View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Walden University

Walden University ScholarWorks

Walden Dissertations and Doctoral Studies

Walden Dissertations and Doctoral Studies Collection

2019

Cybersecurity Policy Development at the State Level: A Case Study of Middle Tennessee

Daniel Leslie Scherr
Walden University

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

Part of the Databases and Information Systems Commons, and the Public Administration Commons

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

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Daniel Leslie Scherr

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. David Milen, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Christina Spoons, Committee Member,
Public Policy and Administration Faculty

Dr. Tanya Settles, University Reviewer,
Public Policy and Administration Faculty

The Office of the Provost

Walden University
2019

Abstract

Cybersecurity Policy Development at the State Level: A Case Study of Middle Tennessee

by

Daniel Leslie Scherr

MBA, American Military University, 2013

BA, North Carolina State University, 1999

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

August 2019

Abstract

Cybersecurity is a growing threat not only to nations, critical infrastructure, and major entities, but also to smaller organizations and individuals. The growing number of successful attacks on all manner of U.S. targets highlights the need for effective and comprehensive policy from the local to federal level, though most research focuses on federal policy issues, not state issues. The purpose of this study was to examine the effectiveness of the decision-making process within the current cybersecurity policy environment in a southern state of the United States. Sabatier's advocacy coalition framework served as the theoretical framework for the study. Data were collected through 5 semistructured interviews with individuals who were either elected or appointed officials, emergency managers, or subject matter experts. These data were transcribed, then coded and analyzed with McCracken's analytic categorization procedure. Participants recognized that the federal government provides some resources but acknowledged that action at the state level is largely funded through the state resulting in a network of dissimilar policies and protocols in states across the country. Findings also revealed that state leadership in some locations better grasps what resources are needed and is more likely to earmark in order to plan for unanticipated cybersecurity needs of the public. Analysis of study data also highlighted areas for future study and identified needed resources or areas of opportunity for creating a more comprehensive and effective cybersecurity policy environment. Implications for positive social change include recommendations for state and federal decision makers to engage in community partnerships in order to more effectively protect the public from cybersecurity threats.

Cybersecurity Policy Development at the State Level: A Case Study of Middle Tennessee

by

Daniel Leslie Scherr

MBA, American Military University, 2013

BA, North Carolina State University, 1999

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

August 2019

Acknowledgements

First and foremost, I would like to give thanks to the Lord, through whom all things are possible.

Secondly, I would like to thank the love of my life and my inspiration, Dr. Tanya Scherr. We have known each other for 30 years, but you still never cease to amaze me. Thank you for your support, prodding, guidance, and love throughout our Master and Doctoral programs, and our lives outside of school, as well. Thank you for believing in me and never giving up. You are the love of my life and there is no way I could have accomplished any of this without you.

Next I would like to thank our children, Caitlyn, Heather, Paige, Tyler, and Nicholas, for their unending love and support throughout this process. I spent many nights, and mornings, and days, hunched over a keyboard instead of playing games, going outside, or otherwise spending as much time with you as I wanted. Thank you for supporting me and providing inspiration to complete this process and not lose hope. I love you all dearly and you mean the world to me.

Of my family I would also like to thank my parents, Doris Latour, Dr. Emile Latour, Cathy Scherr, and Leslie Scherr. Your support and love throughout this process, and my entire life, has helped me achieve this and everything else in my life. Thank you for setting my path, guiding when I am astray, and helping to motivate me when needed. Thank you also to Peter Rizzi for your support and, most especially, for your daughter.

I would also like to thank my dissertation chair, Dr. David Milen, for your continued support, patience, and flexibility in helping me navigate this process. This was a long process, and I thank you for your unceasing efforts and guidance along the way that helped me reach this point. I greatly appreciate the time invested on the phone, via emails, and in person at the different residencies. Thank you also to Dr. Christina Spoons for your insight, guidance, and constructive criticism throughout the process. Thank you to Dr. Tanya Settles, my URR, for your hard work and dedication to making all the students better. Thank you also to Dr. Tara Kachgal with Form and Style. I do not know how you are able to read and edit so quickly, but thank you for all your efforts and feedback.

Finally, thank you to Rich Schoeberl and the rest of the faculty at Martin Methodist College for their support, guidance, and encouragement during this process. Thank you also to all those participating in this study both directly and indirectly.

Table of Contents

Chapter 1: Introduction to the Study

Introduction

The threat of cyberattacks and the need for effective defenses against these attacks are now part of everyday life around the world for major government entities as well as individual citizens. Attacks may come in the form of hacks committed against companies or agencies at the local, state, or national level; spam e-mail or *phishing* attacks aimed at theft of personal information; or communication and coordination of terror attacks. For as much as these threats are discussed as an emerging trend, it should be noted that they have existed in one form or another for at least 50 years. The beginning decades of the Internet, threats were mitigated by barriers to entry for hackers and the limited connectivity of different networks and systems. As the Internet flourished, so too did attacks, threats, and competency of hackers. In recent years, and especially since the September 11, 2001 (9/11) attacks, the ability of terrorists and state actors to utilize computers and other devices to coordinate and execute attacks has emerged as a primary focus of computer defense efforts (Kallberg & Thuraisingham, 2013). These threats are not just increasing in number, but also in complexity and origin. As threats evolve, there is an intensifying need to adjust techniques to address such threats.

The global population is rapidly transitioning aspects of daily life from face-to-face interactions onto the Internet for a variety of functions. Leeuw and Leeuw (2012) stated that in 2011 over 2.1 billion users were using the Internet, a figure that increased 500% since 2000, and has only increased in the last few years. Such an increase in volume both provides a larger target audience for attacks and more space for hackers and others to hide behind. Hackers and other malicious actors and organizations benefit from the added volume as the sheer volume complicates the defense of networks proactive measures taken to identify potential hostile actions. Those who pursue criminals and terrorists on the Internet, primarily intelligence agencies and law enforcement, require the ability to identify potential problems, conduct surveillance, and address threats. With the increasing complexity and ubiquity of electronic devices and the number of technology savvy users, additional tools and permissions are needed to defend against cyberattacks.

The modern phase of cybersecurity policy and procedures began in the immediate aftermath of the 9/11 terror attacks. When the details began to emerge about these attacks, lawmakers, members of the public, and others deliberated over the lengths to which the terrorists used Internet resources to coordinate their movements and plans. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, commonly referred to as the Patriot Act, was intended to close some of the identified holes in security and provide resources to address future threats. In crafting this sweeping and comprehensive legislation, legislators sought to address weaknesses in tracking terror financing, surveillance, law enforcement abilities, and coordination amongst the U.S. agencies charged with identifying and fighting terrorism, both online and on the ground (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001). This legislation was passed in a matter of weeks following the attacks, marking a significant inflection point in U.S. policy making. Such a large-scale policy can typically take years to put together and pass through the normal channels of policy making (see Electronic Privacy Information Center, n.d.), but the attacks compelled lawmakers to address the issue immediately.

The Patriot Act set forth a new era of permissions and authorizations for the fight against terrorism and cyberattacks and was primarily focused on issues at the federal level. The next major national policy was not published until 2011, in Presidential Policy Directive (PPD) 20. In PPD-20, the administration provided for two separate goals (safeguarding cyberspace and confronting those who would disrupt it) and identified areas where responsible agencies could conduct either defensive or offensive actions to counter those threats (International Strategy for Cyberspace, 2011). This policy, along with most other legislation and international laws, assumes that national-level agencies maintain some level of primacy in the fight against cyberattacks (Glennon, 2012). The federal government has several different initiatives under the Department of Homeland Security (DHS) to assist state and local governments with improving cybersecurity, but the initiatives remain a patchwork system. These programs range from voluntary membership in groups to help guide policy and educate the public to voluntary reporting of cyberattacks against individuals or interests (Cybersecurity and Infrastructure Security Agency, n.d.). Under this umbrella, each of the 50 states, along with local, territorial, and tribal governments, enact their own legislation, policies, and procedures to fight cyberterrorism and cyberattacks against their interests and citizens interests (Cybersecurity and Infrastructure Security Agency, n.d.).

The state of Tennessee has a diverse population in terms of its citizens, public and private entities, and infrastructure. The state legislature, in its governance of such a diverse base, is required to develop policies and procedures that can cover all contingencies, something that can be difficult considering the varied resources and populations included. Legislators have found it a challenge to draft cybersecurity laws to address concerns of large cities, small towns, urban, and rural areas alike. In conducting this inquiry, I sought to determine whether the current policy development process and decision-making framework meets the needs of the field agencies throughout the state. Tennessee has 95 counties, each with its own mayor and sheriff's department, in addition to over 200 police departments that serve as first responders for crime, terror, and cyberattacks. Across these entities, counties range from among the richest in the country to the poorest, with a wide array of social, educational, and cultural backgrounds (County Technical Assistance Service, n.d.). In this study I focused on four counties in Middle Tennessee: Davidson, Giles, Maury, and Williamson. Davidson County is home to Nashville, the state capitol, and is primarily an urban environment. Williamson is a suburban community with several more affluent and rapidly expanding areas (County Technical Assistance Service, n.d.). Giles and Maury County are primarily rural counties comprised mostly of small towns and agricultural lands (County Technical Assistance Service, n.d.).

Making policies and procedures to account for the different resource levels, infrastructure, and usage differences across these counties is a demanding task. The behaviors of the legislators can be described using the bounded rational choice theory. In this theory of policy setting and behavior, the actions of legislators is intended to be rational (McLean, 1991). However, several factors can influence the decision-making process, with emotion and attention standing out as the main causal factors (McLean, 1991) . The emotional aspect may encompass a range of influences, from the individual's personal beliefs on a subject to pressures posed by friends or colleagues on how to vote for a particular issue (McLean, 1991). These pressures can be the result of political party affiliation, activist positioning, or self-interests, to name a few. Attention is an important factor to consider when examining legislative decision-making as there are generally more issues being deliberated than a given legislature can manage at once (McLean, 1991) . This can provide an opportunity for small, vocal groups to take a larger role in setting the agenda than might otherwise be anticipated. Areas of interest that are believed to be under control or successfully managed might take less precedence than those believed to need more direct intervention in the near term, no matter the reality.

Background

Cybersecurity is an emerging topic in public discourse, but it is hardly a new phenomenon. The first concerns over computer security date back to the use of the first computers in government facilities in the 1960s. At that time, it was understood that multiple users on the same mainframe could access shared data, requiring standard clearance to certain systems or the removal of classified data after its use (Warner, 2012). That realization was followed, over the next three decades, by three additional insights, according to Warner (2012): “Computers can be hacked and data stolen, we can build computer attack into military arsenals, [and] others might do that to us – and perhaps already are” (p.782). These insights and realizations among U.S. leadership evolved along with the use and broader acceptance of computers for a wide range of uses. The ongoing threats and concerns over cybersecurity led to a series of national policies, culminating in the 1990s with the first national cybersecurity strategies and directives (Warner, 2012).

It was in this period of flux and policy development of the 1980s and 1990s that the events that led to September 11, 2001, occurred. The policies created under the USA PATRIOT ACT sought to close loopholes and provide intelligence and law enforcement with additional tools to combat the threats identified in that attack (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001). One of the lasting lessons of 9/11 was how well suited the Internet is for coordination and collaboration for terrorist groups. The lack of unified standards across the globe and the uneven enforcement of standards provide any number of loopholes for groups to create their own web pages or smaller sections in existing frameworks (Heidenriech & Gray, 2014). Al-Qaeda was known at the time of the law's passage to have an extensive Internet presence, a fact that was only reinforced during intelligence gathering efforts during the war in Afghanistan (Heidenriech & Gray, 2014).

In the years since 9/11, the usage of the Internet has grown, but there has not been a unified effort to close security gaps around the world. Certain regions and groups are seeking a more comprehensive stance, but there are loopholes and opportunities for terror groups and individuals in every country (Tripathi, 2015). Into this landscape, the United States inserted the Department of Defense's Cyber Command, several intelligence agencies, and the DHS, each with their own missions, rules of engagement, and virtual territories. Current legislation before Congress seeks to enhance the cooperation of DHS and the private sector, as private interests are believed to own and operate 95% of the information infrastructure in the United States (Tripathi, 2015). Although the United States has devoted a significant amount of resources to cybersecurity and will for the foreseeable future (Department of Homeland Security, 2019), it lacks both leadership for its cybersecurity efforts and a comprehensive policy for directing them.

Underneath this umbrella of federal agencies and policies, each of the individual states also manage cyberattacks. Under the current framework, federal agencies, especially the DHS, Secret Service, and Immigrations and Customs Enforcement, are the main conduit for investigation and pursuit of cyber criminals and terrorists who mount attacks against U.S. interests. Federal lawmakers have given states a certain amount of leeway in their prosecution of cyberattacks but have requested voluntary reporting to federal agencies if the activity falls within certain parameters. Specifically, if the attack could impact national security or interests; corrupt networks; or is a violation of federal or State, Local, Tribal, or Territorial (SLTT) law, a report is recommended (Department of Homeland Security Law Enforcement Cyber Incident Reporting Guide, 2016).

