develop plans to replace, upgrade or decommission the software (State of Iowa, 2019, p. 5). **New Mexico**: The project plan states the $6 million will be used to purchase and install new equipment, however, is there a need for additional equipment if DoIT is only hosting applications for seven of 67 state agencies and leasing space for 27. State agencies should consult and evaluate DoIT's service offerings prior to expending state resources outside of the state on things such as cloud storage, and other hosting scenarios (Garcia, 2020, p. 6).

Leadership	**Missouri**: Without determined leadership, cyber security will continue to be perceived as a burden that is unnecessarily placed on state employees by IT staff that don't understand "what needs to get done (Missouri Office of Administration, 2020, p. 6).	**Louisiana**: Establish a Cybersecurity Commission to advance the State's cyber ecosystem and position Louisiana as a national leader and preferred location for cyber business, education, and research (Louisiana Cybersecurity Commission, 2018, p. 1). **Delaware**: The Delaware Department of Technology and Information will take a leadership role across the state to deliver programs and services by advancing new ideas and pursuing collaborative partnerships (Delaware Department of Technology and Information, 2016, p. 24).
Training	**Louisiana**: Grow Louisiana's cybersecurity workforce and educate the public/private sectors about cybersecurity (Louisiana Cybersecurity Commission, 2018, p. 1).	**Alabama**: Implement Statewide Specialized Cyber Security Training in line with Alabama IT Security Program Plan (Alabama Office of Information Technology, 2017, p. 12). **Illinois**: Create and maintain comprehensive information/cyber security awareness and privacy training programs (Department of Innovation and Technology, 2017, p. 11).

Partnership	**West Virginia:** Strengthen working relationships with internal and external partners (MS-ISAC, Fusion Center, NASCIO, FBI, State Police, Department of Homeland Security, etc.) (West Virginia Office of Technology, 2014, p. 6).	**Connecticut**: Emergency management participants will need to anticipate unprecedented shortages and be prepared to identify actions necessary to alleviate them, including collaboration with the private sector, municipal governments, Connecticut state agencies, other states and federal agencies (State of Connecticut, 2018, p. 36). **Montana**: Protect information systems across the state by leveraging the public-private partnerships established by MT-ISAC to enhance information sharing, outreach, and risk awareness (Montana State Information Technology Services Division, 2018, p. 5.1)..
Coordination and Communication	**Minnesota**: Solid relationships and ongoing communication can also help security professionals respond to incidents faster (Minnesota IT Services, 2018, p. 7).	**Maryland**: Develop a cyber incident response plan to coordinate federal, state, local, and private sector activities and manage the risks associated with an attack or malfunction of critical information technology systems within the State (Governor's Office of Homeland Security, n.d., para. 9).

		Wisconsin: Describing the coordination structure that integrates the various cybersecurity governance teams (Senior Policy Advisors Group, Cybersecurity Management Team, and the Wisconsin Cyber Disruption Response Advisory Group) (Wisconsin Department of Administration, 2017, p. 7). **New Jersey**: Develop an interactive web portal for cybersecurity communications and information sharing with NJCCIC members. (New Jersey Office of Homeland Security, 2016, p. 16).
Awareness - Culture	**Kansas**: Each respective government and private sector organization has a need for increased cybersecurity awareness and defense (Kansas Cybersecurity Task Force, 2021, p. 30). **New Jersey:** Champion and grow a culture of cybersecurity and privacy across executive branch departments and agencies (New Jersey Office of Homeland Security, 2016, p. 9).	**Michigan**: The state developed a comprehensive cybersecurity strategy that addressed threats in 2011, and our new three-pronged approach to changing culture was an essential element to our risk reduction approach (State of Michigan, 2015, p. 8).

		Indiana: Supporting a statewide cybersecurity public relations and awareness campaign designed to nurture fundamental change in culture that will make not only citizens of Indiana safer in their personal endeavors, but also the places they work as good cyber hygiene is presented, understood, and employed over time (Indiana Executive Council on Cybersecurity, 2018, p. 27).
National Security	**Hawaii**: Among state actors, China and Russia are of particular concern. As indicated in the October 2011 biennial economic espionage report from the National Counterintelligence Executive, entities within these countries are responsible for extensive illicit intrusions into U.S. computer networks and theft of U.S. intellectual property (State of Hawaii, 2012, p. 9).	**Florida**: This triumphant event served as a platform for the Center to establish stronger relationships with key players in the international cybersecurity world and to communicate our intention to have an active voice in this space. We continue to build these relationships with military and federal partners who share our commitment to improved national cybersecurity, enabling the Center to contribute to the national policy conversation, reach a broader audience, and further position Florida as a national leader in cybersecurity policy, research, education, and employment (The Florida Center for Cybersecurity, 2020, p. 16).

		Oregon: CTIIC also provides integrated all source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests (State of Oregon Enterprise Information Services, 2021, p. 13).

The examples demonstrate the distinction between an acknowledged theme and a theme that is analyzed in-depth. For instance, the *funding* theme is addressed by both Kansas and Rhode Island's cybersecurity planning documents. In the State of Kansas' plan, there is a goal to bring together cybersecurity funding resources; however, the exact mechanisms and ways are not clarified. In contrast, Rhode Island specifies the agency that they will request more funding and assets from. Similarly, the state of Missouri acknowledges the critical role of determined leadership in cybersecurity but does not lay out how to establish it. On the other hand, Louisiana takes action to establish a commission that clearly has the leadership role in managing state cybersecurity. Finally, the *coordination and communication* theme is acknowledged by mentioning its potential role in expediting responses to cyber incidents in the Minnesota's plan. In addition to this acknowledgement, New Jersey goes one step further and plans developing a web portal in order to advance communication.

4.4.2 Level of Coverage

In terms of the predetermined themes derived from the scholarship, there is a variation in states' coverage of the themes. While some state cybersecurity planning documents address all of the themes in-depth, there are others that mention none of them. The level of coverage is calculated based on how many predetermined themes, derived from the literature, are addressed in the planning documents in detail for each state. This analysis shows both the comprehensiveness and the depth of the planning documents with respect to the predetermined themes. Four categories emerge out of this distribution. States with planning documents that acknowledge 6 to 8 predetermined themes are called "High Coverage States," 4 or 5 predetermined themes are called "Moderate Coverage States," 2 or 3 predetermined themes are called "Low Coverage States," and 0 and 1 predetermined themes are called "Minimal Coverage States". At this stage, the analysis considers the number of in-depth themes as the criteria for coverage. Table 4.4 categorizes states based on how comprehensive their cybersecurity planning documents are with respect to eight scholarly themes.[8] The themes that are just acknowledged in the planning documents are excluded from the level of coverage analysis.

---

[8] For instance, Table demonstrates that the State of Louisiana's plan just acknowledges the *training* theme: "…grow Louisiana's cybersecurity workforce and educate the public/private sectors about cybersecurity…" (Louisiana Cybersecurity Commission, 2018, p. 1) whereas the same document covers the *leadership* theme with a specific action plan: **"**Establish a Cybersecurity Commission to advance the State's cyber ecosystem and position Louisiana as a national leader and preferred location for cyber business, education, and research." (p. 1). Thus, in comparing states, this analysis counts only the number of in-depth themes for each state.

Table 4.4 States categorized based on level of coverage.

Minimal Coverage (0-1)	**Low Coverage** (2-3)	**Moderate Coverage** (4-5)	**High Coverage** (6-8)
Alaska Arkansas Idaho Louisiana Maine Minnesota Nebraska New Hampshire Ohio Oklahoma Pennsylvania South Carolina South Dakota Tennessee Utah Washington Wyoming	Arizona Colorado Hawaii Kentucky Maryland Massachusetts Missouri Nevada North Dakota West Virginia	Alabama Indiana Kansas Michigan Mississippi New Jersey New York Wisconsin	California Connecticut Delaware Florida Georgia Illinois Iowa Montana New Mexico North Carolina Oregon Rhode Island Texas Vermont Virginia

Table 4.4 shows that a big portion of states are in the minimal coverage category as they address either none or one scholarly themes in-depth. Many of the minimal coverage states do not have a separate cybersecurity specific document, instead their official website has some information about their cybersecurity plans. The low and moderate coverage states have cybersecurity specific plans or a section in IT security plans, but they are not as comprehensive as the high coverage states. The states that address six or more themes in-depth are the most successful states in terms of cybersecurity planning. The states in the high coverage category are also most compliant with the NIST Cybersecurity Framework, with Connecticut, Rhode Island, and Virginia being the model states (see Chapter 5).

One important theory that explains cross-state variations is the political culture theory of Daniel Elazar. The theory explains political ideologies, legislative activities, and actions of state governments based on socio-political culture of the citizens of the states. The analysis finds that all three political cultures are almost equally distributed in all four categories.[9] This is a surprising result as political culture is considered a major factor that explains states' activities such as planning.

[9] In the minimal coverage category, 5 out of 18 states are individualistic, 6 of them are traditionalistic, and 7 of them are moralistic states. In the low coverage category, there are 5 individualistic, 3 traditionalistic, and 2 moralistic states. In the moderate coverage category, there are 3 individualistic, 2 traditionalistic, and 3 moralistic states. In the high coverage category, there are 4 individualistic, 6 traditionalistic, and 5 moralistic states. Thus, there is no meaningful correlation between political culture distribution and level of coverage distribution.

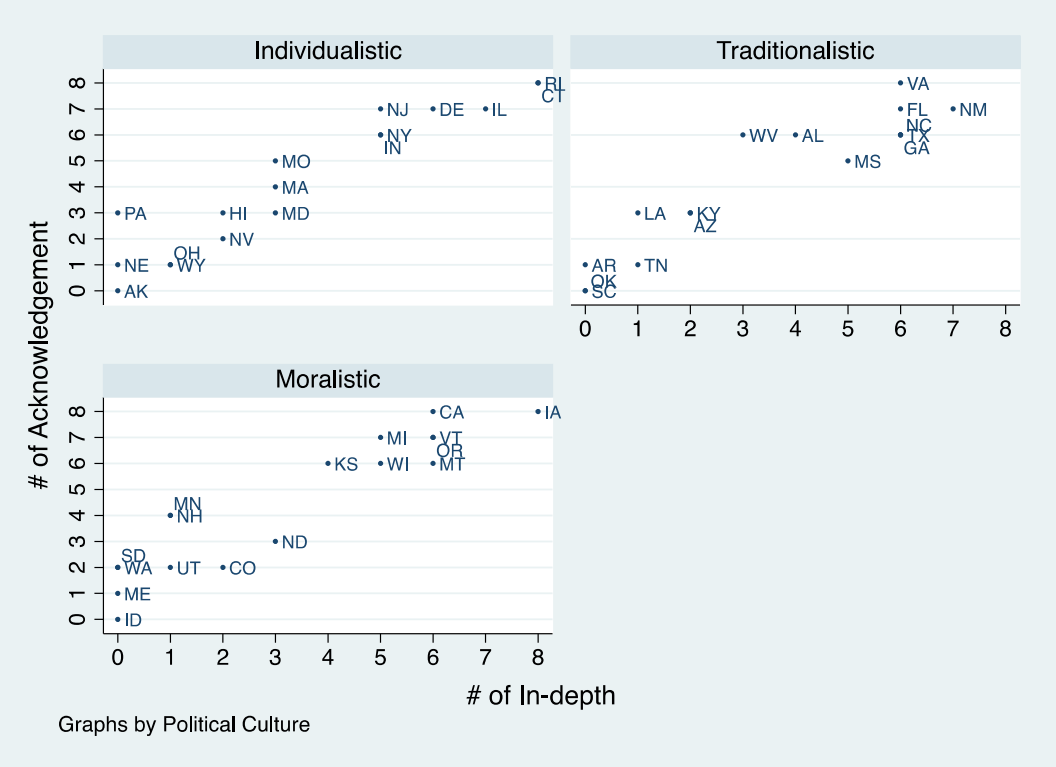

Figure 4.2 Scatter plot analysis of States based on scholarly themes and political culture. Source: Author's calculation.

Figure 4.2 illustrates the correlation between the number of acknowledged themes and the number of in-depth themes. As mentioned earlier, states that have comprehensive (high coverage) cybersecurity planning documents also incorporate action plans for addressing those themes (in-depth). Moreover, the approximately fare distribution of both well-functioning and poor cybersecurity planning documents into three political culture categories supports the null finding between political culture and state cybersecurity planning coverage with respect to eight scholarly themes.

Another finding from the cross-state analysis of scholarly theme coverage shows that some of these themes go together in the planning documents. Table

demonstrates that the highest correlation (0.7893) exists between the *partnership* and *coordination and communication* themes.

Table 4.5 Correlation Among the Coverage of Eight Scholarly Themes

	funding	better equipment	leadership	training	partnership	coordination & communication	awareness & culture	national security
funding	1							
better equipment	0.275	1						
leadership	0.322	0.3355	1					
training	0.451	0.3612	0.3914	1				
partnership	0.3619	0.5644	0.4543	0.4712	1			
coordination & communication	0.3363	0.4909	0.3506	0.474	0.7893*	1		
awareness & culture	0.4367	0.5305	0.4881	0.6505*	0.6175*	0.6207*	1	
national security	0.5368	0.1909	0.38	0.3657	0.3189	0.2259	0.3891	1

Note: * R>0.6. Correlations are estimated with Pearson R.

In many planning documents, *coordination and communication* is addressed right after the discussion on *partnerships*. For instance, the State of Georgia's official website on cybersecurity states that:

> the second annual virtual Georgia Cyber Summit brought together partners in federal and state government and private industry to build cyber knowledge. The sharing of information is crucial to the common defense of critical infrastructure and applications for the state of Georgia. (Georgia Technology Authority, n.d.))

Similarly, the *awareness and culture* theme go hand in hand with the *training* theme (r=0.6505) as many of the training programs aim to create awareness. For example, State of Iowa Cybersecurity Strategy states that:

> The ISO distributes Security News about emerging cyber-threats and security best practices to 1500+ individuals annually in the public and private sectors and hosts in-person cybersecurity training sessions for state and local government and educators. Online security awareness training was made available to K-12 educators and public librarians to help raise awareness about the importance of good cybersecurity practices. (State of Iowa, 2016, p. 16).

The other two high correlations emerge (1) between the *awareness* theme and the *partnership* theme and (2) between the *awareness* and *coordination and communication* theme.

4.5 Conclusion

This chapter primarily provides a landscape of state-level cybersecurity planning. This unique contribution brings together 50 states and their different practices in planning cybersecurity. The chapter, first, analyzes the state level cybersecurity planning documents and finds a great variation in terms of the document types, centralization level in approaching cybersecurity planning, and targeted groups.

Furthermore, this chapter conducts the first step of analyzing the incorporation of best practices in cybersecurity planning by applying the eight scholarly themes to cybersecurity planning documents. The chapter finds that the *training* and *partnerships* themes are the most frequently addressed scholarly criteria with 38 and 32 states addressing the issue in their planning documents, respectively. Educating state officials on cybersecurity is a cost-effective and convenient strategy which might explain the frequency of the *training* theme in state cybersecurity documents. The theme-based analysis also finds that the *funding* and *national security* themes are the least mentioned scholarly criteria in the planning documents. The reason behind relatively low number of state plans that address the *national security* theme is due to states not perceiving national cybersecurity beyond their responsibility.

Moreover, the cross-state analysis distinguishes acknowledgement and in-depth analysis of a theme to categorize states into minimal, low, moderate, and high coverage states based on the number of in-depth themes. The analysis points out that most of the states address either none or one scholarly theme in their planning documents. These states also lack a cybersecurity specific separate planning document. According to the results, the high coverage states both acknowledge most of the scholarly themes and incorporate action plans for addressing those themes. The cross-state analysis also finds that some of the themes go together in the planning documents. A high correlation (0.7893) exists between the *partnership* and *coordination and communication* themes. Similarly, the *awareness and culture* theme go hand in hand with the *training* theme (r=0.6505) as many of the training programs aim to create awareness. The other two high correlations emerge between (1) the

awareness and the *partnership* themes and (2) the *awareness* and *coordination and communication* themes.

Finally, the chapter finds that the political culture theory does not have a significant explanatory power towards state cybersecurity planning practices because all three political cultures are almost equally distributed to minimal, low, moderate, and high coverage categories. This is a surprising result as political culture is considered a major factor that explains states' activities such as planning. The second step of analyzing the best practices, which is to examine the incorporation of the NIST Cybersecurity Framework Functions, is the main focus of Chapter 5.

Chapter 5

INCORPORATION OF NIST CYBERSECURITY STANDARDS

This chapter analyzes the extent to which cybersecurity planning documents of states incorporate the best practices as defined by the 2018 NIST Cybersecurity Framework. The framework is considered a guidance to improve the nation's critical infrastructure; however, it can also be adopted by any size of companies and organizations across different sectors in addition to federal, state, and local governments (NIST, 2018, p. v). As discussed in Chapter 3, this research considers the NIST framework as standards of best practice because many scholars, policy makers, and NIST itself concur that the framework is a useful guidance to state governments to improve their cybersecurity posture. This chapter first defines each NIST function and then describes how these functions were coded in the analysis of state planning documents. The chapter reports the results of a text analysis of the incorporation of NIST Cybersecurity Framework Functions within the cybersecurity planning documents of the states. The analysis continues with an examination of cross-state variations in terms of incorporation of NIST Cybersecurity Framework functions. Finally, it discusses the most common best practices of model states.