Law enforcement is viewed by the DHS as the first line of defense for responding to reports of cybercrime and conducting preliminary investigations. Furthermore, the DHS relies on the SLTT governments to “maintain systems and data, hire and train cybersecurity professionals, determine and enforce policy, and engage in cybersecurity awareness to develop a cyber-savvy public” (National Initiative for Cybersecurity Careers and Studies, 2016) With the escalating pace and rigor of cyberattacks at all levels of the government and against private citizens, there is a dearth of research on whether the current policy environment is sufficient for state agencies to combat this emerging threat. Existing research focuses on federal efforts to secure government websites and networks, not on policies and programs at the state level.

Problem Statement

Cybersecurity is a rapidly evolving issue across all walks of life and has direct impacts on states, individuals, corporations, and national interests (Cybersecurity and Infrastructure Security Administration, n.d.). Many news stories and research articles revolve around how national governments and private companies are fighting these attacks, with new information coming almost daily from around the world). However, U.S. states are also addressing cybersecurity issues, with at least 35 states passing over 312 laws on cybersecurity in 2018 and 2019 alone (National Conference of State Legislatures, 2019 (2)). There is much less understanding of how well the current policy environment suits field agencies at the state level. This gap in knowledge is important because such agencies play a pivotal role in addressing such threats. During 2018 and 2019, an average of 6 U.S. government agencies were reported hacked per month (Passeri, 2019). Due to the nature of cybersecurity and the sensitive nature of the information, the true number of attacks and the impact of those attacks remains unknown.

Purpose of the Study

The purpose of this study was to evaluate the current policy development and environment in Middle Tennessee regarding cybersecurity. The primary focus of the study was with federal policies and programs on cybersecurity; I tracked the guidance and resources provided from the federal government to the lower tiers of government. The federal government has primacy in addressing cybersecurity policy and enforcement, but the state and local governments also have a place in the process. I also sought to determine the impact of current policy development and enactment on cybersecurity agencies and operations at the state level, specifically in Tennessee. With the rapid evolution of cyber threats and their increased preeminence, the standard policy process can leave agencies without required tools and resources (President's Information Technology Advisory Committee, 2005). The terror attacks of 9/11 marked a significant increase in the tools and permissions granted to intelligence and law enforcement to identify, track, and pursue those involved in terrorist activity and cyberattacks. As the rate of attacks has increased in the intervening years, it is unclear whether the policies are keeping pace with the needs of the field agencies.

Research Questions

The main research question (Research Question 1) for this inquiry was whether the current cybersecurity policy at the federal level provides sufficient guidance and tools for the State of Tennessee, along with connecting state, county, and municipal governments. I analyzed study data to assess whether the current guidance meets the threats and structure of the state, or if the changing nature of the threats against the state require a different methodology to better support the field agencies. The secondary question (Research Question 2) centered on whether the current implementation of cybersecurity policies and programs match the original plans. Discrepancies can arise from a variety of factors, ranging from lack of resources or communication to conflicting organizational goals and legislative directives.

Theoretical Framework

As cybersecurity emerged as a topic of concern and importance for the United States, researchers have conducted numerous studies to clarify how policies came to be, what should happen next, and what needs to be done to fix the current state of the field. Although there are many perspectives on what is broken in the current cybersecurity system, how to fix it, and who is to blame for not having a better system, there is limited published research on how the policy decisions impact the operational field of cybersecurity, according to my review of the literature. This is particularly true regarding the decisions and framework at the state and local levels. I used the advocacy coalition framework (Sabatier, 1988) to evaluate the policy development and decision-making process around cybersecurity in Tennessee.

Paul Sabatier first described the advocacy coalition framework (ACF) in 1988. Sabatier derived this methodology from the works of several other scholars, including Heclo, Weiss, Mazmanian, and Ostrom, and sought to both synthesize their work and close identified gaps. In his readings and research, Sabatier stated that the higher-level influences included in established frameworks only captured part of the impact of the policy actors within the decision cycle (Sabatier, 1988). To improve upon these influences and dynamics of the policymaking process, Sabatier identified three different aspects of policy development: inclusion of subject matter experts and groups working in the targeted field; the use of feedback loops in the decision-making process; and recognition that interest groups in development cycles often behave similar to individuals, with corresponding beliefs and behaviors (Sabatier, 1988). Each of these aspects supplements the macro approach originally described by Heclo and helps to provide a much more thorough exploration of the policy development and decision-making process (Sabatier, 1988, p. 129-133).

When examining the cybersecurity framework and policy environment in Tennessee, it is important to understand how policy decisions are made by the legislators. I used Sabatier’s (1988) ACF outline as shown in Appendix A to examine in detail the wide range of influences, actors, events, interest groups, and learning behaviors that affect the policy making process. The policy subsystem is the area of the framework where Sabatier focused most of his attention, particularly the learning feedback loop. This subsystem includes policy analysts, subject matter experts, and others studying established policy to provide lessons learned, unintended consequences, and secondary impacts of the policy decisions (Sabatier, 1988). Use of the ACF requires at least a decade worth of data to properly capture the learning process for a given policy environment (Sabatier, 1988). For this study, I examined the United States’ cybersecurity policy from the 9/11 attacks onward.

Nature of the Study

I used a qualitative design and a case study approach. This research utilized multiple sources of information to evaluate the nature and scope of guidance and resources provided by federal cybersecurity policy to the states, specifically Tennessee. Further, it examined whether the operational policies and programs in the State of

Tennessee match the published policies and legislative vision. The first section of research included an in-depth examination of publicly available federal, state, and local policies, along with an outline of the various programs currently in use to improve communication and reporting among the states and localities.

Once I completed the policy analysis, I conducted targeted interviews with legislators and agency representatives to gain insight into the policy process. I requested interviews with the Senators and Representatives at the Federal and State levels, along with representatives from the governor's office, the state information officer, Safety and Homeland Security, the Tennessee Bureau of Investigation (TBI), the Tennessee Emergency Management Agency (TEMA), cybersecurity experts working with the State, County, and local governments, and the county executive offices of the four counties targeted for this study. I also contacted city leadership in each of the nine major cities located in the four targeted counties to solicit interviews for the study. The intent was to conduct interviews with every willing participant to gain a broad base of understanding into the policy environment, process, and operations across the geographic area. Interview questions included how threats are identified, what the follow-up procedures are, how success is measured, and who is included in the development of new and/or updated policies.

I collated and evaluated the interview responses to provide a more robust understanding of the current state of cybersecurity in Tennessee. The information from legislators provided details about policy development and what information feeds into the decision-making process surrounding cybersecurity. This can assist in shaping future discussions and policy development going forward, both within the current organization and ways to improve the process. The data gleaned from the field agencies was examined alongside the responses from the legislators to identify any gaps or convergences in their views of cybersecurity in Tennessee.

Definitions

Cybersecurity literature and discussions of policy decisions include a myriad of specialized definitions. Some key terms for this study and their definitions follow:

Attack: Any unauthorized activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself (Committee on National Security Systems, 2009.

Blue Team: A term signifying a group of individuals who serve as defenders in training exercises during planned exercises. This term also refers to groups brought in to harden commercial or third-party networks before attempted penetration by an authorized party (Committee on National Security Systems, 2009).

Chief information officer: The agency official responsible for (a) providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information systems are acquired and information resources are managed in a manner consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency; (b) developing, maintaining, and facilitating the implementation of a sound and integrated information system architecture for the agency; and (c) promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency (Committee on National Security Systems, 2009).

Computer network attack: Actions taken through use of computer networks to disrupt, deny, degrade, manipulate, or destroy computers, computer networks, or information residing in computers and computer networks (National Security Presidential Directive 54, 2008).

Computer network defense: Actions taken to defend against unauthorized activity within computer networks. These actions include monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities (Committee on National Security Systems, 2009).

Critical infrastructure: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on security, national economic security, national public health, or safety, or any combination of those matters (Committee on National Security Systems, 2009).

Cyberattack: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information (Committee on National Security Systems, 2009).

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (National Security Presidential Directive 54, 2008).

Cyberspace: A global domain within the information environment consisting of the interdependent network of information systems infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (Committee on National Security Systems, 2009).

Denial of service (DoS): The prevention of authorized access to resources or the delaying of time-critical operations. Time-critical may be milliseconds, or it may be hours, depending upon the service provided (Committee on National Security Systems, 2009).

Digital forensics: The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes (National Initiative for Cybersecurity Careers and Studies, n.d.).

Distributed denial of service (DDoS): A denial of service technique that uses numerous hosts to perform the attack (Committee on National Security Systems, 2009).

e-government (e-gov): The use by the U.S. government of web-based Internet applications and other information technology (Committee on National Security Systems, 2009).

Enterprise risk management: A comprehensive approach to risk management that engages people, processes, and systems across an organization to improve the quality of decision-making for managing risks that may hinder an organization's ability to achieve its objectives (National Initiative for Cybersecurity Careers and Studies, n.d.).

Exposure: The condition of being unprotected, thereby allowing access to information or access to capabilities that an attacker can use to enter a system or network (National Initiative for Cybersecurity Careers and Studies, n.d.).

Federal Information Processing Standard (FIPS): A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce (Committee on National Security Systems, 2009). A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability (Committee on National Security Systems, 2009).

Incident: An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system, or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies (Committee on National Security Systems, 2009).

Information assurance (IA): Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation (Committee on National Security Systems, 2009). These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (Committee on National Security Systems, 2009).

Information operations (IO): The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making processes, information, and information systems while protecting one's own (Committee on National Security Systems, 2009).

Information security (IS): The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Committee on National Security Systems, 2010).

Information system: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (United States Code 44, 2009).

Information system security officer (ISSO): An individual assigned the responsibility by the senior agency information security officer, authorizing official, management official, or information system owner of ensuring that the appropriate operational security posture is maintained for an information system or program (National Institute of Standards and Technology, 2017).

Investigation: A systematic and formal inquiry into a qualified threat or incident using digital forensics and perhaps other traditional criminal inquiry techniques to determine the events that transpired and to collect evidence (National Initiative for Cybersecurity Careers and Studies, n.d.).

Mitigation: The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences (National Initiative for Cybersecurity Careers and Studies, n.d.).

Network resilience: A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands (Committee on National Security Systems, 2009).

Passive attack: An actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations (National Initiative for Cybersecurity Careers and Studies, n.d.).

Penetration testing: A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system (Committee on National Security Systems, 2009).

Phishing: The act of deceiving individuals into disclosing sensitive personal information through deceptive computer-based means (Committee on National Security Systems, 2009).

Red Team: A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture (Committee on National Security Systems, 2009). The Red Team's objective is to improve enterprise information assurance by demonstrating what works for the defenders in an operational environment (Committee on National Security Systems, 2009).

Security policy: A rule or set of rules that govern the acceptable use of an organization's information and services to a level of acceptable risk and the means for protecting the organization's information assets (National Initiative for Cybersecurity Careers and Studies, n.d.).

Security test and evaluation (ST&E): Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system (Committee on National Security Systems, 2009).

Social engineering: An attempt to trick someone into revealing information (e.g., a password) that can be used to attack an enterprise (Committee on National Security Systems, 2009).

Supervisory Control and Data Acquisition System (SCADA): Networks or systems generally used for industrial controls or to manage infrastructure such as pipelines and power systems (Committee on National Security Systems, 2009).

Threat assessment: The product or process of identifying or evaluating entities, actions, or occurrences, whether natural or constructed, that have or indicate the potential to harm life, information, operations, and/or property (National Initiative for Cybersecurity Careers and Studies, n.d.).

US-CERT: A partnership between the DHS and the public and private sectors, established to protect the United States' Internet infrastructure (Committee on National Security Systems, 2009). US-CERT coordinates defense against and responses to cyberattacks across the nation (Committee on National Security Systems, 2009).

Assumptions

There were four main assumptions for this inquiry. The first and greatest assumption was that some level of access will be granted to both legislative and field offices to conduct the interviews. While each of the individuals included in the description of the study had a full schedule and many duties, I assumed that either the lead or a representative from each office would be made available to provide insight and a response for the inquiry.

The second assumption was that any feedback or information received would be a true and honest representation of the current operating environment to the best of the ability of the respondent. There are many reasons why responses could have been incomplete or not fully accurate. These include everything from an incomplete knowledge of the situation, a rushed response, conflicting loyalties, or suspicion of a lack of anonymity of the responses. I did not attempt to qualify responses or determine the veracity of each response. Multiple sources were targeted for this inquiry to help identify outliers and mitigate the potential impact of inaccuracies or incomplete information.

The third assumption was the current policy environment had a measurable or demonstrable impact on field agencies in Tennessee. With cybersecurity a rapidly evolving and high-visibility issue in the world today, any new policy could have a major impact. The last assumption was that each of the targeted individuals (legislators, subject matter experts, law enforcement officers) had some level of engagement with the cybersecurity environment. The legislators and law enforcement professionals have a wide range of demands on their time, but it was expected they would have at least a basic knowledge and understanding of the current policy and operational environment. The lack of resources available agencies to undertake all desired cybersecurity activities or programs was also assumed. It was hoped participants would provide wider insight into the challenges faced than simple lack of manpower, specialized training, or additional funding on their own.

Scope and Delimitations

Scope

This inquiry began with a brief exploration of the history of information security and cybersecurity policy from their inception until approximately 2000. The overview of these areas provided background about cybersecurity, framed current policy issues and concerns, and identified trends in security posture and oversight through the years. A more in-depth examination of the cybersecurity policy environment from 2000 through the 9/11 terror attacks, and the implementation of the USA Patriot Act and related legislation through 2003, was also conducted. This period provided insight into law enforcement and government attitudes on cybersecurity before 9/11 and the significant changes in legislation, oversight, and authority that originated from this period. The main focus of the inquiry traced the cybersecurity policy environment from this post-9/11 wave of legislation to the present day. The intervening span of 14 years met the ACF time requirement to capture the learning and feedback loops and allowed for tracking and identification of trends and changes within the environment. Department of Defense Policies and Organizations and the current federal priorities, issues, and pending legislation were also addressed to capture the emerging state of the federal policy environment. At that point, legislative actions since 2003 in the state of Tennessee were examined, along with current state operations, programs, and pending legislation. The differences or gaps between the federal and state policies and programs were used to create the interview instrument and shape the inquiry going forward.

The interviews, as noted previously, reached out to legislators, appointed officials, and subject matter experts of multiple tiers within three counties in the state of Tennessee. This included the Governor, state Chief Information Officer, county mayors and information officers, sheriffs, local mayors, chiefs of police, chief detectives, and cybersecurity professionals supporting or assigned to public agencies. If the principal for each if these offices was not available, representation from the offices was requested for the targeted interviews. Over 100 interviews were requested during this process. The information from the initial round of interviews was collated and analyzed to determine if any individuals stand out for follow up or additional requests. The interviews focused on policy development and engagement levels around cybersecurity by the participants, how well they feel the state's needs are being met, and any areas they felt should be improved.

Delimitations

The most important delimitations for this study were gaining Institutional Review Board permissions and presenting a clear and concise plan to the agencies targeted for inclusion. The Institutional Review Board, or IRB, is an organization within a university (Walden University IRB for this study) that ensures research conducted by students "complies with the university's ethical standards as well as U.S. federal regulations. IRB approval is required before collection of any data, including pilot data" (Walden University Center for Research Quality, n.d.). As noted in the subsequent discussion of limitations, gaining access and overcoming resistance of agency officials will be among the most significant hurdles. Being able to ensure the anonymity of all those involved in the study, along with providing information on what information will be collected and how it will be used are critical for the success of the study. The secondary delimitation for the study was to be as efficient as possible in my dealings with the different agencies and when conducting interviews to make the inquiry as painless as possible for those willing to participate.

Limitations

There were several different limitations for this inquiry into the current state of cybersecurity policy in Tennessee. While the Congressional Record has many different pieces of legislation and many Executive Orders are public knowledge, some aspects of cybersecurity policy are classified. The same may also be true for state and local governments, constraining this investigation to publicly available information. This left the inquiry open to incompleteness but does not obviate the potential benefits of the study. There were also time limitations for the inquiry, especially regarding the demands on the time of the individuals targeted for the study. Legislators, subject matter experts, and law enforcement professionals each have many daily demands on their time, requesting dedicated time beyond their scheduled duties added to that workload.

Alongside the time constraints, gaining access to each of the individuals targeted was also a potential limiting factor. Along with the concerns about time available of each of those targeted, there were also concerns about the line of questioning or how responses would be communicated. Politics, fear of reprisal, concern about the responses provided, unwillingness to admit limited knowledge, or lack of control all tempered the willingness for individuals, agencies, or groups to participate. Each of those concerns was addressed to ensure maximum participation and adequate coverage of all viewpoints.

The final limitation also tied into the access question and dealt with the possibility of identifying weaknesses or openings in the current cybersecurity framework. This limitation was potentially the most significant issue to be addressed when dealing with the legislators and field agencies targeted. The purpose of this study was not to delve into specifics or operational concerns but focus on the policies and procedures that allow field agencies to conduct cybersecurity operations. Providing advance information on the type of responses requested and explaining how that information would be packaged and utilized assisted in setting parameters for interviews.

Significance

The results of this study are important as they can help define the existing cybersecurity environment in Tennessee from multiple perspectives. By examining the current framework from different points of view, a better snapshot could be taken of opportunities for improvement and areas of strength. Currently, only minimal research exists on how states are reacting to the threat of cyberterrorism and other cyberattacks, leaving a gap in understanding of how the different sides view the whole. It was anticipated this inquiry would suggest additional research areas to better define the current cybersecurity environment and available options. It was also hoped this inquiry would help to open dialogue on both sides, legislative and operational, particularly in areas of disagreement. Identifying such areas of opportunity may also help push conversations on other topics, such as adding a cybersecurity post to the Tennessee Cabinet, creating additional opportunities or programs for cybersecurity education and training, or establishing best practices for vendor selection and security considerations.

With differences in perspectives shared between legislators and field offices, it may be possible for the subject matter experts to better fill in the gaps. Those individuals in the Strategic Technology, Tennessee Bureau of Investigation, Tennessee Department of Homeland Security, and others remain best positioned to react to changes in the cybersecurity landscape and keep both legislators and other field agencies apprised of emerging trends. Law enforcement professionals and legislators alike are not always educated and equipped to follow technical trends and may not be able to work proactively with regard to cybersecurity. This research could help to inform those involved in the policy development process of the challenges and impacts faced by the cybersecurity field as a result of the current environment. While making this information available may not change the way policies are created or developed, it can be utilized to start the conversation or push for additional updates.

Social Change Implications

The primary benefit of this inquiry from a social change standpoint is the improved safety and security for both the state and the individual. By collecting data from the legislative and operational sides of the cybersecurity environment gaps and potential weaknesses could be more readily identified and solutions prepared before they become significant issues. Addressing these issues from the state level could also help inform discussion at both the federal and local levels, further enhancing security and counterterrorism initiatives.

Another social change benefit is the potential for the protection of civil liberties. As proactive measures are put into place to correct weaknesses and identified gaps in the cybersecurity framework less drastic measures will likely be needed in the event of a shift in threat or severe cyber-attack. One legacy from the 9/11 attacks was the discussion on whether the regulations put into place in the immediate aftermath of the attacks went too far in their authorizations for surveillance and other activities. By establishing a more dynamic system such transformative events may be prevented or the impact or reality of them better understood.

Summary

The complex and diverse nature of the cybersecurity threat in the current global environment is difficult to overstate. Reports on new threats, attacks, or tools used by nation-states, terrorists, or hackers appear daily in news reports around the world. With much of the focus going towards national security and developing cross-border standards to combat this threat, it is critical to improve our understanding of the effectiveness of the current cybersecurity environment at the state and local levels. This chapter outlined the issue and discussed the advocacy coalition framework, which can impact the direction and effectiveness of policy decision-making.

Chapter 2 provides an in-depth overview of cybersecurity, highlight critical legislation over the years, and conduct and intensive review of cybersecurity policy from five years ago through current day. The next chapter provides insight into the origins and usage of the advocacy coalition framework in qualitative research and the existing policy development and operation framework in Tennessee. Chapter 3 describes the research methodology, the instruments that will be utilized for both the interview and survey portions of the inquiry, and the utility of the measuring instruments. Chapter 4 will present the results of the study, and Chapter 5 will summarize the findings of the study, and offer possible recommendations for social change, potential changes in the cybersecurity framework, and future avenues of research.

Chapter 2: Literature Review

Introduction

Protecting the United States against cyber threats is a complex undertaking with no single solution or path to prevention. The very underpinnings of cybersecurity strategy vary depending on the source of the strategy and the focus of the agency involved. The individual citizen has a very different set of risks and behaviors than a local bank, and each of these differ from government entities and industries at the national and international level. Much of the current literature focuses on cybersecurity at the larger scale, along with how to protect interests through national and international action (see CITE). To address this gap in the literature, I examined the role played by state and local legislators and agencies, as the federal government lists these as the first line of defense and investigation in cybercrimes (see CITE). Specifically, I examined the current state of cybersecurity legislation and policy from both elected official and emergency management perspectives.

This chapter includes an overview of the literature search strategy and theoretical foundation of the study, along with a detailed review of the scholarly literature on cybersecurity. The literature review includes sources from the past 5 years. I consider the history of and ongoing issues in cybersecurity, as well as review material related to the development and deployment of cybersecurity strategies in the United States and Tennessee. The discussion also includes the rationale for the emphasis on cybersecurity at the state and local levels. A brief history of cybersecurity from the 1970s onward is also included to provide a frame of reference for the current discussion and policy environment. The chapter begins with an overview of my literature search strategy. In the section on the theoretical foundation for the study that follows, I will provide background information on and explain the choice of the ACF for this study.

Literature Search Strategy

The literature review for this study includes several different sources. For the initial search I used the White House Archives and Congressional Records at the federal level and the Tennessee Congressional and Gubernatorial Legislature Records for the state level. The searches of the records included key words such as *telecommunications, computer security*, *critical infrastructure*, *cyber*, *cybersecurity*, and *state/local governments*. Congress did not have a single definition or usage for cyber issues prior to the Clinton Administration, which was the first presidential administration with widespread access to computers and e-mail (Warner, 2012). Throughout the government an evolution of descriptors can be seen, from *telecommunications*, *critical infrastructure, computer security*, and various uses of *cyber*, in tracing the legislative and executive records from the earliest decisions to the current results. My search of the Congressional Record, including all legislative formats, and using the specified key words, yielded several thousand results going back to 1850. These results included bills, amendments, and resolutions of various types proposed by Congress, the majority of which are only remotely related to the matter at hand, if at all. The earliest results concern installing communications wires in Florida while the latest provided specific details on cybersecurity operations and issues in today’s digital environment. While most of the information does not apply, or need consideration in this study, these proposals are instructive, if only to gain additional insight into the policy development process for telecommunications networks over time. The search of the National Archive's Presidential Libraries similarly returned a range of results on similar topics over time. The decision directives and executive orders over the past 40 years, however, provided an overview of the federal government's priorities for communications security and structure of oversight (National Archives, 2016). The search of the Tennessee Gubernatorial and Congressional Archives yielded many fewer proposals or directives.

I performed secondary searches using the Homeland Security Digital Library, Walden University' online library, and Google Scholar. These sites provided academic sources and articles on the history, scope, and nature of current cybersecurity policy and the different theoretical frameworks currently utilized in policy development. The Homeland Security Digital Library yielded a number of sources and articles from individuals working in the cybersecurity and homeland security fields. Use of this database also helped me to frame the standard problems cybersecurity researchers, scholars, and operators identify in the course of their work, along with proposed solutions and counters. Demographic material and information on the different departments and agencies in the area came from the Tennessee government websites in the respective state, county, and local jurisdictions.

I conducted a number of separate searches using Walden University Library resources. A search for *cybersecurity* on the Thoreau multidatabase engine for peer-reviewed articles returned 20,298 results. A time-limited search between 2012-2017 with the same database and search term returned 9,500 results. A search in SAGE Premier journals (2001-2017) within the Public Administration and Politics and International Relations databases yielded 302 results. A search for *cybersecurity* in the ACM Digital Library (2002-2017) returned 294 results. The same key word search on Political Science Complete (1988-2017) returned 426 results, including 301 peer-reviewed articles in the full time period and 167 from 2012-2017. A key word search of Science Direct yielded 2,296 results from 1998-2017 and 1,763 from 2012-2017. Various key word searches were also conducted using a combination of terms (*computer security*, *information security*, *cyberattacks,* and *cyberwarfare*) across several other electronic databases, returning several hundred results. I conducted these searches until July of 2017, at which point I closed my literature review and competed the research proposal section of the research.

Theoretical Foundation

Cybersecurity is an inherently complex subject with different levels of oversight, engagement, and investment throughout the various layers of government. When beginning the conversation about cybersecurity policy, it is important to realize it is not a recent issue. One of the first works concerning information security was a paper by Thomas Rona, a scientist for Boeing, in 1976 (Berkowitz & Hahn, 2003). Over the next four decades, cybersecurity gradually became known and generally accepted as an issue in public discourse (see Warner, 2012). The public demand for additional protections was limited over the next several decades. That attitude has changed significantly in the last few years, as identity theft, ransomware, and other malicious attacks have risen dramatically (Warner, 2012).