5.1 Conceptualization Of NIST Cybersecurity Framework Functions

There are 5 NIST functions that define best practices in cybersecurity planning: (1) *identify*, (2) *protect*, (3) *detect*, (4) *respond*, and (5) *recover*. The NIST Cybersecurity Framework defines the *identify* function as: "Developing the

organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities." (NIST, 2018, p. 46). In other words, state cybersecurity plans are expected to describe their assets, including data, personnel, devices, and systems; their governance, including policies and procedures; and their risk assessments. The second function, *protect*, is defined as "developing and implementing the appropriate safeguards to ensure delivery of critical infrastructure services." (p. 46). Specifically, the protect function requires elaboration on data security management, information protection processes, and protective technical security solutions. The third function, *detect*, is defined as "developing and implementing the appropriate activities to identify the occurrence of a cybersecurity event." (p. 46). Particularly, the detect function focuses on detection mechanisms and monitoring of anomalies and incidents. The fourth function, *respond*, is defined as "developing and implementing the appropriate activities to take action regarding a detected cybersecurity event." (p. 46). Thus, the planning documents need to explain their response processes, ways to improve their coordination and communication for effective response activities in order to fulfill the *respond* function. Finally, the fifth function, *recover*, is defined as "developing and implementing the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event." (p. 46). This final stage focuses on the aftermath of a cyber incident, and state governments are recommended to plan for their restoration activities and incorporating lessons learned into future activities.

The NIST Cybersecurity functions can overlap with, but essentially are different from the scholarly themes. While the scholarly themes refer to specific areas of cybersecurity planning, the NIST functions cut across those specific action areas. In

other words, the NIST functions intended to describe the key elements of a cybersecurity planning system while the scholarly themes are action areas within that system. For instance, the *protect* function of NIST Cybersecurity Framework involves systemic guidelines that are relevant for multiple scholarly themes such as awareness, training, and better equipment. Raising cyber awareness, training state officials, and adopting proactive technology are all specific action areas for the *protect* function to be fulfilled.

5.2 Operationalization of NIST Cybersecurity Framework Functions

Each of these functions are coded as present when the planning documents include the categories derived from NIST Cybersecurity Framework. Table 5.1 shows the coding keywords for each function. These keywords are sourced from the NIST Cybersecurity Framework categories.[10] For instance, to code the *identify* function, this project searches for the term "identify" and the categories of the *identify* function, namely: "asset management, business environment, governance, risk assessment, risk management strategy, and supply chain risk management." The research analyzes if the planning document discusses any of these keywords. If there is a discussion and it aligns with the definitions of the functions mentioned above, then, the planning document is coded as "1" for the *identify* function. If none of these keywords are mentioned, or their discussion is in a different context, then, that planning document is coded as "0" for the *identify* function. The same process is applied to all 5 functions.

[10] The NIST Cybersecurity Framework categories which are used as keywords for the applied text analysis and their descriptions are provided in Table 3.2.

Table 5.1 Coding NIST Cybersecurity Framework Functions.

Function	Keywords
Identify	identify, asset management, business environment, governance, risk assessment, risk management strategy, supply chain risk management
Protect	protect, identify management and access control, awareness and training, data security, information protection process and procedures, maintenance, proactive technology
Detect	detect, anomalies and events, security continuous monitoring, detection processes
Respond	respond, response planning, communications, analysis, mitigation, improvements
Recover	recover, recovery planning, improvements, communications

Based on the conceptualization and operationalization of the NIST Cybersecurity Framework Functions, the next section discusses the coverage of these functions and their frequency amongst 50 States' cybersecurity planning documents.[11]

5.3 Incorporation of NIST Cybersecurity Standards

This section analyzes how the cybersecurity planning documents of 50 States address the NIST Cybersecurity Framework functions. For each function, the section, first, explains the coverage of these functions. After then, the section provides examples from planning documents to further unpack their incorporation by the plans.

The *identify* function is the most consistently addressed NIST item in the planning documents of the states. Thirty-seven out of 50 states refer to this function in their planning documents. It is not surprising that the *identify* function is the most

[11] In contrast to Chapter 4, this chapter analyzes the coverage of NIST Cybersecurity Framework functions without categorizing acknowledgement versus in-depth. This is due to the nature of the framework functions as ideal typification.

frequently addressed because it is typically the first step of the cybersecurity planning process (NIST, 2018). In addressing the *identify* function, states point out their critical assets, potential risks and threats, and the role of governance in their cybersecurity planning documents. For instance, the Information Assurance and Cyber Security Strategic Plan of Hawaii plans for risk assessment to identify the most critical assets: "Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important" (State of Hawaii, 2012, p. 16). In addition, Kansas Cybersecurity Task Force Interim Report focuses on identifying the role of governance in improving cybersecurity in the state of Kansas: "The Task Force is charged with identifying and developing actionable recommendations to approach cybersecurity with a "whole-of-state" concept…Identify key needs and develop components for a holistic statewide strategic plan for advancing cybersecurity in the State of Kansas" (2021, p. 7). Typically, when state plans address *identify* function they describe their assets, resources, and various sources of risks to those assets.

The second function, *protect*, is addressed by 33 out of 50 States. The *protect* function requires an analysis of states' efforts to enhance data security, protective technologies, and information protection processes and procedures. The number of states that address the *protect* function is fewer compared to the states that address the *identify* function. In their cybersecurity planning documents, States generally identify their assets before discussing how they protect these assets. Hence, it is plausible to see fewer states addressing the *protect* function. Some states focus on information protection processes and procedures, such as West Virginia:

> The Office of Technology is currently in an exploratory stage of implementing a network access control (NAC) solution. The goal of

> this solution is to provide the ability to prevent end-stations that lack updated antivirus, latest patches, or other required protection software from accessing the network and placing other computers at risk (West Virginia Office of Technology, 2014, p. 8).

Furthermore, other states like Texas emphasize data security and specifies tools and strategies for effective protection of confidential and sensitive data (Texas Department of Information Resources, 2022, p.7).

One of the least addressed NIST Cybersecurity Framework function is *detect* in states' cybersecurity planning documents. There are only 25 states that acknowledge the *detect* function in their plans. Thus, planning for better detection systems and improving detection capabilities is not addressed by the majority of the states. This might be the case either because detection requires a constant monitoring prior to a cyber attack or because states don't consider detection a state responsibility. The states that address the *detect* function focus on how to notice anomalies, monitor security, and improve detection processes. For instance, the State of Oregon plans to "…detect the introduction of malicious code and unauthorized mobile code and to protect the integrity of software and information" (Oregon Enterprise Security Office, 2018, p. 39). In addition, Michigan aims to improve detection capabilities in support of the Presidential Inauguration: "Michigan National Guard provides intrusion detection capabilities and skillsets to four Joint Incident Site Communications Capabilities deployed throughout the National Capital Region in support of the Presidential Inauguration" (State of Michigan, 2015, p.19).

Thirty-three out of 43 states acknowledge the *respond* function of the NIST Cybersecurity framework. The *respond* function is also an important aspect of cybersecurity planning as it lays out the immediate reaction to a cyber incident. In explaining their response mechanisms, States focus on response planning,

communications, mitigation of the damage of the incident, and analysis of root causes enabled cyber attacks. For instance, Minnesota's Information Security Strategic Plan (2018) aims to simplify and normalize response processes to reduce timeframe required to respond. It also acknowledges the significance of solid relationships and ongoing communication in helping security professionals to respond cyber incidents faster (Minnesota IT Services, p.7). In addition, Hawaii's Information Assurance and Cyber Security Strategic Plan (2012) emphasizes the mitigation of the damage and analysis of root causes: "When systems are affected by a security event, administrators must be ready to respond as efficiently as possible to limit the damage, determine the root cause, and get the system back up and running quickly" (p. 44). Some of the states focus on timeframe and quickness whereas others emphasize mitigation of damages from cyber attacks. Overall, state cybersecurity planning documents refer to an immediate reaction to a cyber incident when they consider the *respond* function.

The last function of NIST cybersecurity framework, *recover*, is addressed in only 25 states' cybersecurity planning documents out of 50. Along with the *detect* function, the *recover* function is also not addressed by the majority of the states.[12] The states that address the *recover* function focus on restoration activities in coordination with internal and external parties (NIST, 2018). For instance, North Carolina plans to coordinate with 16 state, local and academic institutions with incident response (IR) support, remediation and recovery. The state also plans for funding and supporting the National Guard's North Carolina Assessment and Assist Team's incident recovery

[12] Recovery requires a long term planning after the incident. It is also costly to return to pre-incident conditions. These might be the reasons for the majority of state cybersecurity planning documents to not address the *recovery* function.

efforts (North Carolina Department of Information Technology, 2020, p. 24). Similarly, Florida plans to "assist state and local efforts to return the community to pre-incident levels" (Domestic Security Oversight Council, 2020, p. 8).

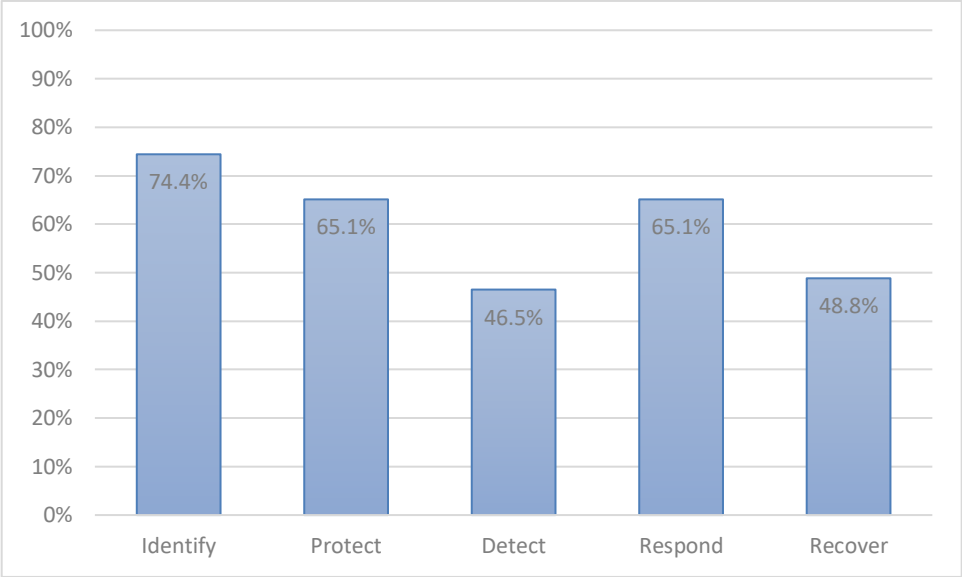

Figure 5.1 The percentages of States that cover each NIST Cybersecurity Framework Function.

Figure 5.1 demonstrates that most States address *identity*, *protect*, and *respond* functions in their plans whereas than half of the States address the *detect* and *recover* functions as well. This result indicates an overall alignment with the NIST Cybersecurity Framework. The relative smaller number of states to address the *detect* and *recover* functions point out the particular difficulties of these stages. The uncertainty that comes with constant sophistication of cyber attacks complicate the detection and recovery stages the most. States might not know how to plan for the detection of or recovery from cyber attacks with unknown techniques. Whereas for

other functions there is an element of familiarity with the available assets, common protection practices, and immediate response strategies. The most substantive implication of not addressing the *detect* function is the overall unreadiness for cyber incidents and potentially higher costs of attacks as some will remain undetected for a while. Similarly, not addressing the *recover* function causes a lack of preparation to anticipate ways to regain the lost data, repair the infrastructure, and address other damages from the cyber incidents.

Some NIST Cybersecurity Framework functions go hand in hand together. Table 5.2 below shows the correlation between planning documents' coverage of each framework function. The highest correlation coefficient (R=.6372) is between the *protect* and *recover* functions. Table 5.2 illustrates that some states do not address the *identify* function address other functions, and this is valid for all five functions, because no correlation coefficient approaches to 1.

Table 5.2 The Correlation Table of NIST Cybersecurity Functions

	Identify	Protect	Detect	Respond	Recover
Identify	1				
Protect	0.5054	1			
Detect	0.4782	0.387	1		
Respond	0.5054	0.566	0.387	1	
Recover	0.4782	0.6372	0.4391	0.5538	1

The next section focuses on the cross-state variation in the coverage of the NIST Cybersecurity Framework functions.

5.4 Cross-state Analysis of Cybersecurity Planning documents in terms of NIST Cybersecurity Framework Functions

Most States acknowledge NIST Cybersecurity Framework functions, albeit to a different degree. Table 5.3 categorizes states based on the number of functions they address out of 5 NIST Cybersecurity Framework functions. Some states such as Kentucky and Ohio do not mention any of the 5 functions in their cybersecurity plans whereas others such as Connecticut and Rhode Island address all of them. The binary code of each NIST Cybersecurity Framework function in state cybersecurity planning documents is provided in the table below.

Table 5.3 Binary Code of State Cybersecurity Planning Documents' Incorporation of NIST Cybersecurity Framework Functions

State	Identify	Protect	Detect	Respond	Recover
Alabama	1	1	0	1	0
Alaska	0	0	0	0	0
Arizona	0	0	1	0	0
Arkansas	0	0	0	0	0
California	1	1	1	1	0
Colorado	1	0	1	1	0
Connecticut	1	1	1	1	1
Delaware	1	1	0	0	1
Florida	1	1	0	1	1
Georgia	1	1	1	0	0
Hawaii	1	1	1	1	0
Idaho	1	0	0	0	0
Illinois	1	1	1	1	1
Indiana	0	1	0	1	1
Iowa	1	1	1	0	1
Kansas	1	1	0	1	0
Kentucky	0	0	0	0	0
Louisiana	1	0	1	0	0
Maine	0	0	0	0	0

Maryland	1	1	1	1	1
Massachusetts	1	1	0	0	0
Michigan	1	1	1	1	1
Minnesota	1	1	1	1	1
Mississippi	1	1	1	1	1
Missouri	0	1	0	1	0
Montana	1	1	1	1	1
Nebraska	0	0	0	0	0
Nevada	1	0	0	1	0
New Hampshire	0	0	0	0	0
New Jersey	1	1	1	1	1
New Mexico	1	1	0	1	0
New York	1	1	1	1	1
North Carolina	1	1	0	1	1
North Dakota	0	1	0	0	0
Ohio	0	0	0	0	0
Oklahoma	1	0	0	0	0
Oregon	1	1	1	1	1
Pennsylvania	1	1	1	1	1
Rhode Island	1	1	1	1	1
South Carolina	1	1	0	1	1
South Dakota	1	1	1	1	1
Tennessee	0	0	0	1	0
Texas	1	1	1	1	1
Utah	1	0	1	1	0
Vermont	1	1	1	1	1
Virginia	1	1	1	1	1
Washington	1	0	0	1	1
West Virginia	1	1	0	1	1
Wisconsin	1	1	1	1	1
Wyoming	0	0	0	0	0

Table 5.4 below categorizes states based on how many NIST Cybersecurity Framework functions they address. The first column refers to the numbers of covered NIST functions out of five. The second column lists the states that correspond with the number of covered NIST functions.

Table 5.4 Cross-state Analysis based on NIST Cybersecurity Framework

# of Covered NIST Functions	States
0	Alaska, Arkansas, Kentucky, Maine, Nebraska, New Hampshire, Ohio, Wyoming
1	Arizona, Idaho, North Dakota, Oklahoma, Tennessee
2	Louisiana, Massachusetts, Missouri, Nevada
3	Alabama, Colorado, Delaware, Georgia, Indiana, Kansas, New Mexico, Utah, Washington
4	California, Florida, Hawaii, Iowa, North Carolina, South Carolina, West Virginia
5	Connecticut, Illinois, Maryland, Michigan, Minnesota, Mississippi, Montana, New Jersey, New York, Oregon, Pennsylvania, Rhode Island, South Dakota, Texas, Vermont, Virginia, Wisconsin

The first row of Table 5.4 has eight states that do not address any of the framework functions. The plans of these states are imprecise as they broadly cover information technology, enterprise security, and digitalization. The plans are also relatively short (e.g., Kentucky's plan is 4 pages) and not user friendly. For instance, they do not event include a table of content. Furthermore, these states perform poorly when it comes to coverage of scholarly criteria. For instance, Ohio's plan only discusses the *training* criteria whereas Kentucky's plan covers the *funding*, *leadership*, and *partnership* criteria.[13]

The second row of Table 5.4 has states that address only one out of 5 framework functions. Similar to Kentucky and Ohio, the planning documents of Arizona, Idaho, North Dakota, Oklahoma, and Tennessee also do not specifically focus on cybersecurity. In the case of Tennessee, there is not a separate document for

[13] See Chapter 4 for the definitions of the scholarly criteria.

cybersecurity or even IT security. Instead, the official Tennessee state government website has a section for cybersecurity.[14] In other states, cybersecurity is mentioned scarcely in broad technology strategic plans. Similar to the first row states, there is an alignment between how these states perform with regards to NIST and scholarly theme. Majority of the second-row states, namely Idaho, Oklahoma, and Tennessee are minimal coverage states while the rest of the second row states, namely Arizona and North Dakota are in the low-coverage category with regards to scholarly themes.[15]

The third and fourth rows of Table 5.4 have states that address two and three NIST functions, respectively. Many of them such as Louisiana and Missouri have a separate cybersecurity planning document, though some have a section devoted to cybersecurity within their IT strategic plan such as Nevada. Even the separate cybersecurity planning documents are not as developed as the fifth and sixth row states. Table 5.5 illustrates the allocation of states based on the NIST Cybersecurity Framework functions in the rows and scholarly theme coverage categorization in columns. In terms of the scholarly criteria coverage, the third row states are in minimal and low coverage categories. The fourth row states, on the other hand, are distributed more evenly across four scholarly theme coverage categorization. Thus, there is an overall improvement compared to the first and second row states of Table 5.4.

---

[14] See http://tn.gov/cybersecurity

[15] The discussion of alignment with the scholarly themes is in Chapter 4.