Within the context of this increasing demand by the public, officials at all levels of government in the United States have and continue to develop policies and procedures to secure cyberspace. While much of this activity occurs at the federal level, state and local officials also have a role to play, along with law enforcement and emergency directors. Federal cybersecurity policy establishes that federal agencies will assume primacy in most cyber cases, which is consistent with the international or interstate nature of many computer crimes (National Cyber Strategy, 2018). The same policies, however, note that state, local, and tribal law enforcement will remain as the first line of defense and investigation for cybercrimes at these levels (Department of Homeland Security, 2018 (2)). Each of these policy actors brings their own views, responsibilities, experiences, and perspectives on which policies to give priority or include in disaster recovery plans. In addition, a range of data streams, discussions, and coalitions on either side of the debate influence policy decisions (see Department of Homeland Security, 2018 (2)). The numerous actors, interest groups, and evolving information on cybersecurity threats, detection, and defense call for a framework that will address each in detail.

Origin of the Advocacy Coalition Framework

The development of the ACF followed the publication of a number of studies and theories, with precursor theories in the 1960s, 1970s, and 1980s by different authors. Sabatier developed this framework and published it in 1988 in *Policy Sciences*. "An Advocacy Coalition Framework of Policy Change and the Role of Policy-Oriented Learning" therein contained a detailed review of previous work by Heclo, Weiss, Mazmanian, and Ostrom, among others, and outlined the framework Sabatier asserted would build on and close gaps in earlier work. The article dealt with environmental policy in general, and air pollution policy development from the 1950s-1970s, specifically. Sabatier focused his efforts on evolutionary learning, belief systems, and advocacy subsystems in the policy development process (Sabatier, 1988, p. 129).

Sabatier leaned heavily on Heclo's work in developing the ACF, which he considered a practical application built upon Heclo's theories. Heclo (1974) stated that the previously considered general or macro-level influences could only account for a certain portion of a given policy change or evolution. To close the gaps, he believed it was necessary to incorporate individuals and groups working in the specialized field (Heclo, 1974). Sabatier carried this line of thought throughout the advocacy coalition framework, broadening the scope of the idea of the lobbyist and policy actor.

Overview of the Advocacy Coalition Framework

In the development of the ACF, Sabatier established three main pillars or premises. The first premise, and one that underpins the rest of the discussion, is the requirement to evaluate policy development and evolution over a period of at least a decade. As he read previous works and developed the ACF for application in policy, Sabatier focused on the so called 'enlightenment function' of research. Under this line of reasoning, the development of additional knowledge by scholars, advocates, or other stakeholders in the policy process is a critical portion or the policy process. There is a built-in delay in the time it takes from the identification of a particular problem to a more thorough understanding of the details and consequences, both intended and unintended, of a policy decision. As stakeholders, scholars, and advocates gather data and work to apply it towards the policy process, the feedback loops can become more complex and time-consuming (Sabatier, 1988, p. 131-133). The figure shown in Appendix A outlines the ACF and demonstrates the feedback loops within the system, as well as how multiple variable types are incorporated into the framework.

The second pillar of the framework is to utilize the entire subsystem associated with a given policy as the unit of inquiry. In reviewing previous research, Sabatier found earlier studies considered the agency or organization developing a policy, then examined the inputs and influences to ascertain what led to its implementation or evolution. Sabatier felt the lobbyists, interest groups, and other stakeholders provided significant input and influence into the process, along with scholars, journalists, and other analysts. Building off the first premise, these stakeholders and advocates provided the bulk of the information influencing public and institutional opinions on a given subject. Neglecting to consider the impact these stakeholders have in the process left policy development with too many unknowns or unaccounted for variables (Sabatier, 1988, p. 131).

The final pillar of the ACF is to view the behaviors and policies of stakeholder organizations like the belief system of an individual. Sabatier argued that the behaviors of the groups in a particular policy subsystem reflect its preferred path and priorities, just as the individual’s beliefs translate into their politics (Sabatier, 1988, p. 132). While an organization may demonstrate its core values or institutional vision, it is also possible for their actions to misrepresent them, as well. These discordant actions might be the result of environmental factors, behavioral limitations, or economic priorities, and may or may not be purposefully misleading. One recent example of such behavior was the revelations regarding Volkswagen and their emissions control systems. That company pled guilty to purposely misleading its consumers about the efficiency and environmental impact of its diesel vehicles. Engineers for the company developed software designed to activate emission controls when the vehicle was tested, but remain off under normal operation. This was not an isolated incident, as a grand jury also indicted six senior executives at the company for their role and knowledge of this scheme, which lasted for a decade or more. In the public eye, Volkswagen was a leader in environmental protection within the auto industry, claiming its 'green diesel' engines surpassed regulatory requirements (Kennedy, 2017). In reality, the company suffered a significant reputation and business impact while attempting to chase larger profits.

The figure Sabatier provided for the ACF contained principal areas of constraint or input into the policy process. These are relatively stable parameters, external events, constraints and resources of subsystem actors, and the policy subsystem itself. The stable parameters are those core principles that evolve very slowly and are most unlikely to change. These parameters frame the larger policy environment the rest of the changes and actions operate within. Changes in these parameters may significantly alter the policy environment and cause major shifts to adjust. The external events are those driven by changes in the subsystem within the larger framework. As constraints are added and the environment takes shape, the events and parameters filter through the constraints and resources of the subsystem actors. The policy subsystem is where the majority of the changes happen within the advocacy coalition environment. In this area, the separate coalitions create strategies and policies based on their beliefs and available resources. The coalitions address the policy authorities and influence the decisions regarding governmental policies and procedures. The outputs and impacts of the policy decision in turn feed back into the beliefs of the coalitions, further shaping the discussion and debate (Sabatier, 1988, pp. 132-138)

Application of the Advocacy Coalition Framework

In order to demonstrate the ACF in more detail, Sabatier examined police brutality and accountability from 1991 forward. On March 3, 1991, police in Los Angeles, California pulled Rodney King over after a pursuit through the city. A nearby witness caught the traffic stop and the subsequent assault on a video camera. Four officers tazed, kicked, and struck Mr. King with batons over 50 times during the stop despite his protestations he did not resist arrest. The major public reaction to events occurred in April of 1992 when the jury acquitted the police officers at trial. The resulting riots left 55 dead and thousands injured, with millions of dollars in damages from the looting. One can then fast forward to the period of 2014-2016 and review the coverage of police-involved shootings and violence. Incidents in Ferguson, New York, Baltimore, Charlotte, and elsewhere led to protests, riots, and continued violence in the streets (Adams, 2016).

Using the pillars described by Sabatier, the first requirement is at least a decade to review policy evolution and development. The 26-year span from the Rodney King assault to the present covered that requirement and allowed for multiple or overlapping feedback loops regarding police violence and community relations. Sabatier stated the accumulation of knowledge has the largest influence on the direction of policy, so ensuring enough time to evaluate this accretion is essential. For this subject, the policy subsystem is very robust and complex, including stakeholders in both the public and private sectors. Law enforcement organizations at the state, local, tribal, and federal levels represent a significant portion of the subsystem. Other public servants, including elected and appointed officials, policy analysts, and others, also occupy the subsystem. Alongside that sector, there are a myriad of organizations working exclusively or occasionally on improving police-community relations, securing civil rights, and reducing racial tensions. Each of these sectors of the subsystem contain a wide range of actors and opinions, with different actors grouped into coalitions based on their actions and behaviors on different sides of the debate. This subsystem follows Sabatier's description of the broader definition, not restricted to the "'iron triangle' – administrative agencies, legislative committees, and interest groups at a single level of government" (Sabatier, 1988, p. 131).

Application of the third premise of the ACF is labor-intensive, especially for such a complex subsystem. The last section provided a description of the separation and classification of the actors and coalitions. The last portion involved identifying each of the belief systems, perceptions, relationships, and priorities of the different coalitions. These aspects are subsequently used to evaluate policy changes throughout the period in question and evaluate causal relationships and their effectiveness (Sabatier, 1988, pp. 132-133). For the police-community discussion, this portion of the framework would require a review of policies and procedures from the federal down to the state and local levels and include violence and rights issues across the country. Further review requires investigation of the different dynamics at the separate levels, making an overall project on this topic cumbersome and laborious, at best. Most policy actors specialize in a smaller area, whether is it restricted to a geographic region, type of incident, or a subsection of the larger criminal justice debate. The advocacy coalition framework provides a blueprint for the evaluation, but it is incumbent on the researcher to frame the investigation in the most effective method.

Evolution of the Advocacy Coalition Framework

Rising from its inception in 1988, with additional refinement in 1993 by Sabatier and Jenkins-Smith, advocacy coalition continues as a popular framework for policy development and analysis (Weible, et al, 2011). Over the last decade, Sabatier and Weible contributed to multiple studies examining the advocacy coalition framework, its uses, and potential future courses of investigation. In one of these, *Themes and Variations: Taking Stock of the Advocacy Framework,* Weible, Sabatier, and McQueen 2009 discussed 80 separate studies that utilized the framework starting at inception and continuing for twenty years. This work included the 2007 revision of the framework outline discussed in the previous section. The updated outline is shown in Appendix B. The key changes in the update are the separation of the constraints and resources in the first draft into short- and long-range categories and removing single path decision-making (Weible, Sabatier, & McQueen, 2009).

In the earlier versions, constraints and resources were a single category, with the decision process moving from stable parameters through system events and constraints and into the policy subsystem. That subsystem has internal feedback loops and fed into the system events. In the updated version of the outline, the authors acknowledged a more complex and simultaneous policy development process. The outline of the system in the newer version retained the relatively stable, system events, and policy subsystem sectors, and the short-term constraints remain a filter from the system events to the policy subsystem. The addition of the long-term coalition opportunity structures (overlapping societal cleavages and degree of consensus needed for major policy change) were coupled with that sector, adding input into system events and short-term constraints, along with acting as a filter for the stable parameters to flow into the policy subsystem (Weible, Sabatier, & McQueen, p. 122-123).

The Advocacy Coalition Framework and Cybersecurity

For the purposes of this study, the 2007 ACF outline was utilized to examine cybersecurity policy in depth. Policy at the federal level was addressed in a more general sense, with policy development at the state and local level receiving a more thorough examination. The ACF was selected as the lens for this study due to its applicability across wide policy frameworks, its utility in complex areas such as environmental policy, and the incorporation of the various constraints and pressures on the policy process. As will be addressed in the subsequent sections, cybersecurity is far from a new phenomenon, despite the recent increase in news coverage and discussion. The origins of cybersecurity date back over one hundred and fifty years to the first telecommunications systems. While the U.S. originally declined to take part in international treaties on the subject, several incidents and issues led to the signing of the 1850 Dresden Treaty, the first the U.S. affirmed in the cybersecurity realm (Rutkowski, 2011).

Review of Literature Related to Key Variables and/or Concepts

The literature review encompasses several different aspects. First, this study examined the origins of cybersecurity policy and trace its evolution to the current day. This research began with the origins of the computing program in the United States and discuss national policies created to erect security policies in the earlier environment. It then follows the evolution of computing to the present day, followed by an in-depth examination of the organizations responsible for different aspects of cybersecurity at federal level. The current national cybersecurity policies and procedures for the civilian sector will then be discussed. The military cybersecurity framework will also be discussed, but specifics about defense cyberwar and technology are beyond the scope of this inquiry.

History of Computing and Security from ARPANET to the Patriot Act

While cybersecurity is an emerging topic of discussion in the news today, it is far from a new area of concern for those in the field. The idea of computer security can be traced alongside the development of the computer. One of the first computers unveiled to the public was the Electronic Numerical Integrator and Computer (ENIAC) at the University of Pennsylvania in 1945 (da Cruz, 2013). This system was exceedingly large and functioned as an automated tabulation machine. While an impressive demonstration of technological advancement and innovation, ENIAC and its immediate followers lacked the ability to execute a stored or embedded program. The Electronic Discrete

Variable Automatic Computer (EDVAC), was developed to resolve the lack of a stored-program capability and completed in 1951. This was the first true electronic computer and paved the way for future development and the computing industry (Pugh & Aspray, 1996). With these large, cumbersome computers, initial concerns for security centered on physical security. The computers could only run one operation at a time, with the results returned to the researcher who designed the operation. With no connectivity, computer security could be limited to the specific area and designated time periods (Warner, 2012).

With the stored-program capability, computers then benefitted from engineering of smaller and more capable processors. The development of the microprocessor in the 1960s and 1970s evolved computers from the behemoths requiring massive space to the smaller desktop models (Abbate, 1999). Alongside these developments, researchers at the Advanced Research Projects Agency (now referred to as DARPA, or the Defense Advanced Research Projects Agency) sought to find a way to connect computers remotely. The development of packet switching theory and connective technology allowed them to establish the beginnings of the modern Internet. The system began with individual computers connected as nodes in a limited network, slowly adding additional machines and locations as technology allowed. This network debuted in October of 1972 at the International Computer Communication Conference (ICCC) (Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts, & Wolff, 2009). Also, during this time, the U.S. government presented legislation to separate how networks would be classified. The Brooks Act, passed in 1965, gave the National Bureau of Standards (NBS) oversight over government networks and required government entities to purchase their computing equipment from the General Services Administration (GSA) (Garland, 2015). There were, however, some provisions built into this legislation. First, the Central Intelligence Agency and those elements of the Department of Defense handling classified data were exempt. The Brooks Act classified these networks as 'operational' in nature and separated them from the general and administrative networks that handle most government traffic (Warner, 2015).