Table 5.5 Allocation of States Based on the NIST Cybersecurity Framework Functions

NIST/ Scholarly	**Minimal Coverage** (0-1 scholarly theme)	**Low Coverage** (2-3 scholarly theme)	**Moderate Coverage** (4-5 scholarly theme)	**High Coverage** (6-8 scholarly theme)
0	Alaska, Arkansas, Maine, Nebraska, New Hampshire, Ohio, Wyoming	Kentucky		
1	Idaho, Oklahoma, Tennessee	Arizona, North Dakota		
2	Louisiana	Massachusetts, Missouri, Nevada		
3	Utah, Washington	Colorado	Alabama, Indiana, Kansas	Delaware, Georgia, New Mexico
4	South Carolina	Hawaii, West Virginia		California, Florida, Iowa, North Carolina
5	Minnesota, Pennsylvania, South Dakota	Maryland	Michigan, Mississippi, New Jersey, New York, Wisconsin	Connecticut, Illinois, Montana, Oregon, Rhode Island, Texas, Vermont, Virginia

The fifth and sixth row of Table 5.4 show the most successful states in terms of addressing NIST Cybersecurity Framework functions. As Table 5.5 shows, many of these states are also successful according to the scholarly criteria. Most of them have

lengthy documents with specified objectives, action plans, allocation of responsibilities, and use of the right and standardized terminology. The exceptions are South Carolina, Minnesota, Pennsylvania, and South Dakota which perform well in terms of NIST Cybersecurity functions but locate in the minimal coverage category based on the scholar themes. The explanation for this lack of correlation is comes from the difference between the general guideline nature of NIST functions and specific action area nature of the scholarly themes. For instance, South Dakota has a well-developed website that aligns with all five framework functions whereas it lacks planning information with regards to specific action areas of scholarly themes.

This analysis demonstrates that the distribution of States based on their coverage of scholarly criteria and NIST Cybersecurity Framework functions resemble one another. In other words, the research finds that states address *identify, protect, detect, respond*, and *recover* functions are also high coverage states based on the scholarly criteria. Figure 5.2 below demonstrates that the fitted regression analysis of NIST compliances based on the scholarly criteria. The Y axis shows how many of functions from the NIST framework are covered whereas the X axis shows how many of scholarly criteria are covered. The fitted analysis with 95% confidence intervals demonstrates a correlation between states' NIST and scholarly criteria performance. The regression table for this graph and its discussion are provided in Appendix A.

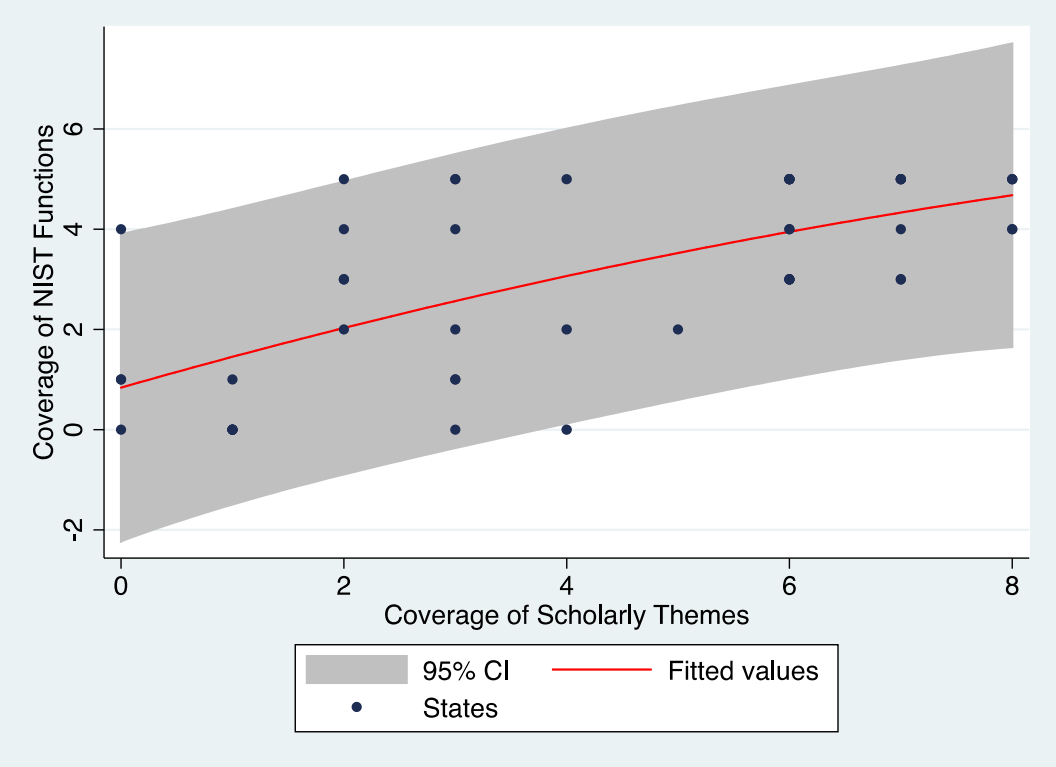

Figure 5.2 Fitted Regression Analysis of NIST Compliances Based on the Scholarly Themes.

The likely reason for the correlation between the scholarly criteria and the NIST functions is that the latter helps to direct attention to the scholarly themes. As mentioned earlier, the NIST functions cut across scholarly themes that are more specific action areas. Thus, if a state plan addresses the *protect* function it is likely to address *awareness*, *training*, and *better equipment* themes as well.

Amongst the states that address the 5 out of 5 NIST Cybersecurity Framework functions, three of them, namely Connecticut, Rhode Island, and Virginia, also address all 8 scholarly criteria. Thus, this research considers these three states as model states

for cybersecurity planning. The next section examines what makes a state cybersecurity plan a model plan with best practices incorporated.

5.5 State Model of the Best Cybersecurity Planning Practices

This analysis reveals three main practices that make a plan as a model. The first common practice of model states is their comprehensiveness. These model states cybersecurity planning documents discuss all eight scholarly themes in addition to the NIST Cybersecurity Framework functions. Thus, none of the stages or themes are neglected in planning documents. Second, these three model states deliberately use a standardized and accurate terminology which corresponds with the language that NIST Cybersecurity Framework uses. These states make an effort to apply NIST Cybersecurity standards in their plans. The third common practice of model states is to conduct cybersecurity planning in detail. The model state cybersecurity planning documents are not only comprehensive in terms of covering eight scholarly themes but also they dig into a specific theme with separate planning documents discussing them in length. The following sections analyze the model states cybersecurity planning documents.

5.5.1 Rhode Island

Rhode Island State Cybersecurity Strategy (2019) fulfills the three common practices that make a plan as model mentioned above. The plan is comprehensive in terms of covering eight scholarly themes. It also uses the same language with the NIST standards and discusses framework functions in detail. For instance, the plan has done an analysis of cybersecurity planning alignment with the NIST Cybersecurity standards. Figure 5.3 is a screenshot that is taken from the planning document titled,

"Rhode Island State Cybersecurity Strategy". The screenshot shows that the document actively uses the same paradigm with the NIST Cybersecurity Framework.

ALIGNMENT WITH THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK

Alignment of the Rhode Island Cybersecurity Strategy with the NIST Cybersecurity Framework	Identify	Protect	Defend	Respond	Recover
Strategic Goal #1 Increase the resilience of the infrastructure supporting the health, safety, and security of citizens, the government and the state's economy. Prepare R.I.'s public and private sector infrastructure for the digital changes and opportunities of the 21st century.					
Objective 1.1: Implement a risk-management program for cybersecurity.	•	•	•	•	•
Objective 1.2: Establish an intelligence-led cybersecurity program within state government that reduces cyber-attack response time and optimizes vulnerability management.	•				•
Objective 1.3: Modernize state government information and security technology.	•	•	•	•	•
Objective 1.4: Exercise new technology and security enhancements annually.	•				
Objective 1.5: Mature state government security processes.				•	•
Objective 1.6: Develop a cyber talent plan for the state.				•	
Objective 1.7: Exercise with critical infrastructure representatives, where exercise objectives identify resiliency-related improvements to counter the cyber threat.				•	•

Figure 5.3 Screenshot from Rhode Island State Cybersecurity Strategy

Rhode Island also manages to create an action-oriented plan with specific goals and objectives. For instance, they match objectives such as proving opportunities for the exposition of new technologies with necessary steps such as working with the Rhode Island Commerce Corporation to assess regional and national opportunities for

businesses so they can demonstrate their new technologies (State of Rhode Island, 2019). The plan also discusses the eight scholarly themes in-depth by sparing a separate section for each theme. For instance, the *leadership, national security, partnerships,* and *training* themes all have a designated subsection where the plan elaborates on future steps about these themes.

Beyond three practices of model states, the Rhode Island's plan also engages in a self-evaluation and assesses its historical evolution of cybersecurity. By doing so, it identifies past activities and operations as well as predicting a future state of state's cybersecurity. This historical analysis and self-evaluation enable the state to adopt a proactive and predictive approach. Table 5.6 illustrates the evolution of Rhode Island's cybersecurity.

Table 5.6 Evolution of Rhode Island's Cybersecurity

Nascent	Reactive	Proactive	Predictive	Next Generation
• 8/5 monitoring • Long review-based analysis • Irregular Patching • Limited GRC • Isolated Remediation • Point Solution	• Assume an attack will occur & treat the symptom • Static signature analysis (looking for bad things dormant on the system) • Port blocking • Domain name system logging & analysis	• Prevent & contain attacks • Eliminate intruder advance • Detect adversary activity on endpoints • Hunt for indicators of adversary activity in the network	• Anticipate & react in real-time • Automated malware analysis • Real-time (+encrypted) traffic inspection & classification based on app, user, & content • Automated cyber security incident response	• Continuous Monitoring • Continuous Diagnostics and Remediation (CDR) • Next Generation Firewalls (NGF) • Continuous Threat Hunting • Advanced Intelligence Analytics • Integrated with other security disciplines (Physical, Personnel, etc.) "Concentric Ring Defense"
Typical 2004	State of the Art 2006	Best practice since ~2011	Industry leading ~2014	Future State of Security in RI 2018>

Source: State of Rhode Island, 2019, p.16.

5.5.2 Connecticut

Similar to Rhode Island, the State of Connecticut's cybersecurity planning documents fulfill the three common practices that make a plan as model. The state has published nine different cybersecurity planning documents since 2016. The State plans its cybersecurity with these documents instead of having only one large document like in the Rhode Island model. This enables the state to devote a lengthy and detailed discussion to each theme. The in-depth discussion and particularity fulfill the third common practice of model states.

The state of Connecticut's plans are also comprehensive enough to cover eight scholarly themes, the first common practice of model states. Furthermore, these plans deliberately engage with the NIST Cybersecurity Framework functions. For instance, the Cybersecurity and Connecticut's Public Utilities plan, first, summarizes NIST Cybersecurity Framework, and then, question the level of standardization that NIST provides (Connecticut Public Utilities Regulatory Authority, 2014). Nevertheless, in these documents, Connecticut uses the NIST terminology and applies the framework to its action plans. Some of the Connecticut's cybersecurity planning documents not only analyze the NIST Cybersecurity Framework functions but also, they go in detail and plan specifics about subcategories of NIST Cybersecurity Framework. Connecticut Public Utilities Cybersecurity Action Plan is an example of a document that is devoted to the *asset management* subcategory of the *identify* function in its entirety.

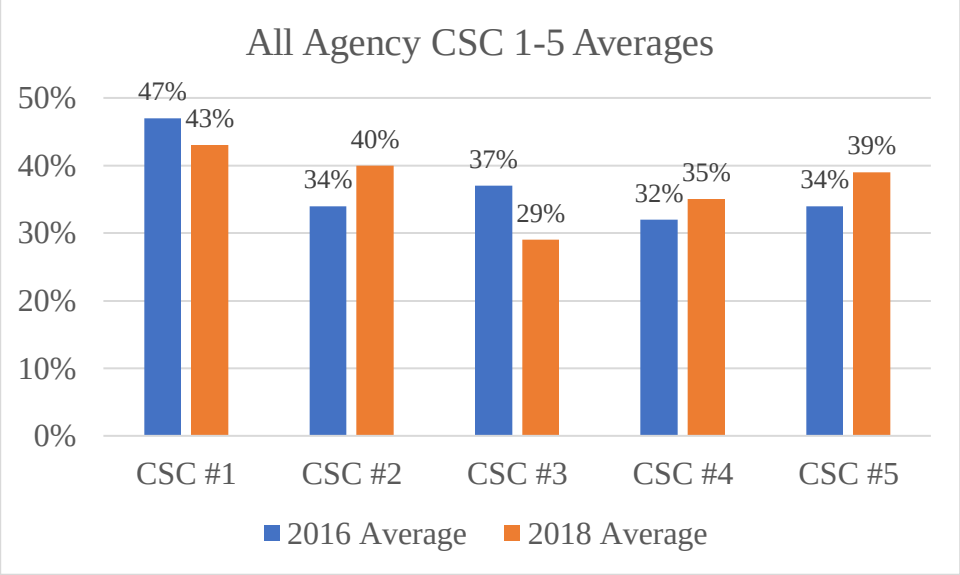

Figure 5.4 2016-2018 Critical Controls Comparison.

Notes: CSC #1 refers to Hardware Asset Control, CSC #2 refers to Software Asset Control, CSC #3 refers to Vulnerability Management, CSC #4 refers to Controlled Administrative Privileges, CSC #5 refers to Secure Configurations. Source: State of Connecticut Cybersecurity Update (Currey, 2018, p.12).

Finally, Connecticut evaluates how well its cybersecurity posture is by conducting surveys with state agencies. Figure 5.4 above demonstrates the change from 2016 to 2018 survey results about five cybersecurity controls listed under Figure 5.4. This is a similar practice with the Rhode Island case in terms of self-assessing the cybersecurity posture of the state. It enables Connecticut to adopt a proactive and predictive approach in designing future cybersecurity plans.

5.5.3 Virginia

The state of Virginia is especially invested in cybersecurity as the state defends its infrastructure against more than 10 million cyber attacks per month (Office of

Virginia's Secretary of Technology, n.d., p. 12). The state also hosts critical national public organizations such as NSA and NASA. As it is expected, Virginia is the last model state that covers eight scholarly themes and five NIST functions. Like the Connecticut case, it has published eight separate planning documents for cybersecurity. Many of these planning documents correspond with the scholarly themes and NIST standards. For instance, Virginia examines its available resources in great detail. This means both a scrutinized asset management and an exploration of potential partnerships with organizations and companies in the region. Figure 5.5 below demonstrates an example of identification of resources.

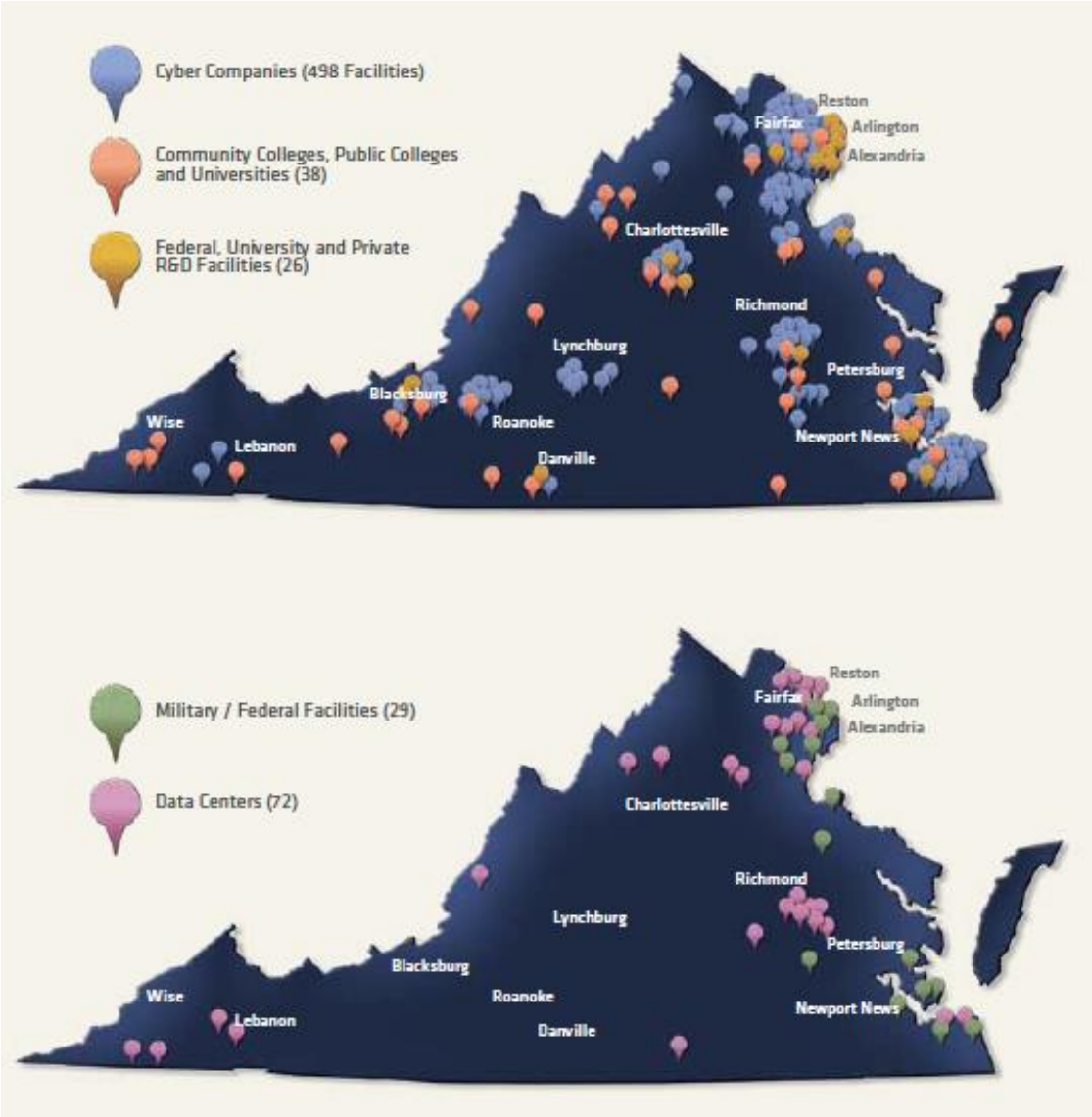

Figure 5.5 Virginia's Cyber Security Resources. Source: Office of Virginia's Secretary of Technology, n.d., p. 13.

With regards to creating specific plans for each theme and framework function, the state of Virginia has a plan titled "Information Security Incident Response Procedures" that just focuses on the response function of the NIST Cybersecurity

Framework. Similarly, the documents, namely "Collaboration & Diversity: Virginia's Winning Strategy for Cyber Security Leadership" and "Virginia's Cyber Security Approach: Leadership through Diversity" concentrate on the State's leadership approach that brings together training programs for the private sector, connections with the Federal Government, and partnerships with different universities. This is a huge contrast to non-model states that scarcely mention cybersecurity in their inattentive cybersecurity-related planning documents.

The state's cybersecurity planning is praised by many sources. For example, Spidalieri (2015) explains that Virginia is the first state to adopt the NIST Cybersecurity Framework to achieve an effective cybersecurity posture.

5.6 Conclusion

This chapter answers the second research question of this project. Similar to Chapter 4, it analyzes the incorporation of best practices into state level cybersecurity planning documents, this time focusing on the NIST Cybersecurity Framework functions. This analysis finds that most States address *identity, protect,* and *respond* functions in their plans whereas less than half of the States address the *detect* and *recover* functions. Furthermore, the analysis also points out that the *protect* and *recover* functions go hand in hand as states usually address them together.

In addition, a cross-state analysis of incorporation of the NIST Cybersecurity Framework functions into state cybersecurity planning documents reveals that states address *identify, protect, detect, respond*, and *recover* functions also are high coverage states based on the scholarly criteria. Finally, the chapter further examines the model states namely, Rhode Island, Connecticut, and Virginia. The model states are similar in terms of covering all eight scholarly criteria and five NIST functions. Furthermore,

they have other common characteristics such as using the NIST terminology in their planning documents and incorporating a self-assessment that compares the state cybersecurity posture historically. Finally, the model states are similar in terms of creating very specific plans that are devoted in their entirety to one function or scholarly theme. In other words, separate planning documents are published for a specific theme. All these common characteristics make Rhode Island, Connecticut, and Virginia model states with regards to NIST and scholarly criteria.

Chapter 6

AN ANALYSIS OF SAMPLE STATES' CYBERSECURITY-RELATED LEGISLATED POLICIES

6.1 Introduction

This chapter analyzes cybersecurity-related legislative policies of eight sample states, namely, California, Delaware, Florida, Maryland, Montana, New York, Virginia, and Wyoming. The focus is on legislation enacted from 2015 to 2021. This research does not include many other policies of states often embodied in executive orders from governors or administrative regulations from state agencies. The sample states were selected through a purposeful sampling method that considers the victim loss index, the cybersecurity job supply index and the three categories of the political culture theory (Elazar, 1991; 1994). More specifically, as described in Chapter 3, for each political culture category, the state with the highest supply of the cybersecurity workers in the public sector and victim loss were selected as sample states.

By reviewing a cross-state analysis of cybersecurity-related policies concerning both scholarly themes and NIST functions, the chapter addresses the third research question:

> *RQ3: In what ways do cybersecurity policies adopted between 2015 and 2021 legislative sessions of states with high cyberattack figures incorporate the best practices as defined by the scholarly criteria and the 2018 NIST Cybersecurity Framework?*

Then, the chapter examines the fourth research question:

RQ4: In what ways do the cybersecurity policies in the sample states correspond to their latest cybersecurity planning documents as of the end of the 2021 legislative session?

The analysis begins with a review of the' cybersecurity-related policies of the sample states as of 2021 and describes how many policies each state enacted or introduced but failed to enact from 2015 to 2021. The analysis then proceeds to examine the ways in which cybersecurity-related legislated policies incorporate themes identified in the scholarly literature. Similar to Chapter 4, the theme-based analysis of cybersecurity-related policies includes selected examples from state legislative policy documents.

The analysis continues with an examination of the correspondence between the cybersecurity-related legislated policies and planning documents, comparing their incorporation of both scholarly themes and NIST functions. The chapter also elaborates on potential reasons for the correspondence level between the legislated policies and the planning documents. Finally, the chapter closes with a summary of findings as they apply to the third and fourth research questions.

6.2 The Landscape of Sample States' Cybersecurity-related Legislated Policies

One of the most important tools for state governments to improve cybersecurity is to enact cybersecurity-related policies through legislation. These legislated policies typically include requirements for public and private organizations to implement security procedures, assign responsibilities to specific task forces, and designate training for government employees to improve cybersecurity literacy. There are also legislated policies that mandate reporting of data breaches for businesses and government and allocating budgets to cybersecurity-related expenses.

As defined in Chapter 3, cybersecurity-related policies refer to state bills and resolutions introduced and enacted from 2015 to 2021. The legislative bills were drawn from the National Conference of State Legislatures (NCSL) website and then validated against information from the NexisUni database as described in chapter 3.

After compiling cybersecurity-related legislative bills of the eight sample states, this research categorizes them as enacted, introduced but failed (not enacted), and still pending as of the end of the 2021 legislative session. Table 6.1 below shows the number of enacted, failed to enact, and pending cybersecurity-related legislative bills per state per year. As reflected in Table 6.1, Virginia, Maryland, California, and Florida are the states that enacted the highest number of cybersecurity-related policies, with 40, 26, 22, and 19 policies enacted, respectively. However, these four states also have similarly high numbers of failed proposals, bills introduced but not enacted (specifically, California: 23, Florida: 30, Virginia: 41, and Maryland: 70). Thus, the enacted policies represent only a subset of the cybersecurity legislative efforts of these four states. In contrast, the states of Montana, Delaware, Wyoming, and New York have a lower number of enacted policies amongst the sample states, with 7, 5, 3, and 1 policies enacted, respectively. Amongst these states, Montana, Delaware, and Wyoming also have small numbers of failed policy proposals, with 2, 1, and 3 proposals introduced but not enacted respectively. These three states with the lowest level of proposed and enacted legislation also have the smallest populations. The only exception to this pattern is New York which introduced but failed to pass 33 cybersecurity-related bills, enacting only 1. It is possible that New York creates more policies by executive action or through agency policies than by enacted legislation.

Table 6.1 Number of Enacted, Fail to Enact, and Pending Cybersecurity-related Policies of Sample States

State	Year	# of Enacted	# of Failed to Enact	# of Pending	State	Year	# of Enacted	# of Failed to Enact	# of Pending
California	2015	1	2	2	Montana	2015	0	1	0
California	2016	4	5	0	Montana	2016	0	0	0
California	2017	1	1	7	Montana	2017	1	0	0
California	2018	8	4	0	Montana	2018	0	0	0
California	2019	5	0	7	Montana	2019	2	1	0
California	2020	1	11	0	Montana	2020	0	0	0
California	2021	2	0	7	Montana	2021	4	0	0
Total		***22***	***23***	***23***	***Total***		***7***	***2***	***0***
Delaware	2015	0	0	0	New York	2015	0	0	6
Delaware	2016	1	1	0	New York	2016	0	0	6
Delaware	2017	1	0	0	New York	2017	0	0	5
Delaware	2018	0	0	0	New York	2018	0	33	0
Delaware	2019	2	0	0	New York	2019	1	0	25
Delaware	2020	1	0	0	New York	2020	0	0	33
Delaware	2021	0	0	0	New York	2021	0	0	23
Total		***5***	***1***	***0***	***Total***		***1***	***33***	***98***
Florida	2015	0	0	0	Virginia	2015	3	1	0
Florida	2016	3	2	0	Virginia	2016	2	6	2
Florida	2017	1	3	0	Virginia	2017	10	13	0
Florida	2018	3	5	0	Virginia	2018	4	6	0
Florida	2019	6	11	0	Virginia	2019	6	5	0
Florida	2020	3	4	0	Virginia	2020	6	5	0
Florida	2021	3	5	0	Virginia	2021	9	5	0
Total		***19***	***30***	***0***	***Total***		***40***	***41***	***2***
Maryland	2015	2	5	0	Wyoming	2015	0	0	0
Maryland	2016	1	2	0	Wyoming	2016	1	0	0
Maryland	2017	2	9	0	Wyoming	2017	1	2	0
Maryland	2018	8	7	0	Wyoming	2018	1	0	0
Maryland	2019	5	6	0	Wyoming	2019	0	0	0
Maryland	2020	3	23	0	Wyoming	2020	0	0	0
Maryland	2021	5	18	0	Wyoming	2021	0	1	0
Total		***26***	***70***	***0***	***Total***		***3***	***3***	***0***

Sample states' level of legislative efforts on cybersecurity issues do not change based on their geographic region or political culture. The high and low legislative effort states cut across regions of the U.S. Table 6.2 shows that states with high and low legislative effort represent mixes of different political parties in leadership, political culture, and region. For instance, California, Virginia, and Maryland have a high number of enacted policies, but they are from different political cultures, located in different regions, and have both political parties in leadership. In addition, there are also states with less legislative activities in terms of cybersecurity issues from different political cultures, regions, and political parties in leadership. For example, both Montana and Wyoming have low level legislative activities on cybersecurity issues; however, Montana is a moralistic state with a democrat governor in 2020 whereas Wyoming is an individualistic state with a republican leader.

Table 6.2 Legislative Activities, Political Cultures, and Regions of Sample States

State	**# of Enacted**	**# of Failed to Enact**	**# of Pending**	**Political Culture**	**Region**	**Political Party in Leadership**
California	22	23	23	Moralistic	Pacific	Democrat
Delaware	5	1	0	Individualistic	South Atlantic	Democrat
Florida	19	30	0	Traditionalistic	South Atlantic	Republican
Maryland	26	70	0	Individualistic	South Atlantic	Republican
Montana	7	2	0	Moralistic	Mountain	Democrat
New York	1	33	98	Individualistic	Middle Atlantic	Democrat
Virginia	40	41	2	Traditionalistic	South Atlantic	Democrat
Wyoming	3	3	0	Individualistic	Mountain	Republican

Note: The political party in leadership refers to the party of the Governor in 2020.

6.3 Key Themes of Cybersecurity-related Policies

The enacted cybersecurity legislation in each of the sample states was examined to identity the incorporation of the eight scholarly themes derived from the local and state-level cybersecurity literature. These themes are *funding, better equipment, leadership, training, partnership, coordination and* communication, *developing awareness & culture,* and *national security.*[16] The theme-based analysis shows that sample states incorporate scholarly themes into their cybersecurity-related legislative policies to a varying extent. The following sections elaborate on how enacted policies address these themes in the case of sample states, starting with those themes most frequently addressed.

[16] Each of these themes is defined in Chapter 3

Table 6.3 The Scholarly Themes and the Sample States that Cover the Themes in Cybersecurity-related Policies

Theme	States
Coordination and Communication	California, Delaware, Florida, Maryland, Montana, New York, Virginia, Wyoming
Funding	California, Florida, Maryland, Montana, New York, Virginia, Wyoming
Leadership	California, Delaware, Florida, Maryland, Montana, Virginia, Wyoming
Better Equipment	California, Delaware, Florida, Maryland, Montana, Virginia
Partnership	California, Delaware, Florida, Maryland, Montana, New York
Awareness & Culture	California, Florida, Maryland, Montana, Virginia
Training	California, Florida, Maryland, Montana, Virginia
National Security	California, Maryland, Montana, New York, Virginia

6.3.1 Coordination and Communication

The most frequently addressed scholarly theme is *coordination and communication*, on which all eight sample states passed cybersecurity-related legislative policies. When addressing the *coordination and communication* theme, the policies require reporting of cyber-related activities to specified entities, regulating correspondence between state agencies, and mandating collaboration to take specified cyber-related actions. For instance, the State of Maryland established the Maryland Cybersecurity Council. It requires the Council "…to work with certain entities to take actions related to cybersecurity (and) …to submit a report on its activities to the General Assembly (Maryland General Assembly, 2015). The requirement to report activities of the Council to the General Assembly is an example of how cybersecurity-

related policies are intended to improve communication. In addition, to advance coordination, states enact policies that regulate the responsibilities for cybersecurity activities of various state agencies. For example, the State of Virginia passed the following bill in 2015 with information technology compliance requirements for state agency directors:

> Relates to IT responsibility of agency directors; provides that the director of every department in the Executive Branch of State government shall be responsible for securing the electronic data held by that department and shall comply with the requirements of the Commonwealth's Information Technology Security and Risk Management Program as developed by the Chief Information Officer (Virginia General Assembly, 2015b).

This bill organizes the relationship between the departments of the Executive Branch and the Chief Information Officer. Thus, it advances the coordination of securing the cyberspace of each department.

6.3.2 Funding

While the *funding* theme is the second least covered scholarly theme in the planning documents, it is the second most frequently addressed theme in cybersecurity-related legislative policies in the sample states. One reason for the frequency of the of the *funding* theme is that the approval of state funding of cybersecurity programs typically requires legislation. By contrast, planning documents often omit information about the funding required for the implementation of the plan. All sample states except for Delaware enacted a cybersecurity-related policy on *funding* between 2015 and 2021 (See Table 6.3). This means that despite avoiding budget-related commitments in planning documents, the states nevertheless enact many policies that allocate funding to cybersecurity expenses. For instance, Wyoming

allocates $2,300,000.00 for cybersecurity with a bill passed in 2018 (Wyoming General Assembly, 2018). Other states, like Virginia, also amend their budget bills to incorporate funding for cybersecurity programs (Virginia General Assembly, 2019). On top of these legislative policies, some states fund their cybersecurity-related expenses through their general budget allocation to different agencies.

Some policies specify the cybersecurity programs and expanses for which the bill provides funding. For instance, the State of Montana enacted a policy that provides funding for updating software, hiring cybersecurity staff, outsourced professional training, and raising cyber awareness through community-oriented programs:

> Appropriates money to various state agencies for the upcoming biennium, including funding for next generation antivirus software; cybersecurity staff; cybersecurity student programs; web application firewall; e-mail security gateway; security information and event management; analytics-driven security and continuous monitoring for threats; governance, risk, and compliance software; enterprise risk assessment; digital forensics lab; source code repository; security orchestration, automation and response; and outsourced professional services. Also provides that the State Information Technology Services Division shall report to the legislative finance committee quarterly on the Montana Cybersecurity Enhancement Project (Montana General Assembly, 2019).

This bill also illustrates how the *funding* theme often overlaps with other scholarly themes such as *better equipment, developing awareness & culture for cybersecurity,* and *training.*

6.3.3 Leadership

Along with *funding*, the *leadership* theme is also the second most frequently addressed scholarly theme in the enacted legislation of the sample states. All sample

states except New York enacted a cybersecurity-related legislative policy on *leadership* between 2015 and 2021 (See Table 6.3). Similar to planning documents, the *leadership* theme in legislation refers to responsibility allocation, and the designation of a clear administrative structure in states' cybersecurity-related policies. For example, to clarify the hierarchical administrative structure and the leadership role of the Secretary of Information Technology, Maryland enacted a bill in 2021 that requires the Secretary, in consultation with the Attorney General, "…to advise and oversee a consistent cybersecurity strategy for units of State government, …to consult with the Legislative and Judicial branches on a cybersecurity strategy, (and) …to develop guidance on consistent cybersecurity strategies" (Maryland General Assembly, 2021b). In addition, in 2015, the State of Virginia enacted legislation that attributes the responsibility for data security to the directors of every department in the executive branch of the state government (Virginia, General Assembly, 2015a). This clear allocation of cybersecurity responsibility is intended to encourage the directors to take necessary precautions such as risk assessment programs, creating specific task forces, and implementing training programs.

6.3.4 Better Equipment

Six out of 8 sample states addressed the *better equipment* theme in their cybersecurity-related legislative policies from 2015 to 2021. The two sample states that did not enact a policy on *better equipment* are New York and Wyoming. Like planning documents, the policies also refer to software updates, renewal of hardware components, and preventing cyber vulnerabilities for infrastructure due to outdated equipment. These policies regulate the equipment standards of both the public and private sectors. For instance, Delaware legislation "authorizes the Department of

Technology and Information to develop and implement a comprehensive information security program that applies personnel, process, and technology controls to protect the state's data, systems, and infrastructure, within the state's computing environment and on partner systems" (Delaware General Assembly, 2020). The technology control component of the implemented information security program requires a technology assessment and potential update to secure the state's cyberspace. While the Delaware law targets the government agencies' equipment, the State of California has enacted legislation requiring the private sector to meet certain requirements to incorporate reasonable security features if they manufacture and sell cyber-connected devices in California. Thus, the private sector must equip "a connected device with a means for authentication outside a local area network" (California General Assembly, 2018).

6.3.5 Partnership

Similar to the *better equipment* theme, six out of 8 sample states cover the *partnership* theme in their cybersecurity-related legislation from 2015 to 2021. Amongst sample states, only Virginia and Wyoming did not enact a cybersecurity-related policy on *partnership between governmental and non-governmental organizations.* The enacted partnership policies are intended to enhance collaborations and cooperation with governmental organizations such as the FBI, Department of Homeland Security, and non-governmental organizations such as firms, companies, universities, and research institutes in different capacities. The partnership areas include using data storage facilities (data centers), new technology transfer, outsourcing training programs for employees.

Some enacted cybersecurity-related policies establish a cooperative relationship between universities and state governments. For instance, in 2021, the

State of Maryland enacted a policy to establish the Center for Cybersecurity at the University of Maryland Baltimore County. Furthermore, the same policy requires the governor to appropriate funding for the Center in their annual budget bills and the Center to report its activities to the General Assembly. Finally, the policy "requires the University of Maryland Center for Economic and Entrepreneurship Development (UMCEED) to develop degree and credential programs in a field of study related to certain technologies" (Maryland General Assembly, 2021a). On top of these legislative policies, some states establish partnerships between state agencies and public (state-funded) universities without legislation, simply as a product of executive action or agency policy.

6.3.6 Developing Awareness & Culture for Cybersecurity

Five of 8 sample states addressed the *awareness and culture* theme in their cybersecurity-related legislative policies. However. Delaware, New York, and Wyoming did not enact a cybersecurity-related policy on *awareness and culture* between 2015 and 2021. The enacted state policies encourage cyber awareness of citizens by organizing public meetings, conferences, and workshops; and publishing publicly available reports. Furthermore, some of these policies target state employees through awareness training programs. A California law enacted in 2019 does both of them by announcing a cybersecurity awareness month: "This resolution proclaims the month of October 2019, and every October thereafter, to be National Cybersecurity Awareness Month in California" (California General Assembly, 2019b).