As the networks expanded in the 1960s and 1970s, the U.S. government in general, and the National Security Agency (NSA) specifically, identified the risks associated with remote access and the need for limits on access. The government, federal agencies, and researchers all sought to develop methodology for securing the networks, but ultimately concluded it was not feasible to close all of the gaps in an integrated secure/nonsecure system. Furthermore, even inside a theoretically closed, secure system there was still the concern for human failure or action to compromise established measures. Whether the human error resulted from negligence, unknown system openings, or deliberate act to compromise security, the most effective actions were to develop measures to limit mistakes and seek to protect data where possible. In response, engineers developed and incorporated file security and protections, administrative privileges, new password protocols, and digital encryption. The development of the Digital Encryption Standard (DES), derived from the algorithm used by IBM for its commercial customers, also marked one of the first instances of government agencies (the NSA in this instance) being accused of manipulating security measures to enhance its surveillance (Warner, 2012).

Several security violations occurred during this time that reinforced the findings of security weaknesses. The first federal prosecution of a computer crime occurred in 1967, “after a bank employee reprogrammed the bank’s computer to ignore his own overdrawn checking account” (Slayton, 2016). One of the first computer espionage cases publicly available occurred in 1968, when police in West Germany apprehended an East German spy in an IBM subsidiary. Building on the earlier theme of human error, in late 1979 a test scenario was loaded into the computers at the North American Air Defense Command (NORAD) that triggered alarms and sent false warnings throughout the national security system that the Soviets had launched over 2000 ballistic missiles (Warner, 2012). It is instructive to revisit these headlines and stories to frame the cybersecurity challenge over time. These are crimes and areas of concern from 50 years ago but are incidents that could easily appear in the news tomorrow. The first proposal for information and cyberwarfare came in 1976, composed by Thomas Rona, a staff scientist at Boeing (Berkowitz & Hahn, 2003).

As computer networks expanded in the 1980s and connected users and organizations the globe, the risks and threats of intrusion, theft, malicious programming, and espionage increased exponentially. This included domestic hackers seeking to find and exploit vulnerabilities in networks to gain access to systems and information. While not all these individuals were believed to be malicious in their desire to break into classified or proprietary systems, the fact that the vulnerabilities existed was problematic.

These actions, and increasing skepticism by defense agencies about their security, led to the issuance of the first major federal policy, National Security Decision Directive (NSDD)-145 on September 19, 1984. Under this guidance, the NSA assumed primacy for cybersecurity, an arrangement that lasted until 1987, with the passage of the Computer Security Act. This effectively split the oversight of cybersecurity between the NSA and the NBS, allowing the NBS to assist with federal networks not belonging to the Department of Defense (DoD). In 1990, the National Institute of Standards and Technology (NIST), the successor to NBS, was given the primary role of cybersecurity for all U.S. networks, ending the military and NSA's lead role. The NSA was authorized to continue to monitor government and military networks containing classified data, but oversight was not included (Warner, 2012).

With more and more connectivity in the early 1990s, security of the Internet was an increasing concern. At the outset of the decade, the United States engaged in Desert Storm, the first Gulf War. Because of the exceedingly rapid success of that effort and the activities employed by military assets, it was the initial information war, with enemy command and communications capabilities systemically attacked, limiting the effectiveness of organized resistance. The benefit of this was codified by the Chairman of the Joint Chiefs at the time, Colin Powell, in a policy memorandum in 1993 (Warner, 2012). As the military found new opportunities to utilize the Internet, a number of other actions shed light on weaknesses in the DoD's own networks and those across the United States. Several instances in the late 1980s and early 1990s. including the introduction of the Morris Worm and the Michelangelo Virus, garnered the public's attention with regard to computer security and potential vulnerabilities. Wargames and other training exercises conducted during this time found glaring inadequacies in connectivity between government agencies, coordination, and cybersecurity in general. The DoD experienced roughly 250,000 penetration attempts per day in 1996, putting increased pressure on the sector to not only harden their defenses, but to take active measures to close any loopholes identified and shore up security across a range of networks and locations (Warner, 2012).

In the middle of the 1990s, government researchers came up with a new idea, using the Internet to cause physical damage or service interruption remotely. This issue was particularly relevant to critical infrastructure across the country, an area ever more reliant on computers. The DoD in 1997 launched ELIGIBLE RECEIVER, an exercise designed to test the reaction and coordination of DoD agencies of a cyberattack on critical infrastructure. The DoD failed to protect the target and the results of this exercise showed how vulnerable critical infrastructure was and how much work needed to be done. This dovetailed with a Presidential commission that reported more or similar damage could be done with a computer as with a bomb in an attack on critical infrastructure. Two hacking attacks around this time, one via Chinese Telecom on California’s power grid in 2001, and a possible Russian operation against the DoD detected in 1998 both lent credence to the conclusions and recommendations provided by these panels (Warner, 2012).

A trio of legislative actions from 2000-2002 altered the cybersecurity framework and how U.S. agencies interacted with the surrounding world. The first, *Defending*

America's Cyberspace: National Plan for Information Systems Protection was published in January of 2000 by the Clinton administration. This was the first national strategy, and it divided cybersecurity between three different elements, the NSA, through the National Security Incident Response Center, the Joint Task Force-Computer Network Defense, and the Federal Intrusion Detection Network (FIDNet). This legislation also made the point that the government oversees government networks only, private sector networks were the domain of the companies that use them. The second was the USA Patriot Act, which provided sweeping powers and authorities to law enforcement in pursuit of terror organizations and to secure the homeland. The third was the creation and organization of the Department of Homeland Security (Warner 2015). These policies are discussed in more detail in the following section, and their impact on computing and security is addressed in the subsequent section that covers operations and incidents from the passage of the Patriot Act through 2016.

History of Cybersecurity Policy in the United States through 2000

The investigation of cybersecurity policy in this country is a cumbersome and exhaustive undertaking. There are a few reasons for the complexity: the evolution of definitions and descriptions of computers and related networks over time, competing interests of military and civilian oversight, national security versus privacy considerations, public and private networks and systems, and various limitations on the powers of the United States government. Each of these issues adds additional challenges in tracing policy, but one of the strongest continuing criticisms is a lack of a single, coordinated, comprehensive policy over all computer or cyber security (Trautman, 2015).

With such a wide-open policy environment, this study will provide as wide a viewpoint as possible on policy evolution while narrowing the focus to relevant legislation, with the greatest focus on the federal side on the executive branch memoranda and congressional actions over the last decade.

The United States and other countries around the world have long acknowledged the need for policies for communications networks. Some of the earliest date back to the 1850 Dresden Treaty, which sought to forge an agreement among member nations to assure the operation of the new electrical communication networks as previous agreements had for postal and other visual systems. Subsequent international treaties followed the evolution of electric communications, including the first international meeting regarding the Internet in Melbourne, Australia in 1988 (Rutkowski, 2011). In the United States, regulation and oversight of computer networks was first addressed by the Brooks Automatic Data Processing Act of 1965, more commonly known as the Brooks Act. This legislation consolidated procurement of automation data processing equipment under the General Services Administration and granted National Bureau of Standards authority to set policies and procedures for government networks. As noted in the previous section, there were built in exceptions for intelligence and military operations networks, which were designated as operational in nature and outside the GSA’s purview (Public Law 89-306, 1965).

The Brooks Act formed the core of computer security policy for a decade, when the Carter administration released Presidential Directive 24 (PD-24), *Telecommunications Protection Policy*, in 1977. In PD-24, the federal government established policy that limited classified data to secure networks, protections for networks transmitting useful but unclassified information, and standards for working with the private sector to secure nongovernmental networks containing useful but unclassified information. Further, this directive required department heads within the government to ensure appropriate security protocols were enacted for their networks, working under Executive Agents. This also assigned the Secretaries of Defense and Commerce as the agents for national security and administrative government networks, respectively (Presidential Directive 24, 1977). Presidential Directive 53, published in November 1979, continued the efforts from PD-24, but added language for the continuity of communications networks in the event of nuclear attack or other major event that might disrupt communications (Presidential Directive 53, 1979).

Executive Order 12333 put several policies in place regarding intelligence activities, including naming the Secretary of Defense as the Executive Agent for all military and classified intelligence networks. This policy further placed the National Security Agency (NSA) as the lead agency for the collection and running of all signals intelligence for the government, including procurement and protection of signals networks, research and development for signals security, and “executing the responsibilities of the Secretary of Defense as executive agent for the communication security of the United States Government” (Executive Order 12333, 1981). Two years later, NSDD-97/EO-12472 (National Security Decision Directive 97/Executive Order 12472) superseded PD-53 and established a new National Communications System. This order established a working group with responsibility for national security and emergency preparedness communications. This included creating standards, procedures, and expertise for the current and future operations and ensuring the networks were survivable in all contingencies and could be rapidly resurrected or covered, as needed. This legislation also required evaluation of new technologies and the creation of disaster training, among other contingencies (National Security Decision Directive 97, 1983). The continuing need for security of communications networks, especially mobile networks for senior U.S. leaders, was addressed in NSDD-113, issued in November 1983 by President Reagan (National Security Decision Directive-113, 1983).

While previous executive memoranda addressed telecommunications security, National Security Decision Directive 145, or NSDD-145, was the first to place exclusive emphasis on “microelectronics technology”. President Reagan published NSDD-145 in 1984 in response to several hacking and intrusion events in the early part of the decade. These included a widely publicized story in the New York Times about teenagers gaining access to unclassified defense networks, and the military losing faith in its security moving forward (Warner, 2012). This directive established three policies to support the government’s efforts to establish, maintain, and protect a continuing telecommunications network. First, classified systems were to be secured against accidental or intentional breach by whatever means necessary. Those systems with proprietary but less than classified information needed protection according to the level of threat they might experience to secure national security interests. Finally, government assets would provide recommendations and assistance to private sector actors or agencies that maintained networks with proprietary information. This policy also created a steering group, an executive committee and subcommittees to develop, implement, test, and provide continuing guidance for the effective security of telecommunications networks across the federal spectrum. This further granted the NSA sole authority of government networks (National Security Decision Directive 145, 1984).

The decision to place the NSA as the primary agency for federal networks across the board received an immediate and strong reaction from Congress. Leaders in both chambers, led by Representative Jack Brooks, the author of the original Brooks Act in 1965. After several hearings and deliberations, the Computer Security Act was passed in 1987. This legislation was considered an updated version of the original Brooks Act, as it transferred the NSA to its previous mission of overseeing the national security/classified military networks and restored the NBS over the unclassified systems. The Reagan administration was successful in changing the original dual definition of national security/unclassified systems to include a third type: confidential systems. The NSA and NBS were granted joint advisory roles over the third type of networks, fundamentally granting the administration its main objectives (Warner, 2015).

The NSDD-145 continued in its amended form until its recension in 1990 by National Security Directive (NSD)-42. This directive established the Policy Coordinating Committee (PCC) for National Security Telecommunications and designated the Secretary of Defense to chair it. It also provided for operations-level groups to ascertain the state of networks, the nature of current and future threats, and work to develop policies, standards, and protections against them. This again placed the Secretary of Defense as the Executive Agent for telecommunications networks and the

Director of the NSA as the National Manager in charge of system security and development, subject to approval of department heads (National Security Directive 42, 1990). The High-Performance Computing Act of 1991 created a program that involved a range of departments to improve coordination, oversight, software, technical support, education and security in federal computing systems. The main contribution to cybersecurity of this act was twofold: it increased the research and development of networking and security throughout governmental systems and tasked NIST with developing security measures, standards, and tests for the developing systems (Public Law 102-194, 1991). President Bush also created the National Industrial Security Program in 1993 under Executive Order 12829. The program director assumed control of the security and integrity of national security and classified information released to non-government organizations, including issuing policies and procedures and conducting site reviews to ensure compliance (Executive Order 12829, 1993).