6.3.7 Training

The *training* theme is the most frequently addressed scholarly theme in state-level cybersecurity planning documents., In the case of sample states, five out of 8 enacted cybersecurity-related legislative policies that cover the *training* theme (See Table 6.3). Similar to cybersecurity planning documents, many policies that address the *awareness and culture* theme also address the *training* theme. If a state enacted a policy on cybersecurity training, the training program was most likely to be mandatory. Voluntary cybersecurity training programs are generally not addressed in enacted legislative policies. For instance, the State of Virginia requires an information security program for all state employees, organized by its Information Technologies Agency. Furthermore, the law also requires the executive, legislative, and judicial branches, and independent agencies to conduct information security training programs, whose curricula are set up by the Chief Information Officer every year (Virginia General Assembly, 2020).

Some cybersecurity training-related policies target voters. California requires "an applicant to take a training course regarding data security as a condition for the receipt of voter registration information" (California General Assembly, 2019a). These free courses train applicants, and thus citizens, on cybersecurity issues.

6.3.8 National Security

The *national security* theme is the least addressed in states' cybersecurity-related legislative policies, similar to the cybersecurity planning documents. Only half of the sample states enacted legislation about the national security dimensions of cybersecurity. Most of the enacted policies relate to election security. For example, the State of Montana requires:

> the secretary of state to adopt rules defining and governing election security; requiring election security assessments by the secretary of state and county election administrations; establishing that security assessments are confidential information; establishing reporting requirements; directing the secretary of state to adopt a rule prohibiting certain persons from receiving pecuniary benefits with respect to certain ballot activities; providing penalties; providing rulemaking authority; and providing an immediate effective date (Montana H.B. 530, 2021).

In some cases, the *national security* theme is acknowledged regarding the importance of preventing cyberattacks. For example, in 2020, California enacted a policy encouraging information sharing to detect or prevent "cyberattacks that threaten public health and safety, economic stability, and national security" (California General Assembly, 2020).

6.4 A Cross-state Analysis of the Correspondence of Cybersecurity-related Policies and Plans of Sample States

This section examines the correspondence between state cybersecurity-related legislation and planning documents with regard to (1) the eight scholarly themes and (2) NIST Cybersecurity Framework functions.

6.4.1 Policy-Planning Correspondence Based on the Scholarly Criteria

The analysis of policy-planning correspondence based on the eight scholarly criteria is summarized in Table 6.4. For each sample state, the scholarly themes are displayed in three categories. The first column, Corresponding Themes, lists the scholarly themes addressed by both the state's planning documents and cybersecurity-related legislation. The second column, Themes Covered Only in the Planning Documents, shows the scholarly themes covered only in the planning documents. Finally, the third column, Themes Covered Only in the Enacted Policies, shows the scholarly themes covered only in the enacted policies. For instance, the State of

California addresses *awareness, better equipment, coordination and communication, leadership, partnership,* and *training* themes in its latest planning documents and its enacted cybersecurity-related legislative policies from 2015 to 2021. Thus, these themes are listed in the Corresponding Themes column. In addition, while California addresses the themes of *funding* and *national security* in its policies, it does not address these two themes in the plans. These two scholarly themes, *funding* and *national security,* are listed in the Themes Covered Only in the Enacted Policies column. Finally, California's policies address all the themes cited in its planning documents.

Table 6.4 A Comparison of Planning Documents and Cybersecurity-related Policies based on Scholarly Themes of Sample States

State	Corresponding Themes	Themes Covered Only in the Planning Documents	Themes Covered Only in the Enacted Policies
California	Awareness, Better Equipment, Coordination and Communication, Leadership, Partnership, Training		Funding, National Security
Delaware	Better Equipment, Coordination and Communication, Leadership, Partnership	Awareness, Training	
Florida	Awareness, Funding, Partnership, Training	National Security	Better Equipment, Coordination and Communication, Leadership
Maryland	Coordination and Communication, Partnership, Training		Awareness, Better Equipment, Funding, Leadership, National Security
Montana	Awareness, Better Equipment, Coordination and Communication, Funding, Partnership, Training		National Security, Partnership

New York	Partnership	Awareness, Better Equipment, Leadership, Training	Coordination and Communication, Funding, National Security
Virginia	Awareness, Better Equipment, Coordination and Communication, Funding, Training	Partnership	Leadership, National Security
Wyoming		Training	Coordination and Communication, Funding, Leadership

The first finding of the cross-state analysis is that for most states there is high correspondence between the planning documents and cybersecurity-related policies. Table 6.4 demonstrates that California, Delaware, Florida, Montana, and Virginia address at least four scholarly themes in both their planning documents and cybersecurity-related legislation. The lower correspondence states are Maryland, New York, and Wyoming. In the case of Maryland, the cybersecurity-related policies incorporate all eight scholarly themes. However, its plans cover only three themes, so the correspondence remains low. In the case of New York, there is only one corresponding theme: *partnership.* This low correspondence may be due to New York's high number of introduced but not approved cybersecurity-related policies, many of which do address themes in the planning documents. There are no corresponding themes in the case of Wyoming, which covers only training in its planning documents (See Chapter 4) and which enacted only three cybersecurity-related policies from 2015 to 2021. Furthermore, unlike New York, the State of Wyoming does not have a large number of proposed bills that would have addressed the scholarly themes in its planning documents. Overall, this research concludes that still there is a significant level of correspondence for most of the sample states based on the scholarly criteria.

The second finding is that for all but two of the sample states, the enacted policies cover more scholarly themes than the state's planning documents. The exceptions are Delaware and New York. The states of California, Maryland, and Montana have policies that cover all the scholarly themes, even though their planning documents cover only a subset of the themes. In addition, Table 6.4 shows that the sample states' cybersecurity-related policies incorporate the scholarly themes better

than the planning documents. Thus, cybersecurity-related policies may be leading planning on responsiveness to best practices rather than the other way around. In most policy areas, state planning documents can lag the demands on policy. While creating a coherent plan takes a long time, cybersecurity issues and the nature of cyber-attacks are constantly changing. For this reason, the issue areas of cybersecurity policies may be more the result of the evolving events as state governments feel the pressure to respond immediately through policymaking. In turn, these policy areas may impact the state cybersecurity plans. Importantly, the sampling method may have contributed to this result of policies driving the plans. This research chooses sample states with high cyberattack incidence. Those are precisely the states that may be acting in response to cyber-attacks more directly, whether they have previously published plans for these actions, or not.

6.4.2 Policy-Planning Correspondence Based on the NIST Cybersecurity Framework Functions

In contrast to planning documents, cybersecurity-related legislative policies of the sample states do not directly refer to the NIST framework. The reason for not explicitly addressing the NIST Framework is likely due to the perception of the NIST Framework as a roadmap for planning rather than actual policy. Nevertheless, cybersecurity-related legislative policies incorporate items that address the functions identified by NIST. With the exception of New York, all sample states cover at least three NIST functions in their policies. This implies that states may still consider the NIST functions when creating cybersecurity-related policies, or that these functions are seen as important quite apart from the endorsement by NIST.

Table 6.5 A Comparison of Planning Documents and Cybersecurity-related Policies based on NIST Functions of Sample States

State	Corresponding NIST Functions	NIST Functions Covered Only in the Planning Documents	NIST Functions Covered Only in the Enacted Policies
California	Identify, Protect, Detect, Respond		Recover
Delaware	Identify, Protect	Recover	Respond
Florida	Identify, Protect, Respond	Recover	Detect
Maryland	Identify, Protect, Detect, Respond, Recover		
Montana	Identify, Protect, Detect, Respond, Recover		
New York	Identify, Protect	Detect, Respond, Recover	
Virginia	Identify, Protect, Detect, Respond	Recover	
Wyoming			Identify, Protect, Respond

The cross-state analysis of cybersecurity-related legislative policies was also conducted with regard to the incorporation of the NIST Cybersecurity Framework functions. Table 6.5 describes the distribution of NIST Cybersecurity Framework functions in three categories for each sample state. The Corresponding NIST Functions column shows the functions that are addressed by both the planning documents and cybersecurity-related policies. The second column, NIST Functions Covered Only in the Planning Documents, shows the NIST Functions that are covered in the planning documents but not in the policies. Finally, the third column, NIST Functions Covered Only in the Enacted Policies, shows the NIST Functions that are covered in the enacted policies but not in the planning documents. For instance, the State of California addresses *identify, protect, detect,* and *respond* functions both in its latest planning documents and in its enacted cybersecurity-related policies from 2015 to 2021. Thus, these functions are located in the Corresponding Themes column. While California addresses the *recover* function in its policies, it does not address the *recover* function in the plans. Thus, it is located in the NIST Functions Covered Only in the Enacted Policies column. Finally, California's plans do not address any functions that its policies do not cover (See Table 6.5).

The cross-state analysis of cybersecurity-related legislative policies finds that *identify* and *protect* functions are addressed by all eight sample states. On the other hand, the *recover* function is the least covered function in policies whereas it is the second least covered in the planning documents. This finding resembles the order of most frequently covered NIST functions in states' cybersecurity planning documents (See Figure 5.1 in Chapter 5).

The sample states' planning documents and policies present a similar level of compliance with NIST functions. For Maryland and Montana, all five functions are addressed by both the planning documents and policies. In California and Wyoming, the enacted policies comply with more NIST functions than the states' planning documents. While California planning documents have four corresponding NIST functions, its legislated policies also address the *recover* function. In contrast, Wyoming has no corresponding NIST functions, but its policies address the *identify*, *protect,* and *respond*. In the cases of New York and Virginia, the compliance with NIST functions is higher in planning documents than in the enacted policies.

6.5 Categorization of Sample States Based on Their Cybersecurity-related Policies

This section explores the sample states' cybersecurity-related policies in further detail. This section discusses the sample states in three groups based on the level of incorporation of the eight scholarly themes and the NIST functions in their legislated policies.

6.5.1 States of California-Maryland-Montana

The States of California, Maryland, and Montana are categorized under the same subtitle because their policies incorporate the eight scholarly themes and the five NIST functions. However, they still have unique conditions.

The successful incorporation of all eight scholarly themes and the five NIST functions by the cybersecurity-related legislative policies of the State of California is not surprising. Table 6.1 of this chapter shows that, in the case of California, there is a substantial and effective legislative effort to promote cybersecurity. The State enacted 22 laws and introduced but failed to approve 23 additional cybersecurity-related

policies from 2015 to 2021. Due to the strategic importance of cybersecurity and data privacy for the IT sector businesses operating in California, the state government is pioneering state-level cybersecurity-related policies. Many of its enacted policies are leading the state-level cybersecurity legislation activities in the country. For instance, the legal involvement of states in cybersecurity policy-making began with the California data privacy and breach notification law of 2003 (Glennon, 2012). More recently, in 2018, the State of California adopted the first Internet of Things (IoT) cybersecurity law, which aims to protect connected devices such as smart home devices against cyberattacks that threaten user information (California S.B. 327, 2018). Even the Federal Government passed IoT law two years after than California in 2020.

Similarly, the State of Maryland demonstrates intensive legislative efforts, with 26 enacted and 70 introduced but not approved cybersecurity-related policies from 2015 to 2021. The peak number of proposed but not approved policies is 2020, which might be due to the COVID-19 pandemic. Even though the policies are frequent and comprehensive, the planning documents of Maryland fail to address five scholarly themes: *awareness*, *better equipment*, *funding*, *leadership*, and *national security.* This implies that in the case of Maryland, the policies lead the planning documents and not vice versa.[17] The comprehensive and successful cybersecurity-related policies based on both the scholarly criteria and the NIST functions are not surprising. Like

[17] Because the methodology of this research excludes the planning documents that are published after 2020, the research does not include a 2021 planning document of Maryland. This recently published plan shows that some of the themes addressed in the policies are adopted into the plans after legislation.

California, the State of Maryland also hosts many tech companies for which state-level cybersecurity is strategically important. Besides the business sector, Maryland's cybersecurity matters greatly for the national government and its agencies as well. For instance, a recent cybersecurity summit in Annapolis, MD, in 2021 featured federal leaders from the White House, Congress, the National Security Agency (NSA), and the FBI (Kirby, 2021). Thus, there is a cybersecurity action culture in California and Maryland that requires rapid legislative response on issues that correspond to and go beyond of planning.

Along with the partnership with federal agencies, the state of Maryland also engages in partnership with many local higher education institutes. The policy examples provided under the *partnership* theme earlier in the chapter evidence this cooperative effort with academia. Similarly, cybersecurity professionals from the University of Maryland Baltimore County were also participants in the aforementioned cybersecurity summit.

The legislative activities of the State of Montana are far less extensive than those of both California and Maryland, with seven enacted and two introduced but not approved cybersecurity-related policies from 2015 to 2021. Montana addresses many scholarly themes and NIST functions with relatively few cybersecurity-policies. For instance, the policy example provided under the *funding* theme earlier in this chapter shows that only one cybersecurity-related policy of the State of Montana addresses five scholarly themes and four different NIST functions. The successful incorporation of all eight scholarly themes and five NIST functions might be surprising for a small state case of Montana. Montana was selected as a sample state because of its high cybersecurity job supply index, which also explains its comprehensive and successful

cybersecurity-related policies (See Chapter 3). Andy Hanks, the CISO of Montana, emphasized the recruitment of skilled cybersecurity professionals as state employees in an interview in 2020:

> The low supply and high demand in the cybersecurity job market makes it difficult to retain and recruit skilled and diverse cybersecurity staff. According to CyberSeek, there are about 600 open cybersecurity positions in Montana and 520,000 open cybersecurity positions in the U.S. I believe these numbers will trend higher each year as more organizations realize that cybersecurity is a business problem, and a strong cybersecurity staff is critical to compete in a global business market and global threat environment. In Montana, the Legislature allocated $2 million to retain and recruit skilled and diverse cybersecurity staff by increasing salaries and training budgets, and implementing flexible work. This has enabled us to retain existing staff and helped us recruit additional staff on the national job market (Lohrmann, 2020).

While the quote above refers to 600 open positions related to cybersecurity in the state of Montana, this number is much less than the average number of open cybersecurity positions per person in the nation. Thus, Montana is doing relatively well in terms of its cybersecurity public employment, which supports that it has a high cybersecurity job supply index, as shown in Figure 3.3 in Chapter 3.

6.5.2 States of Florida-Virginia

The States of Florida and Virginia's cybersecurity-related legislative policies cover seven scholarly themes and four NIST functions. While they address the same functions: *identify, protect, detect,* and *respond,* they differ about the one scholarly theme missing in their planning documents. Florida's policies address all scholarly themes except *national security,* whereas Virginia's policies address all scholarly themes except *partnership.*

Similar to California and Maryland cases, both Florida and Virginia engage in cybersecurity-related legislative activities to a great extent. For instance, Florida enacted 19 and introduced but did not approve 30 cybersecurity-related policies while Virginia enacted 40 and introduced another 41 policies from 2015 to 2021.[18] The high level of legislative activities might be due to the fact that Virginia is a key federal government hub. Arguably more so than Maryland, Virginia's cybersecurity has strategic importance in terms of national security because it hosts many federal organizations related to security. Florida hosts many tech industries such as Gartner, Nielsen, UKG, Tech Data, L3Harris, and Lockheed Martin each with at least 10,000 employees that require constant cybersecurity update.

6.5.3 States of Delaware-New York-Wyoming

This final category of sample states includes the states whose cybersecurity-related legislative policies cover the least number of scholarly themes and NIST functions. The states of Delaware, New York and Wyoming are somewhat surprising cases as well as exceptions to the overall research findings.

The cybersecurity-related policies enacted by the state of Delaware cover four scholarly themes and three NIST functions. Furthermore, Delaware is the only sample state whose planning documents cover all eight scholarly themes, but its policies do not. This is an exception to the overall research finding that policies are more comprehensive and prioritized than plans with regard to the scholarly themes. Thus, the state of Delaware, might rely more on executive orders and agency-based policies

[18] Both these states are large, southern, and traditionalistic in terms of their political culture.

in promoting their cybersecurity, rather than legislation. For example, Delaware's Department of Technology and Information publishes its twenty-five cybersecurity related non-legislative policies on its official website.[19]

In the case of New York, the cybersecurity-related policies cover four scholarly themes and two NIST functions. Surprisingly, the State of New York enacted only one cybersecurity-related policy between 2015 and 2021, whereas it introduced but failed to approve 33 policies. This extremely low enacted policy number meant that the state has the second-lowest correspondence between its plans and policies among all eight sample states. While its planning documents address five scholarly themes and its policies cover four, only the *partnership* theme exists in both. This low correspondence also exists with regard to NIST functions. One of the reasons for enacting just one policy in the New York case is that the state gives more authority to state agencies and their directors to regulate cybersecurity compared to the other sample states. In other words, similar to Delaware, the State of New York also organizes its cybersecurity with administrative policies rather than legislation. For instance, in 2021, the States' Office of Information Technology Services published 10 cybersecurity-related administrative policies on its official website.[20]

The cybersecurity-related policies enacted by the state of Wyoming cover three scholarly themes and three NIST functions. However, the research finds no correspondence with respect to both scholarly themes and NIST functions due to its planning documents that are located in the minimal coverage category in Chapter 4. In

---

[19] See https://dti.delaware.gov/technology-services/standards-and-policies.

[20] See https://its.ny.gov/ciso/policies/security.

other words, the state does not produce substantial cybersecurity planning documents and enacted few cybersecurity-related policies. From 2015 to 2021, Wyoming enacted three cybersecurity laws and introduced but failed to approve three cybersecurity-related policies. Overall, there was a low level of legislative activity as compared with other sample states. The logic behind including Wyoming as a sample state is its high victim loss index (See Chapter 3). This research hypothesizes that states with high cybersecurity loss index attribute more significance to cybersecurity planning documents and legislative policies. However, the case of Wyoming implies that the victim loss index can be high due to poor cybersecurity planning and policies.