The next step in presidential action was President Clinton's Presidential Decision Directive (PDD)-5, *Public Encryption Management*. This document identified the emergence of public encryption keys and their potential to impede law enforcement efforts. To counter this, PDD-5 tasked the Attorney General with coordinating with encryption manufacturers to place government-developed keys into their products. These would allow law enforcement, after appropriate judicial permission, to bypass encryption no matter the source. Coupled with this, it directed the Secretary of Commerce to create a process to procure and install the key-enabled devices into government systems (Presidential Decision Directive-5. 1993). The Clinton administration reinforced its desire for improved security with PDD-63 in 1998. This directive set a goal of 2000 for an initial capability and 2003 for federal agencies to be able to defend critical infrastructure against attack, including cyber systems. The intent was that the government would be able to provide a minimum level of service no matter how extensive the attack or threat to critical infrastructure. To achieve this, the directive planned to lean heavily upon the public-private partnerships and desired for market pressures to motivate cooperation, leaving additional regulations as a last resort. Each department was given six months to secure its systems and was required to appoint a Chief Information Assurance Officer (CIAO) to take the lead on system security (Presidential Decision Directive 63, 1998).

Public-private partnerships and the need for positive working relationships with non-governmental agencies is a continuing theme in both Congressional and Executive policies. The Brooks Act acknowledged the use of outside actors on government networks and the Computer Security Act recognized not all government operations remain solely within government-controlled systems. The addition of the CIAO in PDD-63 provided an assurance side to the installation of a Chief Information Officer (CIO) in major federal agencies by the Information Technology Management Reform Act (ITMRA) of 1996, otherwise known as the Clinger-Cohen Act. The Clinger-Cohen Act is an amalgamation of both the ITMRA and the Federal Acquisition Reform Act (FARA). This legislation ended the provisions of the Brooks Act, removing government procurement duties from the GSA and investing newly established CIOs with that mission. It also acknowledged the growing use of private networks and joint systems of government agencies, areas not secured by federal authorities. Within the next two years the Department of Defense would be tasked with eliminating redundancies between the different branches of service and agencies, as well as ensuring connections between secured and administrative networks (Warner, 2015).

Also, in 1996, President Clinton published Executive Order 13010, *Critical Infrastructure Protection*. This memorandum split threats to infrastructure into two sides, physical threats and cyber threats, established the President's Commission on Critical Infrastructure Protection, and established an Infrastructure Protection Task Force (IPTF). The President's Commission was tasked with analyzing the critical infrastructure network, determining the major players in the public and private sectors, and coordinating with Congressional leaders and other stakeholders to develop a new CIP program. This directive tasked this committee to incorporate legal and policy issues and recommend policy and regulatory changes to counter both physical and cyber vulnerabilities (Executive Order 13010, 1996). This order tied into the Clinger-Cohen Act to improve public-private partnerships in cybersecurity and contributed to Executive Order 13011. This legislation established the CIO position in all federal agencies and set forth their duties and responsibilities, with a significant emphasis on security of the national security systems (Executive Order 13011, 1996).

Around this time, the federal government established security rules and standards for industries in the private sector. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established a five separate rules for the health insurance sector, including the Privacy Rule, Transactions and Code Sets Rule, Security Rule, Unique

Identifiers Rule, and the Enforcement Rule. Each of these had its own impacts, but the Security rule had direct effects on cybersecurity, including administrative, physical, and technical safeguards. The administrative included how companies would comply with the regulations, including written rules and regulations, restrictions on which employees had access to data, training, and contingency standards for emergent issues. The physical guidelines outlined preventing unauthorized access to hard copy files and information. The technical safeguards outlined required and recommended security protocols for health information, networks, and computer systems utilized by companies in this sector (Public Law 104-191, 1996).

In 1999, Congress also established new standards for the financial sector. The Gramm-Leach-Blilley (GLB) Act, also known as the Federal Home Loan Bank System Modernization Act of 1999, repealed the 1933 Glass-Steagall Act, removing barriers to mergers between banking, securities, and insurance companies. Under Glass-Steagall, no company could serve as a combination of investment, commercial, and insurance agency nor could officers at those institutions work in simultaneous position with multiple types of companies. Along with modifying restrictions for mergers and the types of business financial institutions could conduct, the GLB Act also put security requirements into place in this sector the way HIPAA did for the healthcare industry. These requirements included risk analysis, program development, written policies and plans (Public Law 106-102, 1999).

Cybersecurity from 2000 to 2003/Post 9/11 Actions

The Bush Administration published the first of a series of executive orders in October of 2001 concerning cybersecurity. The first, *Critical Infrastructure Protection in the Digital Age*, set standards and policies for securing CIP in the interconnected information age in which we now live. This order built off the previous policies established by President Clinton and set the stage for legislation coming later in the year. Assignments were given to the OMB and DCI for the oversight of policy creation and security of federal networks. A Critical Infrastructure Protection Board was also named, with the Chair also tasked to serve as the President's senior cybersecurity advisor (Executive Order 13231, 2001). One of the most important and far-reaching policy initiatives in the United States was Public Law 107-56, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*, also known as the USA Patriot Act. This act was a direct response to the September 11, 2001 terror attacks and included a wide range of actions dealing with counterterrorism, enhanced surveillance for law enforcement agencies, money laundering, border protection, communications between agencies, improving intelligence, and others. The Patriot Act contained several different aspects relating to cyber and computer security. This included an increased budget for the Federal Bureau of Investigation's (FBI's) technical division, expansion of the National Electronic Crime Task Force Initiative, a significant expansion of electronic surveillance and authorities for law enforcement agencies, and the creation of additional cybersecurity capabilities, among others (Public Law 107-56, 2001). This legislation had an enormous impact on agencies and security considerations at many levels and served as a precursor to the first official Homeland Security policy and the Homeland Security Act, both published in 2002.

The first of these published policies was the *National Strategy of Homeland Security* in July of 2002. This document, from the Office of Homeland Security, laid out three strategic objectives: "prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, [and] minimize the damage and recover from attacks that do occur (Office of Homeland Security, 2002). In addition, it identified six critical mission areas: intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response" (Office of Homeland Security, 2002). For each of these six areas, the policy provides major initiatives to guide planning and preparation. The final section of the strategy document outline four major foundations and outlines both federal- and state-level initiatives to support those areas. This initial document lays out a multi-tiered and complex policy environment encompassing a wide range of topics and agency responsibilities (Office of Homeland Security, 2002). The national strategy document provided the foundation and guidance codified in the Homeland Security Act which was enacted later that year.

Public Law 107-296, also known as the *Homeland Security Act of 2002* sought to close some of the gaps in the operational and oversight in these areas by creating the Department of Homeland Security (DHS). This department was given the primary role of preventing terrorism across the United States, with multiple roles and points of emphasis (Public Law 107-296, 2002). This reorganization encompassed 22 federal agencies and over 170,000 employees. One of the main purposes of this was to consolidate intelligence operations and provide central guidance and direction for counterterror and security operations. Among these were communications security and interaction and coordination with non-federal entities, including state and local agencies (Clarke, 2004).

Of the departments within the DHS, the most pertinent to this study is the Directorate for Information Analysis and Infrastructure Protection (IAIP). Requirements for the directorate include collecting information from federal, state, local, and private agencies and organizations to identify, detect, understand, and communicate emergent threats and vulnerabilities to the appropriate departments. To accomplish this, tasks include conducting assessments of potential vulnerabilities, identifying risks and potential mitigation factors, make recommendations to outside departments on vulnerabilities and collection priorities, liaise with state and local governments for needed information, and to ensure a secure telecommunications and information system, among others. Under the new law, responsibilities for the department included all critical infrastructure, including all physical and computer-based telecommunications, information systems, storage, or processing elements, and all of the peripheral equipment required for transmission. The new reporting structure also transferred reporting requirements for elements of the FBI, DoD, Department of Commerce (DoC), Department of Energy (DoE), and the GSA to the Under Secretary for IAIP. The Homeland Security Act of 2002 also included additional provisions for cybersecurity. The IAIP was granted authority to supply state and local authorities, along with those private agencies that own or operate critical infrastructure, with information on threats and vulnerabilities to CIP and support in response to a threat or an attack on those systems. The *Cyber Security Enhancement Act of 2002* is also included within this Act, addressing sentencing, disclosures, and amending U.S. codes regarding computer crimes (Public Law 107-296, 2002).

The Homeland Security Act also established the Office of Science and Technology (OST) with the oversight of the development and deployment of different technologies across the federal, state, and local levels. Assigned duties included creation and maintenance of performance standards, certification of technology used at the federal, state, and local levels, ensuring interoperability of telecommunications, and overseeing programs to develop and distribute tools to counter cybercrime, among others. Included with discussions on telecommunications technologies was the need to share information with agencies at all levels and the reliance of the federal government on State and local law enforcement to serve as the first line of defense against terrorism and other attacks. Decisions on the sharing of information require a balance between the need for information in the field and restricting access for national security purposes. (Public Law 107-296, 2002). Coupled with the Patriot Act, the Homeland Security Act represented a paradigm shift in security in the United States.

Where the Patriot Act and Homeland Security Act focused on terrorism and homeland security, the *Cyber Security Research and Development Act*, enacted in November 2002, set out a plan to close both knowledge and technical gaps in the national computer security framework. This legislation laid out several the findings originally published after the 1997 “Eligible Receiver” exercise previously discussed while also acknowledging the increasing pace of interconnectivity and the lack of adequate planning and support for these within the government. This legislation established programs within the National Science Foundation (NSF) and National Institute of Science and Technology (NIST) to expand cybersecurity programs throughout academia, including grants for research, undergrad, and graduate programs. The Director of NIST also gained responsibility for coordination with the National Academy of Sciences to conduct research on network and computer security across the critical infrastructure system in the United States (Public Law 107-305, 2002). Public Law 107-347, the *E-Government Act of 2002*, contained one final publication for 2002, the *Federal Information Security Management Act of 2002*. This act placed the Director of the Office of Management and Budget (OMB) as the overseer for information security across the federal system and required all agencies to care for their own information security. This security included not only network security, but that of information and supporting infrastructure, along with threat prevention and mitigation. The Director of NIST became responsible for the creation and distribution of standard information protocols and providing security (Public Law 107-347, 2002).

In addition to these policies, there a number of Executive Orders published between 2001 and 2004 that modified different aspects of cybersecurity oversight and management, with the next major change occurring in 2004 with the creation of the National Counterterrorism Center (NCTC). This organization was given primary oversight of all intelligence relating to terrorism, apart from purely domestic issues, which remained the purview of the FBI. This included service as the primary clearinghouse for intelligence and liaising with and assigning operational tasks to federal, state, local, and tribal organizations and law enforcement for issues related to their jurisdictions. The NCTC took over intelligence responsibilities previously handled by the Terrorist Threat Integration Center and received information from intelligence agencies under authority of the DCI (Executive Order 12333, 2004). Changes to Executive Order 12333 were incorporated in Executive Order 13355, *Strengthened Management of the Intelligence Community* (Executive Order 13555, 2004). Executive Order 13470, *Further Amendments to Executive Order 12333,* further refined these orders and noted the need to account for state, local, and tribal government agencies in the collection and distribution of intelligence, along with applicable. This order also designated functional managers for different types of intelligence, including the Director of the NSA as the manager for signals intelligence, including aspects included in cybersecurity, the NSA as the head of signals intelligence operations, and the DIA as primary overseer of defense operations and excepted from the oversight of the NSA for DoD operations, as well as the intelligence assets of the armed forces. The intelligence agencies in other federal departments were also tasked with supplying supporting intelligence to support designated needs (Executive Order 13470, 2008).

Presidential Actions on Cybersecurity Post 9/11-2014

In 2007, the Homeland Security Council published an updated policy directive, the *National Strategy for Homeland Security*. This was an update of the original policy published in 2002 in the aftermath of the 9/11 terror attacks. This strategy document provided an overview of the new security environment, outlined a strategy and vision for the future, and addressed methods to protect against threats, recover from potential attacks, and proposals to ensure success moving forward. One area of emphasis in this strategy was to reiterate the prominent role State, local, tribal, and territorial (SLTT) governments and agencies maintain in serving as first responders and subject matter experts on how to protect their citizens. Also incorporated was the private sector, especially those organizations owning or operating critical infrastructure. While the federal government and its agencies maintain primary responsibility and authority for prevention of attacks on the homeland and their investigation, localized attacks and events place burdens on lower levels of government in the immediate results, impacts on citizens, and response. The strategy noted the increased coordination and increased level of grant issuance to lower governments to bring them up to speed and address identified vulnerabilities (Homeland Security Council, 2007).

In addressing current and future threats, the 2007 strategy drew on the ongoing threat of terrorism, natural disasters (especially the lessons of Hurricane Katrina), and other accidents and hazards. This strategy outlined a few different techniques to protect against terrorism, including intelligence-led policing in the U.S. and increased border security and screening to prevent terrorists from entering. For a cybersecurity standpoint, the strategy centered on countering extremism and radicalization online, securing cyberspace, and updating the Foreign Intelligence Surveillance Act (FISA). Cybersecurity was noted as an especial in the strategy, with previous directives and policies referenced as guiding principles for the ongoing battle to harden the networks, reduce vulnerabilities, and improve recovery operations. This strategy covered a range of policies and procedures but maintained focus upon the primacy of the federal effort to protect the nation and on the importance of the SLTT governments and private sector organizations to support that effort. Another major theme of this strategy was the inclusion of risk-based management and incorporating lessons learned to improve operations and plans on a continual basis (Homeland Security Council, 2007).

Also, in 2007, Congress, acting on recommendations of the 9/11 Commission's report, created the Office for State and Local Law Enforcement (OSLLE) within the Office of Policy within the DHS. This department received primacy as the lead agency for coordination and communication of standards and policies with the SLTT agencies in areas including disaster management, terrorism, or other incidents. As the lead liaison for SLTT agencies, the OSLLE did not gain authority for operational control or jurisdictional powers within the separate states. The intent for this organization was and is to serve as a single point of contact for the various agencies around the country with the federal government and push best practices and DHS standards out to the field (Department of Homeland Security, 2009).

In Executive Order 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities,* President Obama expanded upon previous orders and consolidated others regarding the access to classified information by State, Local, Tribal, and Private Sector Actors. With the ever-increasing interconnected nature of different levels of government, the oversight of CIP across multiple levels, and the complexities of cyber resources, previous legislation left potential gaps related to this type of information. This program provided for the accreditation of different agencies to receive and store classified data, but also provided for oversight and monitoring of facilities, whether in or outside of the federal government. The Secretary of Defense received oversight of this program, with the DNI also receiving authority over intelligence affairs (Executive Order 13549, 2010). Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,* enacted various reforms to improve the security of classified information around the world while maintaining appropriate protections for civil liberties. To accomplish these goals, the order established the Classified Information Sharing and Safeguarding Office (CISSO) to support, advise, and consult various federal agencies on the security of classified networks. It also created an Insider Threat Task Force to create and administer programs to counter potential threats across federal networks (Executive Order 13587, 2011).

In 2013, the Obama Administration published two separate policies regarding CIP and cybersecurity. The first was Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*. This order reiterated the increasing reliance on the cyber environment in both the public and private sectors. To counter increasing threats against the cyber domain, this order directed significant increases in communications with private sector partners and expediting granting of clearances to those agencies and entities needing access to classified information under EO 13549. A framework to identify and mitigate cyber threats against the CIP resulted from this legislation. The primary framework fell under the purview of NIST as a required, risk-based tool to assist federal agencies in the risk identification and mitigation process. NIST also published a second, voluntary version, of the framework for private CIP entities and other interested parties to enhance their cybersecurity, as well (Executive Order 13636, 2013). The administration published Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, within days of EO 13636. This policy reiterated the need for the federal government to work with SLTT governments and agencies, along with private-sector CIP owners, operators, and international partners to identify and address vulnerabilities, mitigate threats, improve recovery efficiency, and minimize disruptions or downtime. The Secretary of Homeland Security received authority and responsibility for oversight of this program, along with the charge to partner with Sector-Specific Agencies (SSAs) to utilize their expertise and knowledge. Each of these SSAs (Commerce, Energy, Justice, GSA, Communications, and others) acquired additional responsibilities and tasks in support of this policy and its strategic initiatives. These imperatives included improving functional relationships regarding CIP, setting minimum needs and standards of operation for networks and systems, and developing and deploying actionable policies for CIP maintenance and protection. The implementation of this policy included updated visibility of the status of CIP threats and operations across systems and enhanced risk management programs to guide future needs and research priorities (Presidential Policy Directive 21, 2013).

Cybersecurity Policy Actions 2014 to Present

In December of 2014, Congress did something it had not done in twelve years, which is pass cybersecurity legislation through both houses. A number of pieces of legislation were proposed between 2003 and the earlier part of 2014, but nothing substantive passed or became law through Congressional action. In December of 2014, however, Congress approved five separate pieces of legislation: The National Cybersecurity Protection Act of 2014, The Federal Information Security Modernization Act of 2014, the Cybersecurity Workforce Assessment Act, the Homeland Security Workforce Assessment Act, and the Cybersecurity Enhancement Act of 2014 (Trautman, 2015).

The National Cybersecurity Protection Act (NCPA) amended the Homeland Security Act of 2002 and provided for the creation of the National Cybersecurity and Communications Integration Center (NCIC). The NCPA directed the NCIC to serve as the "federal civilian interface for sharing cybersecurity risks, incidents, analysis, and warnings for federal and non-federal entities" (Public Law 113-282, 2014). The NCIC also received responsibility for enabling action across federal and non-federal entities, facilitating coordination to address risks and incidents across sectors, conducting and sharing analysis, and providing "technical assistance, risk management, and security measure recommendations" (Public Law 113-282, 2014). The NCPA also tasked the Under Secretary of Homeland Security to create and maintain response plans for cybersecurity incidents and risks against critical infrastructure and required the OMB to submit reports to Congress and impacted individuals when data breaches occurred in protected federal systems (Public Law 113-282, 2014).

The Federal Information Security Modernization Act (FISMA) of 2014 amended the FISMA of 2002 to reset the Director of the OMB with oversight over information security policies and the Secretary of the DHS with implementation authority of the same. The FISMA further provided for the DHS to operate the Federal Information Security Incident Center (FISIC), deploy technology to assess and mitigate cybersecurity vulnerabilities, and required several reports on data breaches, effectiveness, and major incidents on an annual basis (Public Law 113-283, 2014). The Cybersecurity Workforce Assessment Act required an assessment of the cybersecurity workforce within the DHS by its Secretary and required a report within 120 to the appropriate Congressional committees on the cost and practicality of creating a Cybersecurity Fellowship Program for the DHS for a designated period. The Homeland Security Workforce Assessment Act provided improvements for compensation rates and hiring practices for cybersecurity positions within the DHS and was enacted as part of the Border Patrol Agent Pay Reform Act of 2014. (Trautman, 2015).

The Cybersecurity Enhancement Act (CEA) of 2014 amended the National Institute of Standards and Technology Act to allow the Director of NIST to facilitate and support the development of voluntary cybersecurity standards for critical infrastructure. This program required the Director of NIST to coordinate with public and private partners in critical infrastructure sectors to identify risks, best practices, corrective measures, and methodologies to mitigate potential impacts and threats against critical infrastructure assets. This program created a revolving, four-year program window, whereas a new set of standards went into effect their effectiveness and utility came under immediate review and those results drove the following set of standards. As this program was voluntary for the public and private partners, the legislation specifically prohibited the Director of NIST or other federal entity from requiring organizations to comply with the accepted standards. The CEA further expanded the research and development for cybersecurity under the Office of Science and Technology Policy (OSTP) (Public Law 113-274, 2014).

After this wave of legislation, President Obama published Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*, in 2015 to build upon previous policies and improve communications within the cybersecurity arena. This order encouraged the establishment of Information Sharing and Analysis Organizations (ISAOs), units that could be based on one of several different common traits to improve communications. The order further directed the National Cybersecurity and Communications Integration Center (NCCIC), established in the 2002 HAS, to maintain communications with these groups and act as overseer and facilitator for needed improvements, along with other minor adjustments (Executive Order 13691, 2015). Six weeks later, President Obama published Executive Order 13702, *Creating a National Strategic Computing Initiative*. This established the Initiative, an effort to incorporate academic and private sector research and improvements across the entire range of government networks and systems to maximize the benefits of the ongoing high-performance computing (HPC) efforts. This initiative involved the DoE, DoD, and NSF as lead agencies, the Intelligence Advanced Research Projects Activity (IARPA) and NIST as research and development agencies, and NASA, FBI, NIH, DHS, and the National Oceanic and Atmospheric Administration (NOAA) as deployment agencies, with directors of OSTP and OMB as leaders of the oversight council (Executive Order 13702, 2015).

In February 2016, Executive Order 13718 created a Commission on Enhancing National Cybersecurity across government, business, and society. This commission included representatives with knowledge or experience in cybersecurity, law enforcement, technology, private industry, and other areas, with further positions available based on recommendations by senior elected officials. This order assigned the commission to recommend improvements and enhancements for cybersecurity across all levels of government and the private sector. The mission and goals of the commission were wide-ranging and complex, including identifying vulnerabilities, threats, and barriers to enacting proposed changes and how to overcome them (Executive Order 13718, 2016).

Presidential Policy Directive 41, *Directive on United States Cyber Incident Coordination*, and its annex, were published in July of 2016. This effort further codified the coordination and communication among federal and other governmental agencies and outside partners regarding responses to cyber incidents. This policy directive provided guiding principles for incident response, including shared responsibility, risk-based responses, respecting affected entities, unity of effort, and enabling restoration and recovery of impacted resources. The policy also designated several efforts to be enacted simultaneously in response to an attack, each of which addressing a separate aspect in a effort to counter and mitigate the threat, enable law enforcement and intelligence operational needs, and bringing any impacted systems back online as rapidly as possible. To coordinate these efforts, a Cyber Support Group received primary authority, with Cyber Unified Coordination Groups (UCGs) available to act in the immediate aftermath of events under the improved agency and government-wide communications protocols established under this directive and others (Presidential Policy Directive 41, 2016). This also involved the creation of the Office of State and Local Coordination.

Cybersecurity in the United States 2002 to Present

In the early part of the 2000s, a wide range of cyber threats emerged with little clear guidance or mitigation techniques in place. Around the turn of the century, businesses and agencies did not understand the impact the so-called Y2K bug would impact systems. Computers produced over the previous decades only recognized a two-digit year identifier, meaning when the calendar rolled over to 2000, computers would default those transactions to 1900, potentially effecting entire sectors. Multiple other attacks also raised the profile of cybersecurity without legislative changes. President Bush started addressing this in 2001-2002, as discussed in other sections. However, even with the updates three different issues were identified with the policies. First, assessment and identification of threats lacked specificity or other evidence-based foundation, instead relying on anecdotal information and institutional knowledge. Secondly, policies and procedures lacked linkage between objectives and incentives, often relying on publishing a policy for how to act but failing to provide with positive or negative consequences for compliance. Last, the established policies averted adding regulations or standards for cybersecurity especially as it related to private sector entities, despite the noted impact and vulnerabilities they faced. The new policy was initially released to the public in late 2002 and published as *The National Strategy to Secure Cyberspace* in February 2003 (Berkowitz & Hahn, 2003).

Reviewing cybersecurity from 2002 to 2012, one can argue computer systems ended less secure than they started. There are a few contributing factors for this, beginning with the increasing number of targets to exploit. If cybersecurity remained constant in its success in preventing attacks, the overall volume would increase in proportion to the larger number of targets. As attacks evolve and become more complex, they also can disrupt wider sectors and impact more systems. Working to counter these trends requires an understanding of the threats and vulnerabilities. While many policies and news stories promote threats as individual or state-sponsored hackers, the insider threat also needs to be considered and addressed. The internal threat, or the risk associated with employees or agencies representatives, can be more difficult to disrupt with policies and procedures, depending on the nature of the threat. If the risk associated is due to a lack of training or understanding, such measures can be beneficial. They are less impactful when insiders take active efforts to circumvent security to steal or introduce vulnerabilities for their own benefit. Mitigating this type of risk requires addressing technical and nontechnical factors, including software development cycles, lack of adequate talent, and inherent security structures and architectures. Many security managers struggle to adequately quantify the risk and financial impact of not making changes to security protocols, which can lead to vulnerabilities left unaddressed and additional risk (Garfinkel, 2012).

At the beginning of this period, cybercrime existed, but was still very much in its infancy. According to the *Internet Fraud Complaint Center (IFCC) 2002 Internet Fraud Report*, the financial impact of cybercrime ran $61 million, arising from virus recovery, computer fraud, and denial of service losses (National White Collar Crime Center & the Federal Bureau of Investigation, 2002). In the 1990s and the early part of the 2000s, individual users assumed primary responsibility for protection against from hacking and cybercrimes, as most Internet service providers (ISPs) and networks did not actively filter information. As the number of users grew and more information passed through and ‘lived’ in these networks, ISPs and other organizations gradually realized the value of providing some level of security to the systems (Eeten & Bauer, 2009).

This early era of cybercrime also saw an evolution from smaller, singular attacks to broader, wider spectrum ones. At the outset, most computer attacks arose from a hacking event or malicious software attacking a single or small group of computers through and e-mail or other entry point. These attacks caused substantial damage to the targeted system, but also alerted the user quickly of the impairment. As users and networks adjusted to mitigate these types of attacks, hackers and other cyber criminals adjusted tactics. This era saw the rise of malware distribution used to infect targeted computers and allow the hackers to take control of these systems and attack third-party systems. These types of attacks, known as ‘botnets’, can include hundreds, thousands, or even millions of corrupted systems remotely controlled by an individual or group to cause significant outages to sites, networks, or systems (Eeten & Bauer, 2009).