The low level of legislative activity in Wyoming consistent with its political culture. The individualist culture refers to a minimalistic approach to the government and priority of marketplace in arranging social affairs. So, "… it is easy to see how outside governmental regulation — whether it is introduction of wolves, restrictions on snowmobiling in Yellowstone, limiting resource development on public lands, whatever — is resented" (King, 2014). The sceptic approach towards government activities explains low legislative efforts in not only the realm of cybersecurity but virtually all policy areas.

6.6 Conclusion

By exploring the landscape of cybersecurity-related legislative policies of the sample states, this chapter finds that the number of enacted policies varies greatly, from 1 (NY) to 40 (VA) to be specific, between 2015 and 2021. On the one hand, the states with the low number of policies, such as New York, have many cybersecurity-related policies that were introduced but not enacted. On the other hand, states like Delaware might regulate this field with executive orders or administrative policies.

Thus, low legislation number does not necessarily imply low cybersecurity-related policy activities. In answering the third research question, how sample states incorporate the best practices into their cybersecurity-related policies, a theme-based analysis was conducted. Overall, the chapter finds that most states incorporate the best practices in their policies to a high degree. For instance, California, Maryland, and Montana's cybersecurity-related policies cover all eight scholarly themes and the five NIST functions. The analysis finds the most frequently addressed scholarly theme is *coordination and communication* whereas the least addressed one is *national security* in the sample states cybersecurity-related legislative policies. In terms of the incorporation of the NIST functions, the analysis finds that the *identify* and *protect* functions are the most frequently addressed whereas the *recover* function is the least addressed one in the policies.

In answering the fourth research question, the chapter finds that the cybersecurity policies in sample states highly correspond to their latest cybersecurity planning documents in terms of the incorporation of the scholarly themes and NIST functions. More than half of the sample states, namely California, Delaware, Florida, Montana, and Virginia, address at least four scholarly themes in both their planning documents and cybersecurity-related policies. Furthermore, all sample states except for New York and Wyoming have at least three NIST functions corresponding between their plans and policies.

Surprisingly, the chapter finds that the enacted policies cover more scholarly themes than the state's planning documents with the exceptions of Delaware and New York. This unexpected finding implies that state policies might lead cybersecurity planning. In other words, states might perform cybersecurity-related legislations as a

result of cyber incidents and constantly evolving attacks. The next chapter further discusses the implications of these findings.

Chapter 7

CONCLUSION

This research analyzed cybersecurity-related planning documents and legislative policies of U.S. state governments as of 2021. The section below summarizes the research findings and discusses the conclusions with respect to the four research questions. The chapter proceeds with a description of the research contributions to state-level cybersecurity scholarship. The analysis then reviews implications and recommendations for state cybersecurity planners and policy makers. The closing sections identify research limitations and future research that might address these limitations.

7.1 Research Findings and Conclusions

The first research question is: W*hat are the characteristics of cybersecurity planning documents of 50 states adopted as of December 2021?* Exploring this question focused the research on describing the landscape of state planning documents. The research confirms that all states engage in cybersecurity planning to some extent. State level planning for cybersecurity is now part of the typical responsibilities being carried out by state governments across the U.S. This is a relatively new and growing activity with states apparently responding to increasing levels of cybersecurity threats or potential threats. New cybersecurity risks that come with technological developments such as connected systems also increase state

government responsibilities because these technological changes embody new potential threats that could impact citizens as well as public and private organizations.

This research demonstrates that there is significant variation across states in planning document types, the level of centralization in approaching cybersecurity planning, and the target groups identified in planning documents. The majority of States plan their cybersecurity either as part of their state information technology (IT) plans or as a separate cybersecurity specific planning document. A smaller number of states (10) provide cybersecurity planning information only on their official websites. Furthermore, the majority of states adopt a centralized cybersecurity planning approach that assigns cybersecurity planning to specific state government agencies rather than delegating that responsibility to their local governments. Finally, all state cybersecurity plans target the public sector and, a majority also target private sector. A small number of states also focus on cybersecurity issues for citizens. Contrary to the initial research expectations, the variations across planning document types, levels of centralization of responsibility, and target audiences do not seem to correspond to regional differences, differences in population or geographic size, or to prevailing political culture.

The lack of uniformity implies that states tailor their cybersecurity plans specifically to perceived state specific needs. That said, part of the variation may be due to the fact that cybersecurity is still an emerging area of state responsibility and that states are engaging these new responsibilities at different rates. The lack of correspondence to regional differences, population, state size, or political culture confirms that this emerging area of state responsibility is not evolving in a consistent manner based on traditional factors to account for state variations.

The second research question is: *In what ways do cybersecurity planning documents of 50 states incorporate the best practices defined by the scholarly criteria and the 2018 NIST Cybersecurity Framework?* There were six main findings with regard to this research question. First, the research shows that virtually all states incorporate the scholarly themes into their planning documents either by acknowledging the issue or by including a specific action plan to address the issue. Most states with a separate cybersecurity specific planning document cover themes in-depth with a specific action plan whereas states that give cybersecurity planning information only on their websites superficially acknowledge the scholarly themes but do not provide an action plan. Second, amongst the eight scholarly themes, states incorporate the *training* and *partnership* themes most frequently whereas the *national security* theme is addressed least frequently. The frequency of the *training* theme likely reflects an "education function" that is typically a state responsibility and an expectation that improved knowledge among target audiences will increase cybersecurity. On the other hand, states might consider improvements in national security beyond their responsibilities.[21] Third, states incorporate some of the themes in pairs. For instance, the *partnership* and *coordination and communication* themes go hand in hand with 0.78 R correlation as overlapping issue areas. Based on this correlation, the research concludes that states seeking partnerships also clarify what

[21] When analyzing the *national security* theme, this research assesses whether the state level cybersecurity plans and policies explicitly acknowledge the context of national security and their benefit to national interest. While many states' plans and policies do not cover the *national security* theme explicitly, this does not mean they do not pursue cybersecurity plans and policies intended to improve national security. From a broader perspective, many state level cybersecurity plans and policies are intended to serve national security interests although they are not labeled as such.

type of coordination and communication mechanisms will facilitate those partnerships. Fourth, in terms of the NIST functions, the research reveals that the *identify* function is the most frequently covered, whereas the *detect* and *recover* functions are the least covered (See Figure 5.1). The research implications section below discusses the consequences of neglecting the *detect* and *recover* functions. Fifth, the level of state incorporation level of the scholarly themes also indicates how well they incorporate the NIST functions. In other words, there is a significant correlation between the coverage of scholarly themes and the coverage of NIST functions. As a result, there is an immense gap between pioneering states (that incorporate both scholarly themes and the NIST functions) and lagging states that incorporate few of either type of best practice. Because the state level cybersecurity responsibilities are relatively new, some states have yet to catch up to recognized planning standards. Sixth, the plans of model states, namely Rhode Island, Connecticut, and Virginia, incorporate all of the scholarly themes, deliberately use a standardized and accurate terminology which corresponds with the NIST Cybersecurity framework, provide detailed action plans, and include a historical self-assessment of their cybersecurity posture. Revealing these common practices of model states is significant because they provide lessons for other states' planning documents.

The third research question is: *In what ways do cybersecurity policies adopted between 2015 and 2021 legislative sessions of states with high cyberattack figures incorporate best practices as defined by the scholarly criteria and the 2018 NIST Cybersecurity Framework?* The research finds that there is a high level of legislative policy activity among the sample states, indicating a growing importance of cybersecurity as a policy issue. Most states have introduced, and some have approved

significant numbers of legislation between 2015-2021. This finding is parallel to the increased level of cybersecurity planning noted above. These high levels of legislative activities indicate a trajectory towards more cybersecurity specific governance at the state level. The growth of state responsibilities increases the likelihood that states will create separate departments of cybersecurity, as some have already done, rather than leaving cybersecurity as a part of the responsibilities of state IT departments.

Most states incorporate best practices in their policies to a high degree. For instance, California, Maryland, and Montana's cybersecurity-related policies cover all eight scholarly themes and the five NIST functions. Similar to planning documents, this categorization of the sample states based on their policy incorporation of best practices does not correspond with their political culture. The research concludes that the new nature of cybersecurity related issues requires states to go beyond their political culture to provide solutions. Thus, not only states that welcome state regulations based on progressive values but also more conservative states demonstrate high levels of legislative activity and incorporate best practices in cybersecurity policy making.

In their cybersecurity-related legislative policies, sample states most frequently address *coordination and communication* theme. The legislative policies about the division of labor and reporting responsibilities of specific state officials indicate that states are still in the process of managing cybersecurity communication and responsibility allocation. Similar to planning documents, cybersecurity policies address *national security* least frequently. In terms of the incorporation of the NIST functions, the analysis finds that the *identify* and *protect* functions are the most frequently addressed whereas the *recover* function is the least addressed one in the

policies. The absence of policies to address the *recover* function means that most states lack a clearly defined roadmap to follow after a cyber incident.

The fourth research question is: I*n what ways do the cybersecurity policies in the sample states correspond to their latest cybersecurity planning documents as of the end of the 2021 legislative session*? This research finds a high level of correspondence between sample states' cybersecurity-related planning documents and policies. The plans and policies of most sample states, namely California, Delaware, Florida, Montana, and Virginia, correspond with one another in addressing at least four scholarly themes. Furthermore, all sample states except for New York and Wyoming have at least three NIST functions corresponding between their plans and policies. Thus, the research concludes that states' cybersecurity planning and policy making are consistent with one another.

The research also finds that the enacted policies cover more scholarly themes than the state's planning documents in all samples states except Delaware and New York. Thus, the best practice status of state cybersecurity legislative policies is better than state planning documents. It appears that state policies might respond to ongoing cyber incidents and constantly evolving attacks to a greater degree than to its own cybersecurity planning. The reason for this might be the nature of planning and policy making timeframes. In many issue areas, state planning documents often lag the demands on policy because it takes a long-while to create a coherent plan. However, the policy needs change to address emerging needs even while the planning process is taking place. Thus, the importance of particular areas of cybersecurity may be more the result of the evolving incidents, threats, and developments than the state plans. Importantly, the research's purposeful sampling may have contributed to this result

since the sample concentrates on states with high cyberattack incidence. Those are precisely the states that may be acting in response to cyber-attacks more directly than to their own longer-term plans. Overall, the research findings conclude that cybersecurity policies often lead planning rather than the other way around.

In contrast to high correspondence between best practice incorporation levels, the research finds that cybersecurity-related planning documents and policies do not align with one another in terms of the most frequently covered scholarly criteria. The *training* theme is most frequently addressed one in the cybersecurity-related planning documents, but it is the second least frequently addressed one in the cybersecurity-related legislative policies. The lesser coverage of the *training* theme in legislative policies might be because states address this training issue in their administrative policies. In many cases, cybersecurity training programs for state officials are voluntary, and voluntary training programs may require only administrative policies rather than legislative action. The opposite case is valid for the *funding* theme which is the second most frequently mentioned theme in policies but the second least frequently mentioned theme in the planning documents. Based on this research, states avoid designating a certain budget obligation for cybersecurity expenses in their planning documents; however, states are aware of the significance of cybersecurity funding, and in most states legislative action is required to provide funding.

7.2 Research Contributions

There is an enormous gap in the literature on the subject of state government cybersecurity planning and policy making. This deficiency is partially overcome by studies and reports from consulting companies, centers and institutes, professional associations, and private IT and cybersecurity firms (Norris et al., 2019; 2020).

However, these non-scholarly works, while valuable, do not provide a systemic and analytical approach to the issue. This research provides the first comprehensive state-level cybersecurity planning document inventory. The research documents a huge variation in states' planning document types and levels of incorporation of best practices.

Prior to this research there were many criteria scattered in various publications for the definition of best practices in state level cybersecurity planning and policy making. This research provides a systematic analysis of the incorporation of best practices which combines these issue-area specific recommendations from the scholarship with overall guidelines from the 2018 NIST Cybersecurity Framework. By doing so, this research contributes the most complete set of assessment criteria for state cybersecurity planning and policymaking. Since cybersecurity is a dynamic and still emerging challenge, the best practice standards to assess planning and policy making must evolve and change. Therefore, the best practices framework used in this analysis is not intended as a definitive set of standards for the future but only as a benchmark as of 2021. That benchmark should be adjusted to reflect changing cybersecurity requirements and needs.

By conducting a cross-state analysis among 50 states, this research offers a categorization of states' cybersecurity planning documents based on the incorporation levels of the Best Practices Framework. This categorization shows how cybersecurity planning documents of each state compares to those of other states in terms of their level of coverage. This research also provides a cybersecurity legislative policy inventory that enables assessment of the correspondence between the planning documents and policies for the sample states. This correspondence analysis is the first

scholarly effort in revealing the cybersecurity planning and policy making relationship, which appears to be different from the expected pattern of planning being the prime guide for cybersecurity policy. Indeed, based on this research, it appears that policy is often the leading edge.

7.3 Research Implications for State Cybersecurity Planning and Policy

There are significant implications of this research for state level cybersecurity planning and policies.

First, while the research finds a high compliance with the NIST cybersecurity functions, the *detect* and *recover* functions have been neglected by many states' planning documents and policies. This neglect implies that states are in danger of noticing cyber-attacks only after they experience negative consequences of an attack. State planners and policy makers should incorporate the *detect* function in their plans and policies in order to recognize attacks as early as possible and thereby enable actions to reduce impacts and costs of the attacks. Similarly, the failure to address the *recover* function in state plans and policies means that states often lack a clearly defined roadmap to follow after a cyber incident. As the Director of the Cybersecurity and Infrastructure Security Agency (CISA) Jen Easterly states:

> It is increasingly difficult in this highly digitalized, highly connected world we live in to prevent a cyber-attack from happening. So, the more you are prepared for it, the more you are able to respond and recover and mitigate risk and damage to your networks the better off you'll be (quoted from Ott, 2022).

States should prepare recovery strategies, principles, and mechanisms. For instance, North Carolina determined that it will not pay a ransom to cyber criminals by passing a no-ransom bill. Thus, in the aftermath of a cyber-attack, that state's officials

will no longer have to deal with the question of whether it will pay for ransom demands. States can improve their planning and policies by identifying the responsible actors and recovery steps after a cyber incident, as well as the coordination and communication required among different decisionmakers. This type of preparedness is typically expected for recovery from natural disasters and that knowledge might be adapted to develop increase preparedness for recovery from cyberattacks.

The field of cybersecurity itself is rapidly changing towards a more comprehensive conceptualization of cybersecurity issues. Specifically, there is increasing interest in cybersecurity preparedness and recovery plans as well as direct responses to attacks. To address this broader context, the term cybersecurity is often replaced by the term "cyber resilience." The latter term incorporates expectations about the ongoing adjustments needed to deal with the broader domains of preparedness and recovery. Looking ahead, states will likely adjust plans and policies to reflect this broader resilience perspective.

Second, state planners should emulate the plans of model states, namely Rhode Island, Connecticut, and Virginia. Beyond incorporating the Best Practices Framework in its entirety, states' planning documents should also use a standardized and accurate terminology which corresponds with the NIST Cybersecurity Framework. The lessons drawn from the model states also include providing detailed action plans that are designed to be implemented in the case of cyber attacks. Finally, including a historical self-assessment of states' cybersecurity posture is critical to identify the unique ways in which states can improve their cybersecurity and address past issues specific to their needs.

Third, the research attributes a leadership role for the National Association of State Legislatures and the National Governor's Association to promote partnership among the states and between the state and the federal governments. They should organize meetings, workshops, and discussion boards for governors, state cybersecurity leaders, and policy makers more often.[22] The Federal Government, with the help of CISA, should partner with the states more directly on the incorporation of best practices. While the NIST Cybersecurity functions provide an overall frame of reference, it proposes neither models nor regulations for state plans and policies. Some states like Connecticut bring up the limited partnership with the Federal Government in their planning documents:

> Connecticut and other states may borrow from the NIST Cybersecurity Framework terminology and processes to discuss the subject and start a dialogue, but federal standards and determination of adequate performance currently do not exist. If states want to establish standards and seek compliance with them, they have to do that without the benefit of federal guidelines (Connecticut Public Utilities Regulatory Authority, 2014, p. 8).

As seen in this quote, some states consider the NIST framework and other federal guidelines inadequate in establishing standards and fostering state compliance. Thus, the federal government should provide more detailed standards and several model options for state cybersecurity plans and policies. While the NIST framework is typically adopted by state government organizations, it is designed for all organizations from all sectors who are part of the critical infrastructure of cybersecurity.

---

[22] According to the official website of NGA, they organize cybersecurity policy academies and workshops only once a year. See https://www.nga.org/statecyber/

Fourth, state policy makers can draw several lessons from this research. On the one hand, being a pioneering state in cybersecurity issues can attract businesses, specifically tech-industries, and promote public trust. Because cybersecurity firms constitute a growing industry, states have incentives in attracting them. The high number of legislative activities in states such as California and Florida signal to tech-companies that the state government is sensitive to cybersecurity issues and willing to meet the potential cybersecurity needs of the private sector. On the other hand, a large number of cybersecurity plans and policies can be interpreted as the indicators of a highly regulatory state policy environment that some companies would like to avoid. Whether state sensitivity to cybersecurity is an attraction or a discouragement might depend on the needs and priorities of particular companies in different sectors. Furthermore, high legislative activity also fosters a cybersecurity culture and awareness. Creating a cybersecurity culture is necessary because it is an integral part of the information culture of society (Malyuk & Miloslavskaya, 2016). It is hoped that this research will contribute to the effort of developing a cybersecurity culture by creating awareness state cybersecurity plans and policies and increased understanding of how they may be strengthened.

Last, the research conclusions also suggest that state policy makers should respond to immediate cybersecurity needs as well as plans. Amongst the sample states, California, Maryland, and Montana incorporate all scholarly themes and the NIST functions into their policies but not into their planning documents. These sample states indicate that cybersecurity needs could be time-sensitive, and policies should be prioritized in taking action to meet those needs. This also means that state

cybersecurity planning is a continuing process which requires ongoing updates in response to emerging challenges.

7.4 Limitations

This research has several limitations. Foremost, many important questions about state cybersecurity planning and policy remained beyond the scope of the research because of the lack of access to primary data and the absence of in-depth state case studies.

First, because of the sensitivity of the topic and privacy concerns, state officials usually avoid publishing all of their administrative policies. Thus, the policy data of this research is limited to cybersecurity-related legislations. Furthermore, cybersecurity managers in state governments are often reluctant to talk about their cybersecurity concerns, efforts, and policies because that information might compromise cybersecurity requirements. Also, most private organizations that conduct surveys with state government cybersecurity leaders do not want to share their experiences with other parties. Ironically, both state officials and private organizations that conduct surveys with them always mention that this field needs a strong collaboration with academia. The absence of such collaboration makes access to needed information and date for research difficult and responses to interviews and surveys unreliable. On top of the sensitivity of cybersecurity issue, the COVID-19 pandemic restrictions also prevented establishing in person connections to conduct interviews and carry-out surveys.

In the absence of publicly available systemic data on administrative policies, and given the obstacles to interview or survey data, this research relied on public data

of available cybersecurity planning documents and policies. That public data does not provide a full picture of state cybersecurity planning or policy.

Second, this research does not examine why cybersecurity planning documents and policies were developed in each state as they were. In other words, the research does not answer why specific states address certain cybersecurity-related issues in their planning documents and policies whereas others do not. The lack of in-depth state case studies with survey and/or interview data restricted the research from exploring these questions.

Third, this research does not study whether and how the plans and policies were funded and implemented. The research focuses on published plans and legislated policies without analyzing their financing, implementation, and evaluation. Thus, whether the plans and policies were effective in addressing the cybersecurity challenges faced by the states is left for future research.

7.5 Future Research

Future research can further explore the relationship between cybersecurity planning and policy making at the state-level. While this research finds a high correspondence between policies and plans in terms of the incorporation of the Best Practices Framework, the mechanisms in which this correspondence occurs remain unclear. Future research should provide more detailed analyses about on how policy makers and planners produce cybersecurity policies and plans. A focus on leadership and agency would highlight the actors who play a pioneering and determinative role in crafting cybersecurity plans and policies. It may also shed light on how state level cybersecurity plans and policies are intended to be interconnected. Future research can also test the implications of this research and find out whether policies really drive

plans in state level cybersecurity, and under what conditions. In other words, do planners design cybersecurity related planning documents to justify recently enacted policies? What are the consequences of making policies that are not informed with thorough cybersecurity planning documents? One anticipated consequence is that state policies may become highly fragmented and, over time, less effective.

Future research can extend these state-level analyses to an assessment of correspondence between the federal and state government plans and policies. To what extent do planning documents and policies at the state level correspond with those of federal government?

This descriptive analysis explores the landscape of states cybersecurity planning documents and policies by analyzing publicly available data. Thus, this research answers some of the "how" questions about state cybersecurity planning documents and policies to provide a profile of the landscape for both. Future research, with interview and survey data, can answer "why" questions about the patterns revealed in this research. For instance, why do states develop their cybersecurity planning documents and policies as they do and why do those include certain priorities and not others? Do states like Delaware and New York rely more on administrative policies than legislative policies, and if so, why?

In terms of the NIST Cybersecurity Framework, this research finds that cybersecurity planning documents of many states comply with its functions and use the standardized language that NIST provides. However, the planning documents emphasize that the functions provide a framework and not precise guidelines. Future research can explore how state governments perceive the NIST framework and how useful the functions are for state level cybersecurity planners and policy makers.

Finally, future research can also address how the plans and policies were funded and whether they were implemented. The budget allocation to cybersecurity planning and policy making can signal how much importance states attribute to this issue. Future research can analyze how the plans and policies are funded and compare states budgets for cybersecurity. This is a challenging issue since the composition of a state's cybersecurity budget is not always easily determined and, in some cases, may even be concealed as a matter of security. Analysis of funding and implementation requires detailed case analysis. In addition to funding and implementation, future research should include policy evaluations that assess the effectiveness of adopted policies in addressing the cybersecurity challenges faced by the states.

REFERENCES

Alabama Office of Information Technology. (2017). *Information Technology Strategic Plan 2017-2020*.

Alexander, A., Graham, P., Jackson, E., Johnson, B., Williams, T., & Park, J. (2020). An Analysis of Cybersecurity Legislation and Policy Creation on the State Level. In K.-K. R. Choo, T. H. Morris, & G. L. Peterson (Eds.), *National Cyber Summit (NCS) Research Track* (Vol. 1055, pp. 30–43). Springer International Publishing. https://doi.org/10.1007/978-3-030-31239-8_3

Alibasic, A., Junaibi, R. A., Aung, Z., Woon, W. L., & Omar, M. A. (2016). Cybersecurity for Smart Cities: A Brief Review. *Data Analytics for Renewable Energy Integration*, 22–30. https://doi.org/10.1007/978-3-319-50947-1_3

Andreasson, K. J. (Ed.). (2012). *Cybersecurity: Public sector threats and responses*. CRC Press.

Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals. *Journal of Legal, Ethical and Regulatory Issues; Arden*, *16*(1), 7–14.

Atoum, I., Otoom, A., & Abu, A. A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, *22*(3), 251–264. https://doi.org/10.1108/IMCS-02-2013-0014

Barzilay, M. (2013). *A simple definition of cybersecurity*. https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Baylon, C. (2014). *Challenges at the Intersection of Cyber Security and Space Security* (p. 53). Chatham House. https://www.chathamhouse.org/sites/default/files/field/field_document/20141229CyberSecuritySpaceSecurityBaylonFinal.pdf

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber Security Policy Guidebook*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781118241530

Bergal, J. (2017, April 10). *Looking to the Feds for Help in Fighting Cybercriminals*. http://pew.org/2oaYEWD

Berry, F. S. (1994). Innovation in Public Management: The Adoption of Strategic Planning. *Public Administration Review*, *54*(4), 322–330. JSTOR. https://doi.org/10.2307/977379

Berry, F. S., & Wechsler, B. (1995). State Agencies' Experience with Strategic Planning: Findings from a National Survey. *Public Administration Review*, *55*(2), 159. https://doi.org/10.2307/977181

Bhaskar, R. (2006). State and local law enforcement is not ready for a cyber Katrina. *Communications of the ACM*, *49*(2), 81–83. https://doi.org/10.1145/1113034.1113075

Blomquist, D. M. (2020). *Comparing Centralized and Decentralized Cybersecurity in State and Local Government* [M.S., Utica College]. https://www.proquest.com/docview/2407282316/abstract/178958BA04264E66PQ/1

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–41.

Bruer, W., & Perez, E. (2016, August 29). Officials: Hackers breach election systems in Illinois, Arizona. *CNN*. https://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/index.html

Bryson, J. M. (2011). *Strategic planning for public and nonprofit organizations: A guide to strengthening and sustaining organizational achievement* (4th ed). Jossey-Bass.

Bryson, J. M., Berry, F. S., & Yang, K. (2010). The State of Public Strategic Management Research: A Selective Literature Review and Set of Future Directions. *The American Review of Public Administration*, *40*(5), 495–521. https://doi.org/10.1177/0275074010370361

Buckland, B. S., Schreier, F., & Winkler, T. H. (2015). *Democratic Governance Challenges of Cyber Security* (p. 50). https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

California General Assembly, Bill: AB1906, 2018 Regular Session, Chapter 860 (2018). https://legiscan.com/CA/text/AB1906/id/1807167

California General Assembly, Bill: AB1044, 2019 Regular Session, Chapter 106 (2019a). https://trackbill.com/bill/california-assembly-bill-1044-elections-secretary-of-state/1699471/

California General Assembly, Bill: AB89, 2020 Regular Session (2020). https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB89

California General Assembly, Resolution: SR54, 2019 Regular Session (2019b). https://trackbill.com/bill/california-senate-resolution-54-relative-to-national-cybersecurity-awareness-month/1765820/

CAN-SPAM Act, no. PUBLIC LAW 108–187, 108th Congress (2003). https://www.govinfo.gov/content/pkg/PLAW-108publ187/pdf/PLAW-108publ187.pdf

Caruson, K., MacManus, S. A., & McPhee, B. D. (2012a). Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. *Jhsem*, *9*(2), 1–22. https://doi.org/10.1515/jhsem-2012-0003

Caruson, K., MacManus, S. A., & McPhee, B. D. (2012b). Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. *Jhsem*, *9*(2), 1–22. https://doi.org/10.1515/jhsem-2012-0003

Cavelty, M. D. (2010). Cyber-Security. In J. P. Burgess (Ed.), *The Routledge handbook of new security studies* (pp. 154–162). Routledge.

Cavelty, M. D. (2015). Cyber-Security and Private Actors. In R. Abrahamsen & A. Leander (Eds.), *Routledge Handbook of Private Security Studies* (1st ed., pp. 89–99). Routledge. https://doi.org/10.4324/9781315850986-10

CBS News. (2012, October 31). *3.6 million South Carolina tax returns hacked*. https://www.cbsnews.com/news/36-million-south-carolina-tax-returns-hacked/

Center for Digital Government. (2014). *The Future of IT in State and Local Government.* [White Paper]. Center for Digital Government. http://www.vion.com/documentlibrary/downloadDocument.aspx?id=70

Choi, S. O. (2008). Emergency Management: Implications from a Strategic Management Perspective. *Journal of Homeland Security and Emergency Management*, *5*(1). https://doi.org/10.2202/1547-7355.1372

Clark, R. M., & Hakim, S. (2017). Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security. In R. M. Clark & S. Hakim (Eds.), *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level* (pp. 1–17). Springer International Publishing. https://doi.org/10.1007/978-3-319-32824-9_1

Cohen, N., & Nussbaum, B. (2018). *Cybersecurity for the States: Lessons from Across America*. 58.

Connecticut Public Utilities Regulatory Authority. (2014). *Cybersecurity and Connecticut's Public Utilities*. Connecticut Public Utilities Regulatory Authority.

Coulson, T., Mason, M., & Nestler, V. (2018). Cyber Capability Planning and the Need for an Expanded Cybersecurity Workforce. *Communications of the IIMA*, 12.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review; Ottawa*, *4*(10), 13–21.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (Fifth edition). SAGE.

Currey, M., Raymond, M., & Connecticut Department of Administrative Services. (2018). *2018 Cybersecurity Update*. Connecticut Department of Administrative Services.

Davis, J. S., Libicki, M. C., Johnson, S. E., Kumar, J., & Karode, A. (2016). *A Framework for Programming and Budgeting for Cybersecurity*. RAND Corporation.

Dawson, G., & Desouza, K. C. (2015, March 5). How state governments are addressing cybersecurity. *Brookings Institution*. https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*(1), 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x

Delaware Department of Technology and Information. (2016). *Statewide Information Technology Strategic Plan*. Delaware Department of Technology and Information.

Delaware General Assembly, Bill: SB153, 2020 Regular Session (2020). https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx

Deloitte and National Association of State Chief Information Officers (NASCIO). (2010). *State governments at risk: A call to secure citizen data and inspire public trust*. https://www.nascio.org/Portals/0/Publications/Documents/Deloitte-NASCIOCybersecurityStudy2010.PDF

Deloitte and National Association of State Chief Information Officers (NASCIO). (2012). *2012 Deloitte-NASCIO Cybersecurity Study—State Governments at Risk: A Call for Collaboration and Compliance*. https://www.nascio.org/Portals/0/Publications/Documents/Deloitte-NASCIOCybersecurityStudy2012.pdf

Deloitte and National Association of State Chief Information Officers (NASCIO). (2014). *2014 Deloitte-NASCIO Cybersecurity Study—State Governments at Risk: Time to Move Forward*. https://www.nascio.org/Portals/0/Publications/Documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf

Deloitte and National Association of State Chief Information Officers (NASCIO). (2016). *2016 Deloitte-NASCIO Cybersecurity Study—State Governments at Risk: Turning Strategy and Awareness into Progress*. https://www.nascio.org/Portals/0/Publications/Documents/2016/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf

Deloitte and National Association of State Chief Information Officers (NASCIO). (2018). *2018 Deloitte-NASCIO Cybersecurity Study—States at risk: Bold plays for change*. https://www.nascio.org/Portals/0/Publications/Documents/2018/2018DeloitteNASCIOCybersecurityStudyfinal.pdf

Department of Innovation and Technology. (2017). *State of Illinois Cybersecurity Strategy 2017-2019*. Department of Innovation and Technology. https://www2.illinois.gov/sites/doit/Strategy/Cybersecurity/Pages/cybersecurity.aspx

Department of Management Services of Florida. (n.d.). *Cybersecurity Task Force / Other Programs / Florida Department of Management Services—DMS*. Retrieved May 3, 2021, from https://www.dms.myflorida.com/other_programs/cybersecurity_task_force

Devine, C., & Griffin, D. (2018, August 14). *6 million Georgia voters' records exposed: "Could have easily been compromised" - CNN Politics*. CNN. https://www.cnn.com/2018/08/14/politics/georgia-brian-kemp-voter-data/index.html

Devivo, M. (2014, August 5). *North Carolina National Guard: Preparing Cyber Warriors for state and national duty*. National Guard. https://www.nationalguard.mil/News/Article/576283/north-carolina-national-guard-preparing-cyber-warriors-for-state-and-national-d/

Domestic Security Oversight Council. (2020). *Florida Domestic Security Strategic Plan 2021-2023*.

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? *Journal of Information Policy*, *9*, 280–306. JSTOR. https://doi.org/10.5325/jinfopoli.9.2019.0280

Eichensehr, K. E. (2016). Public-Private Cybersecurity. *Texas Law Review*, *95*(3), 467–538.

Elazar, D. (1991). *Exploring federalism* (1. paperback ed). Univ. of Alabama Press.

Elazar, D. (1994). *The American mosaic: The impact of space, time, and culture on American politics*. Westview Press.

Falessi, N., Gavrila, R., Klejnstrup, M. R., & Moulinos, K. (2012). *National Cyber Security Strategies: Practical Guide on Development and Execution* (p. 45). https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

Federal Communications Commission. (2012). *Cyber Security Planning Guide* (p. 45). Federal Communications Commision. https://www.fcc.gov/sites/default/files/cyberplanner.pdf

Feiman, J. (2019, September 11). *Can STEM Qualifications Hold The Key To The Future Of Cybersecurity?* Forbes. https://www.forbes.com/sites/forbestechcouncil/2019/09/11/can-stem-qualifications-hold-the-key-to-the-future-of-cybersecurity/

Freeman, D. B. (2022, May 6). Why Local Governments Are a Target for Cyber Attacks and Steps to Prevent It. *Governing*. https://www.governing.com/sponsored/why-local-governments-are-a-target-for-cyber-attacks-and-steps-to-prevent-it

Garcia, J. T. (2020). *Status of Cybersecurity Memorandum*.

Garcia, M., Forscey, D., & Blute, T. (2017). Beyond the Network: A Holistic Perspective on State Cybersecurity Governance Symposium. *Nebraska Law Review*, *96*(2), 252–280.

Geers, K. (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal: A Global Perspective*, *18*(1), 1–7. https://doi.org/10.1080/19393550802676097

Georgia Technology Authority. (n.d.). *Georgia Cyber Summit*. Georgia Technology Authority. Retrieved July 12, 2022, from https://gta.georgia.gov/cybersecurity-1/georgia-cyber-summit

Ghernouti-Hélie, S. (2010). A National Strategy for an Effective Cybersecurity Approach and Culture. *2010 International Conference on Availability, Reliability and Security*, 370–373. https://doi.org/10.1109/ARES.2010.119

Gibson, W. (1984). *Neuromancer*. Ace Books.

Giles, K., & Hagestad, W. (2013). Divided by a common language: Cyber definitions in Chinese, Russian and English. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, 1–17. https://ieeexplore-ieee-org.udel.idm.oclc.org/document/6568390

Glennon, M. J. (2012). *State-Level Cybersecurity* (SSRN Scholarly Paper ID 1997565). Social Science Research Network. https://papers.ssrn.com/abstract=1997565

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology & People*, *22*(2), 92–108. https://doi.org/10.1108/09593840910962186

Goodin, D. (2009, May 5). *Hackers demand $10m ransom for Virginia medical data*. https://www.theregister.com/2009/05/05/virginia_medical_records_extortion/

Goodyear, M., Goerdel, H., Portillo, S., & Williams, L. (2010). *Cybersecurity Management In the States: The Emerging Role of Chief Information Security Officers* (SSRN Scholarly Paper ID 2187412). Social Science Research Network. https://papers.ssrn.com/abstract=2187412

Government of Montenegro. (2013). *National Cyber Security Strategy for Montenegro 2013-2017* (p. 27). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Montenegro_2013_Cyber%20Security%20Strategy%20for%20Montenegro.pdf

Governor's Office of Homeland Security. (n.d.). *Cybersecurity and Critical Infrastructure Protection*. Retrieved July 12, 2022, from https://gohs.maryland.gov/va/

Gulick, L. (2015). Notes on the Theory of Organization. In J. M. Shafritz & A. C. Hyde (Eds.), *Classics of public administration* (8th ed, pp. 105–113). Cengage Learning.

Harknett, R. J., & Stever, J. A. (2009). The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal of Homeland Security and Emergency Management*, *6*(1). https://doi.org/10.2202/1547-7355.1649

Harknett, R. J., & Stever, J. A. (2011). The New Policy World of Cybersecurity. *Public Administration Review*, *71*(3), 455–460. https://doi.org/10.1111/j.1540-6210.2011.02366.x

Hendrick, R. (2003). Strategic Planning Environment, Process, and Performance in Public Agencies: A Comparative Study of Departments in Milwaukee. *Journal of Public Administration Research and Theory*, *13*(4), 491–519. https://doi.org/10.1093/jpart/mug031

Huang, K., & Pearlson, K. (2019). *For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture*. 10.

Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: A case study. *The Journal of Supercomputing*, *74*(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2

Indiana Executive Council on Cybersecurity. (2018). *Indiana Cybersecurity Strategic Plan*. Indiana Executive Council on Cybersecurity.

Janairo, E. (2002). States fight against cyber-terrorism. *Homeland Security*, 2.

Jose, K. (2008, July 16). Obama Adds "Cyber Security" to National Defense Plan. *Observer*. https://observer.com/2008/07/obama-adds-cyber-security-to-national-defense-plan/

Kansas Cybersecurity Task Force. (2021). *Kansas Cybersecurity Task Force Interim Report*. Kansas Cybersecurity Task Force.

Karakoç, M. (2017). Understanding the Barriers to Addressing Cybersecurity Challenges in American State and Local Governments [M.A.P., University of Delaware]. In *ProQuest Dissertations and Theses*. http://search.proquest.com/pqdtlocal1006271/docview/2001286247/abstract/EA38593F93434C3FPQ/1

Kemp, R. L. (Ed.). (2010). *Homeland security: Best practices for local government* (2nd ed). International City/County Management Association.

Kerschberg, B. (2011, April 26). *Don't Mess With Texans' Personal Data—Texas Comptroller's Massive Data Breach Will Cost State Millions*. Forbes. https://www.forbes.com/sites/benkerschberg/2011/04/26/dont-mess-with-texans-personal-data-texas-comptrollers-massive-data-breach-will-cost-state-millions/

Khouzani, MHR., Malacaria, P., Hankin, C., Fielder, A., & Smeraldi, F. (2016). Efficient Numerical Frameworks for Multi-objective Cyber Security Planning. In I. Askoxylakis, S. Ioannidis, S. Katsikas, & C. Meadows (Eds.), *Computer Security – ESORICS 2016* (pp. 179–197). Springer International Publishing.

King, J. (2014, February 18). *Wyoming's Political Culture: Our own but not unique*. WyoFile. http://wyofile.com/wyomings-political-culture-unique/

Kirby, D. (2021, July 30). *Maryland is launching these 5 cyber initiatives to better secure state data*. Technical.Ly. https://technical.ly/civic-news/hogan-maryland-cyber/

Knell, N. (2012, October 29). *South Carolina Breach Compromises Millions of Records*. https://www.govtech.com/security/South-Carolina-Breach-Compromises-Records.html

Lewis, J. A., Porrúa, M. A., & García de Alba Díaz, A. C. (2016). *Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States*. Inter-American Development Bank. https://doi.org/10.18235/0000420

Liaropoulos, A. (2015). Securing the Human in the Era of Cyberphobia: Securing the Human in the Era of Cyberphobia. *Journal of Information Warfare*, *14*(4), 15–24. JSTOR.

Liebowitz, M. (2011, April 12). *Data Breach Exposes 3.5 Million Social Security Numbers*. NBC News. https://www.nbcnews.com/id/wbna42555471

Liu, C.-W., Huang, P., & Lucas, H. C. (2016). IT Governance, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2850178

Lohrmann, D. (2012). *Cybermania: How do you spell cyber... everything?* https://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cybermania-How-do-you-081212.html

Lohrmann, D. (2017a). *Ransomware in Government: Who, What, When, Where and How?* http://www.govtech.com/blogs/lohrmann-on-cybersecurity/ransomware-in-government-who-what-when-where-and-how.html

Lohrmann, D. (2017b, April 10). *Government Ransomware: Stories and Tips*. LinkedIn Pulse. https://www.linkedin.com/pulse/government-ransomware-stories-tips-dan-lohrmann

Lohrmann, D. (2017c, April 15). *Will Congress Help Fund New State and Local Cyber Programs?* http://www.govtech.com/blogs/lohrmann-on-cybersecurity/will-congress-help-fund-new-state-and-local-cyber-programs.html

Lohrmann, D. (2020, November 13). *Montana CISO Shares State Security Actions and Priorities*. GovTech. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/montana-ciso-shares-state-security-actions-and-priorities.html

Louisiana Cybersecurity Commission. (2018). *Louisiana Cybersecurity Commission (Strategy Map)*. Louisiana Cybersecurity Commission. https://lacybercommission.la.gov/wp-content/uploads/2018/07/Strategy-Map-Louisiana-Cybersecurity-Commission.pdf

Luiijf, E., Besseling, K., & Graaf, P. D. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, *9*(1/2), 3. https://doi.org/10.1504/IJCIS.2013.051608

Macmanus, S. A., Caruson, K., & Mcphee, B. D. (2013). Cybersecurity at the Local Government Level: Balancing Demands for Transparency and Privacy Rights. *Journal of Urban Affairs*, *35*(4), 451–470. https://doi.org/10.1111/j.1467-9906.2012.00640.x

Malloy, D. P. (2017). *Connecticut Cybersecurity Strategy*.

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

Marquis, C., & Battilana, J. (2009). Acting globally but thinking locally? The enduring influence of local communities on organizations. *Research in Organizational Behavior*, *29*, 283–302. https://doi.org/10.1016/j.riob.2009.06.001

Maryland General Assembly, Bill: SB943, 2021 Regular Session, Chapter 683 (2021a). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/sb0943?ys=2021RS

Maryland General Assembly, Bill: SB49, 2021 Regular Session (2021b). https://legiscan.com/MD/bill/SB49/2021

Maryland General Assembly, Bill: SB0542, 2015 Regular Session (2015). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/sb0542?ys=2015RS&search=True

McQuade, S. C. (2006). *Understanding and managing cybercrime*. Pearson/Allyn and Bacon.

Merrill, M. (2009, May 2). *Hacker says he stole confidential medical data on 8 million Virginia residents | Healthcare IT News*. https://www.healthcareitnews.com/news/hacker-says-he-stole-confidential-medical-data-8-million-virginia-residents

Minnesota IT Services. (2018). *Information Security Strategic Plan*. Minnesota IT Services.

Mississippi Department of Information Technology Services. (2019). *Mississippi Department of Information Technology Services Annual Report*. Mississippi Department of Information Technology Services.

Mississippi Department of Information Technology Services. (2020). *Strategic Master Plan for Information Technology*. Mississippi Department of Information Technology Services.

Missouri Office of Administration. (2020). *OA Cyber Security Plan FY 2020*. Missouri Office of Administration. https://cybersecurity.mo.gov/files/plans/OCS%20Strategic%20Plan%20FY2020%20public.pdf

Montana General Assembly, Bill: HB2, 2019 Regular Session, Chapter 483 (2019). https://leg.mt.gov/laws/advanced_agenda/?chamber=H&agenda_dt=03-19-2019&agendano=1&session_id=20191

Montana State Information Technology Services Division. (2018). *State of Montana Information Technology Strategic Plan 2018-2020*.

NASCIO. (2015). *State IT Workforce: Facing Reality with Innovation*. http://new.nascio.org/Portals/0/Publications/Documents/NASCIO_StateITWorkforceSurvey2015_WEB.pdf

National Governors Association. (2020, April 30). NGA Selects 7 States to Focus on Advancing Statewide Cybersecurity. *National Governors Association*. https://www.nga.org/news/selction-seven-states-advancing-cybersecurity/

Nelson, A. C., & French, S. P. (2002). Plan Quality and Mitigating Damage from Natural Disasters: *A Case Study of the Northridge Earthquake with Planning Policy Considerations*. *Journal of the American Planning Association*, *68*(2), 194–207. https://doi.org/10.1080/01944360208976265

New Jersey Office of Homeland Security & Preparedness. (2021). *New Jersey Cybersecurity & Communications Integration Cell Cybersecurity Strategic Plan 2021-2025*.

Newcombe, T. (2011, December). Hacking Pleasantville: What happens when cybercriminals attack computers in small-town America? *Governing: The States and Localities*, *25*(3), 48–50.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST Cybersecurity White Paper; p. NIST Cybersecurity White Paper). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2018). Cybersecurity at the Grassroots: American Local Governments and the Challenges of Internet Security. *Journal of Homeland Security and Emergency Management*, *15*(3). https://doi.org/10.1515/jhsem-2017-0048

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. *Public Administration Review*, *0*(0). https://doi.org/10.1111/puar.13028

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2020). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, 1–23. https://doi.org/10.1080/07352166.2020.1727295

Norris, D., Mateczun, L., Joshi, A., & Finin, T. (2017). *Cybersecurity 2016 Survey Summary Report of Survey Results*. https://doi.org/10.13016/M2TB0Z004

North Carolina Department of Information Technology. (2020). *Annual Report.*

Obama, B. H. (2009, May 29). Text: Obama's Remarks on Cyber-Security. *The New York Times*. https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html

Office of Virginia's Secretary of Technology. (n.d.). *Virginia's Innovation Ecosystem: The Trusted Leader in Growing Cyber Security Solutions*.

Oregon Enterprise Security Office. (2018). *Statewide Information Security Plan*.

Ostrom, V. (1991). *The meaning of American federalism: Constituting a self-governing society*. ICS Press.

Ott, M. C. (2022, February 7). Governors Look at Preparing for and Responding to a Cyber Crisis. *National Governors Association*. https://www.nga.org/news/commentary/governors-look-at-preparing-for-and-responding-to-a-cyber-crisis/

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (Fourth edition). SAGE Publications, Inc.

Pfeiffer, M. H. (2015). *Managing Technology Risks Through Technological Proficiency: Guidance for Local Governments*. https://doi.org/10.7282/T3TT4T5H

Ponemon Institute. (2015). *State of Cybersecurity in Local, State & Federal Government*. https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-2563enw.pdf

Privacy Rights Clearinghouse. (2018). *Privacy Rights Clearinghouse: Data Breaches*. https://www.privacyrights.org/data-breaches

Rainie, H., & Wellman, B. (2012). *Networked: The new social operating system*. MIT Press.

Reddick, C. G. (2010). Impact of Citizen Relationship Management (CRM) on Government: Evidence from U.S. Local Governments. *Journal of E-Governance*, *33*(2), 88–99. https://doi.org/10.3233/GOV-2010-0216

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, *27*(2), 23–39.

Rosner, E. (2017). *Cyber federalism: Defining cyber's jurisdictional boundaries*. 127.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2017.1476

Shoemaker, D., Kohnke, A., & Sigler, K. (2019). What the Profession of Cybersecurity Needs to Know and Do. *EDPACS*, *59*(2), 6–18. https://doi.org/10.1080/07366981.2019.1565106

Spidalieri, F. (2015). State of the States on Cybersecurity. *Pell Center for International Relations and Public Policy*, 42.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063

State of California. (n.d.). *CDT | CA Dept of Technology*. Retrieved July 12, 2022, from https://cdt.ca.gov/

State of Connecticut. (2018). *Cybersecurity Action Plan*. State of Connecticut.

State of Hawaii. (2012). *Information Assurance and Cyber Security Strategic Plan*. https://ets.hawaii.gov/wp-content/uploads/2012/09/Governance_Info-Assurance_Cyber-Security.pdf

State of Iowa. (2016). *State of Iowa Cybersecurity Strategy*.

State of Iowa. (2019). *State of Iowa Cybersecurity Strategic Plan*.

State of Michigan. (2015). *Michigan Cyber Initiative*.

State of Oregon Enterprise Information Services. (2021). *Oregon Cyber Disruption Response & Recovery: Voluntary Resource Guide for Local Government*. State of Oregon Enterprise Information Services.

State of Rhode Island. (2019). *Rhode Island State Cybersecurity Strategy*.

Steiss, A. W. (2003). *Strategic management for public and nonprofit organizations*. Marcel Dekker.

Stone, A. (2014). *State and Local Governments Try to Fix the Cybersecurity Staff Problem*. http://www.governing.com/news/headlines/state-and-local-Governments-dont-have-the-cybersecurity-staff-they-want.html

Stubley, D. (2013, June 7). What Is Cyber Security? *7 Elements*. https://www.7elements.co.uk/resources/blog/what-is-cyber-security/

Techconnect. (2019). *West Virginia Cybersecurity Workforce Strategic Initiative Report*.

Texas Department of Information Resource. (2020). *Information Security Plan*. https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=5

Texas Department of Information Resources. (2022). *State Strategic Plan for Information Resources Management: Accelerating the Next Generation of Technology in Texas*.

The Florida Center for Cybersecurity. (2020). *2020 Cyber Florida Annual Report*.

Theofanos, M. F., Stanton, B., Furman, S., Prettyman, S. S., & Garfinkel, S. L. (2017). *Be Prepared: How US Government Experts Think About Cybersecurity*. https://doi.org/10.14722/usec.2017.23006

Torres, K. (2015, December 15). *Report Gives Details on Massive Georgia Secretary of State Data Breach*. https://www.govtech.com/security/Report-Gives-Details-on-Massive-Georgia-Secretary-of-State-Data-Breach-.html

Truong, N., Jayasinghe, U., Um, T.-W., & Lee, G. M. (2016). A Survey on Trust Computation in the Internet of Things. *The Journal of Korean Institute of Communications and Information Sciences (J-KICS)*, *33*, 10–27.

U.S. Department of Homeland Security and National Association of State Chief Information Officers (NASCIO). (2017). *State Cybersecurity Governance Case Studies*. https://www.nascio.org/Portals/0/Publications/Documents/2018/DHS/State%20Cybersecurity%20Governance%20Cross%20Site%20Report.pdf

USA Patriot Act, no. 107–56, 107th Congress (2001).

Van Dine, A., Stoutland, P., & Assante, M. (2017). Outpacing Cyber Threats: Priorities for Cyber Security at Nuclear Facilities. *International Conference on Nuclear Security: Commitments and Actions. Summary of an International Conference. Companion CD-ROM*. http://inis.iaea.org/Search/search.aspx?orig_q=RN:50017480

Veiga, A. D. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *2016 SAI Computing Conference (SAI)*, 1006–1015. https://doi.org/10.1109/SAI.2016.7556102

Verizon. (2019). *2019 Data Breach Investigations Report*. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

Vermont Agency of Digital Services. (2019). *ADS Strategic Plan 2019*. Vermont Agency of Digital Services.

Vermont Agency of Digital Services. (2021). *ADS Strategic Plan 2022-2026*.

Virginia General Assembly, Bill: SB1121, 2015 Regular Session, Chapter 261 (2015a). https://lis.virginia.gov/cgi-bin/legp604.exe?151+ful+CHAP0261

Virginia General Assembly, Bill: HB1700, 2019 Regular Session, Chapter 854 (2019). https://lis.virginia.gov/cgi-bin/legp604.exe?191+sum+HB1700

Virginia General Assembly, Bill: HB852, 2020 Regular Session (2020). https://legiscan.com/VA/bill/HB852/2020

Virginia General Assembly, Bill: SB1121, 2015 Regular Session (2015b). https://lis.virginia.gov/cgi-bin/legp604.exe?151+sum+SB1121

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wamala, F. (2011). *ITU National Cybersecurity Strategy Guide*. International Telecommunication Union. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

Ward, M., & Brunner, M. (2020). *Stronger Together: State and Local Cybersecurity Collaboration* (p. 11). NGA and NASCIO. https://www.nascio.org/resource-center/resources/stronger-together-state-and-local-cybersecurity-collaboration/#:~:text=The%20publication%20outlines%20promising%20programs,local%20government%20officials%20on%20cybersecurity.

Warner, M. (2012). Cybersecurity: A Pre-history. *Intelligence and National Security, 27*(5), 781–799. https://doi.org/10.1080/02684527.2012.708530

Weiss, J., Perkins, E., & Walls, A. (2013). *Definition: Cybersecurity*. Gartner Research. https://www.gartner.com/en/documents/2510116

West Virginia Office of Technology. (2014). *West Virginia Office of Technology Strategic Plan 2014-2017*. West Virginia Office of Technology.

Whitmer, M. G. (2007). *IT Security Awareness and Training: Changing the Culture of State Government*. NASCIO. https://www.nascio.org/wp-content/uploads/2019/11/NASCIO-ITSecurityAwarenessAndTraining.pdf

WikiLeaks. (2009, April 30). *Over 8M Virginian patient records held to ransom*. https://wikileaks.org/wiki/Over_8M_Virginian_patient_records_held_to_ransom,_30_Apr_2009

Williams, P. A. H. (2008). In a 'trusting' environment, everyone is responsible for information security. *Information Security Technical Report, 13*(4), 207–215. https://doi.org/10.1016/j.istr.2008.10.009

Wisconsin Department of Administration Division of Enterprise Technology. (2017). *State of Wisconsin Cybersecurity Strategy*.

Wolff, J., & Lehr, W. (2018). When Cyber Threats Loom, What Can State and Local Governments Do? *Georgetown Journal of International Affairs*, *19*(1), 67–75. https://doi.org/10.1353/gia.2018.0008

Wood, C. (2013, May 20). *California Launches Cybersecurity Task Force*. GovTech. https://www.govtech.com/em/safety/California-Launches-Cybersecurity-Task-Force-052013.html

Wylder, J. O. (2003). Improving Security from the Ground Up: Moving toward a New Way of Enforcing Security Policy: Encouraging Personal Accountability for Corporate Information Security Policy. *Information Systems Security*, *11*(6), 29–38. https://doi.org/10.1201/1086/43324.11.6.20030101/40429.6

Wyoming General Assembly, Bill: HB0001, 2018 Regular Session, Chapter 134 (2018). https://www.wyoleg.gov/Legislation/2018/HB0001

Appendix

LINEAR REGRESSION ANALYSIS OF THE COVERAGE OF SCHOLARLY THEMES

The table below shows the linear regression results that coverage of NIST functions positively and significantly impact the coverage of scholarly themes. Whereas other control variables such as Digitalization Score, State Integrity, Per capita Income, Victim Loss Index, and Cybersecurity Job Supply do not significantly impact the coverage of scholarly themes at p<.05 level.

VARIABLES	Scholarly Themes
NIST	0.924***
	(0.158)
Digitalization Score	-0.115
	(0.184)
State Integrity	0.289
	(0.229)
Per capita Income	-0.000
	(0.000)
Victim Loss Index	-0.026
	(0.843)
Cybersecurity Job Supply	-0.866*
	(0.509)
Constant	3.682
	(2.689)
Observations	50
R-squared	0.493
ll	-101.3

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1