As access to technology grew easier over the last decade and a half, the frequency and impact of cyberattacks increased exponentially. Not only more users logged into networks around the world, but more business was and is conducted in the digital realm, and more data is stored there. In 2012, Norton reported 556 million individuals as victims of cybercrime at a cost of $388 billion (Galeotti, 2012). A 2014 report by the University of Singapore put the damages of cyberattacks for that year at over half a trillion dollars and a 2015 study from the Ponemon Institute found a 19% increase in cybercrime from the previous year (Greengard, 2016). Over the last few years, reports of hacking and its impacts on companies, organizations, and citizens garnered much attention. Government agencies, such as the Internal Revenue Service and Office of Personnel Management, and private companies like Target, Wells Fargo, and Home Depot suffered massive data breaches. In each of these both the companies and the consumer/citizen suffered as a result. The companies dealt with loss of consumer trust, loss of proprietary information, and investment to harden systems while the individual faced a range of possibilities from identity theft and damaged credit ratings to loss of confidence, but little to no damage (McCollum, 2015).

Even with all the reports, data, training, and investment in cybersecurity over the last few decades, cybersecurity remains a widespread issue from the individual to the national level. Over the last two decades several different descriptions and views of cybersecurity arose, each with its own strengths and weaknesses. Cybersecurity can be viewed as an insider issue, an economic problem, a public health-type issue, and a wicked problem with no obvious solution. The insider issue seeks to prevent individual users from making poor decisions, either maliciously or in error, that cause security vulnerabilities inside the systems. The economic model seeks to match increased spending with improved security, but to date evidence does not support direct correlation between straight investment and improved security due to outside factors. The public health description frames cyber hygiene in the context of keeping systems clean by running up-to-date antiviral programs, making proper decisions about browsing and file downloads, and user security protocols. The most common description, however, is cybersecurity as a wicked problem with a myriad of inputs and variables and no single solution or set of steps to take to improve the situation (Garfinkel, 2012).

Department of Defense Policies and Organizations

The Department of Defense (DoD) has a long and complex history regarding computers and cybersecurity policy and development. From the few operators and rudimentary operations of the ARPA Net to the billions of users and complex activities of today’s world, the Department of Defense remains on the forefront of cybersecurity. As noted previously, legislation throughout the years saw changes in the oversight of federal networks and security between the military and civilian control. The DoD had some of the first cybersecurity organizations in the U.S. as a result of their early responsibilities, but these evolved over the years and currently focus on defense intelligence operations and national security networks. Military agencies were established at different points and with different types of missions from the creation of the first telecommunications networks onward. The defense agencies with primary missions centered on cybersecurity itself were the Air Force Information Warfare Center (1993), the Navy Information Warfare Activity (1994) and the Army Land Information Warfare Activity (1994). The Chief of Staff and Secretary of the Air Force published *Cornerstones of Information Warfare* in September 1995, which served as an initial glance at the possibilities and threats in the cyberwarfare arena. This was not the first time it was considered but served as one of the earliest cyberwarfare policies in the U.S. (Warner, p. 791).

In its current form, DoD cyber operations are overseen by the U.S. Cyber Command (USCYBERCOM), an organization encompassing all military branches and the federal government. The Secretary of Defense signed the order to establish this organization on June 23, 2009 as a support unit for the U.S. Strategic Command (STRATCOM). USCYBERCOM was designated as fully mission capable on October 31, 2010. Under USCYBERCOM are five separate service elements: Army Cyber Command (ARCYBER), Fleet Cyber Command (FLTCYBER), Air Force Cyber Command (AFCYBER), Marine Corps Cyber Command (MARFORCYBER), and Coast Guard Cyber Command (CGCYBER). CGCYBER, while in a direct support role for USCYBERCOM, is also a subordinate command for the Department of Homeland Security (U.S. Strategic Command, 2016). In its current form, USCYBERCOM is jointly located with the NSA, utilizes personnel and networks of that agency, and is headed by the Director of the NSA.

As a mission, USCYBERCOM oversees the operation and defense of the DoD information networks (DODIN) and both prepares and conducts military cyber operations to secure and ensure viability of cyberspace for the United States and its allies and deny use to enemies of the state. To complete these tasks, USCYBERCOM “has three focus areas: defending the DODIN, providing support to combatant commanders for execution of their missions around the world, and strengthening our nation’s ability to withstand and respond to cyber-attack” (United States Strategic Command, 2016). Defending the

DODIN is an incredibly complex task with multiple layers of oversight, coordination, and communication required from departments across the defense sector. The DoD Chief Information Officer (CIO) published new guidance for the department in November of 2013, with an unclassified version following five months later. The DoD Cybersecurity Policy Chart is the visual map of the strategy laid out by the DoD CIO and is updated as needed, most recently on June 30, 2017. The strategy issued included four focus areas that the policy chart is organized to address: “establish a resilient cyber defense posture, transform cyber defense operations, enhance cyber situational awareness, and assure survivability against highly-sophisticated cyberattacks” (Cyber Security & Information Systems Information Analysis Center, 2017).

The DoD Cybersecurity Policy Chart includes five separate goals, along with authority, guidance, and oversight offices for each. The chart is also color-coded, based on the office of primary responsibility (OPR), and provides hyperlinks to many external resources. This chart demonstrates the complex and interconnected nature of the cybersecurity environment at the federal level. The chart includes fifteen separate OPRs, in addition to other sources, including Executive Orders and other national strategies and policy documents. The policy chart includes overarching authorities for cybersecurity, and flows from organization (leading and governing, designing the fight, developing the workforce, and partnering for strength), to enabling (securing data in transit, managing access, and assuring information sharing), anticipation (understanding the battlespace and preventing and delaying attackers and preventing attackers from staying), to preparation (developing and maintaining trust, strengthening cyber readiness, and sustaining missions) (Cyber Security & Information Systems Information Analysis Center, 2017).

To support combatant commanders and ensure the continuity and utility of cyberspace for the United States and its allies, USCYBERCOM operates across multiple sectors. First and foremost is the need to transform cyber policies, programs, and activities into elements that can be used to support operational objectives and needs around the world. This includes integrating cyber capabilities into operational planning, strategic, and tactical decision-making processes. To support this operationalization, USCYBERCOM has to not only field a range of support teams, but also must ensure those teams have proper training, capacity, and authority to protect national interests and continue to improve the security and resilience of cyberspace moving forward (United States Cyber Command, 2015).

As described above, each military department maintains their own specific cyber command, which include Computer Emergency Response Teams (CERTS) and Cyber Mission Forces (CMFs). The CMFs, as envisioned in this policy, consist of 133 separate units, organized to provide a defense-in-depth against cyberattacks and closely aligned with other cyber forces both within the DoD and those outside. The construct and overall design of the CMF program flowed from the nature of the networks maintained by the DoD, especially the size, complexity, and the fact the DoD does not own and operated its entire network, relying in some areas on private sector resources. The prevalence of private sector assets is another reason the DoD felt the need to alter its policy to include a greater emphasis on deterrence before the attack and risk-based analysis to cover the highest threats as quickly as possible. By decentralizing the CMF structure, the DoD also gains the ability of highly flexible and narrowly focused cyber teams while maintaining a larger vision and set of strategies to guide their efforts (Department of Defense, 2015). Under the ‘133 teams by 2018’ goal, the DoD currently fields 13 National teams, 68 cyber protection teams, 27 combat mission teams, and 25 support teams consisting of over 6,000 personnel from the military and private sectors (Department of Defense, 2015).

The changing landscape of cyber networks and cybersecurity over the years necessitated changes and updated priorities. Defense strategies likewise adapted to changes and priorities, with new guidance and policies periodically released. *Department of Defense Strategy for Operating in Cyberspace* released in July of 2011 included an overview of the strategic cybersecurity environment and five strategic initiatives to provide a roadmap forward for the DoD. The strategy noted at the time the DoD ran more than 15,000 networks with over 7 million connected devices, and the department was ever more reliant on information systems to conduct its operations and ensure national security. The strategic initiatives included reorienting cyberspace from a support structure to an operational domain, developing proactive techniques for network defense, establishing working relationships with SLTT governments, private CI partners, and U.S. allies, along with leveraging the knowledge and abilities of the citizenry to strengthen operations (Department of Defense, 2011).

The DoD overhauled its cybersecurity strategy in 2015 after additional changes to their mission and increasingly destructive and frequent attacks. The department, as referenced in the new strategy, owns and operates one of the most extensive computer networks in the world. As this grew in complexity and scope, the needs for improved cybersecurity and policies to safeguard it expanded. In 2012, President Obama tasked the DoD to develop more robust cybersecurity and risk mitigation in concert with other federal departments. The DoD also needed a new guiding strategy that incorporated the Cyber Mission Force (CMF) concept, a group created by the department in 2012 to execute its cyber operations. The 2015 Cyber Strategy drew on those three key motivators and sought to capture the need to bring in assets from the private sector and community, along with improving the deterrence aspect of cyber operations and providing a roadmap for DoD cyber operations through 2020. The policy laid out five key goals for DoD cybersecurity: build and maintain forces and capabilities for this domain, defend networks while securing data and mitigating risks, create plans for significant cyberattacks that could disrupt CI, develop new cyber weapons to shape the battlefield and control the fight, and work with international partners to improve cross-border security. (Department of Defense, 2015).

In the latest decision-making paradigm, DoD cyber leaders are treating cyberattacks like other domains of warfare. Based on the DoD Cyber Strategy published in 2015, DoD officials examine attacks individually to determine their level of impact to classify the nature and severity of each incident. As discussed in earlier sections, cyberattacks are no longer constrained to denial of service or information security operations, but can now cause physical damage to systems or, in the case of CIP attacks, death due to service interruption. While no absolute threshold is provided, there is a level of impact and injuries to citizens that can equate a cyber-attack to a more traditional armed attack. The specifics of each attack are collected and provided to senior leaders and the Office of the President to determine how the threat will be addressed. The inclusion of cyber into this conversation is another facet of deterrence, which was a key point in the 2015 Cyber Strategy. At this time, it is unknown how this evolution of warfare will play out, or what type of impact it will have on international and interstate relations (Pellerin, 2016).

Current Federal priorities

As the federal government evaluates is cybersecurity policies and priorities, there are several different factors to consider. One of the main issues the current administration must address is what shape does the United States want the Internet to take in the coming years and what type of governance will be acceptable. The Internet is a worldwide asset that largely ignores borders and jurisdictional considerations, forcing countries around the world to work together to manage growth, capacity, security, and a myriad of other issues regarding cyberspace. Federal authorities need to develop plans for security, privacy, governance, freedom of speech, and any other priorities desired and work to collaborate with international partners to push the desired agenda (Healey & Jordan, 2016).

Another issue is whether to rely on defensive measures for protection or to develop offensive countermeasures for first strike/retaliatory capability. For several years, the U.S. government was adamant its interest was in defensive measures only, but events over the last decade showed the development and willingness to use offensive capabilities. The STUXNET worm previously discussed was the first publicly acknowledged use of offensive cyber tactics by the U.S. government against a foreign power, but there have been other reports, as well. There are multiple questions that arise from the militarization of cyberspace and the development of offensive weapons to deploy in this space. Policy questions on when cyberattacks can be used, if they are an appropriate counter or response to physical attacks, who can conduct attacks, and what types of attacks can be utilized are all emerging issues under development (Gjelten, 2013).

In developing techniques, tactics, and weapons to be utilized within cyberspace, there remains a debate on how defined the cyber arena is for warfare. Cyberspace is often described as an alternate domain like the more traditional arenas of land, air, space, and sea. There is still discussion about the characterization of the virtual world and whether it should be considered as a separate battlefield or dealt with as a business environment (Barnard-Wills & Ashenden, 2012). Wingfield and Sharp discuss this difference in opinion, likening it to the development of the tank in World War I. When first conceptualized, many military leaders had difficulty figuring out how to use the machine effectively. The machinery broke down frequently, were underequipped, and did not possess enough firepower. By World War II, however, the Germans recognized the potential of the tank in maneuver warfare, creating new doctrine and shifting the course of the war. Cyberwarfare and the tools for cyberattacks are following a similar path as the tank in the early years of its development. Governments are still debating how to effectively and properly use cyber warfare, but different actors have varying opinions on how to use cyberwarfare. The threat now is the same as it was with the development of the tank, allowing enemies to develop offensive weapons or tactics while leaders debate proper applications (Wingfield & Sharp, 2014).

With the DHS serving as the primary government agency for cybersecurity policy, oversight and conflicting political motivations complicate the development process. Over 100 separate committees in Congress claim some level of oversight of DHS programs, requiring leadership to spend significant amounts of time testifying before Congressional leaders and limiting the time available for running the department. The DHS, with such extensive oversight commitments, is effectively accountable to everyone and no one at the same time. The federal government not only needs to determine where its priorities lie, but also to streamline the oversight and guidance for the DHS if it hopes to reach the level of agility needed to address the cyber threat going forward (O'Hara, Murphy, Vreeburg, Giaier, Maurer, Geffroy, & Lowe, 2015).

Policy analysis – Current Issues in Cybersecurity at Federal Level

Cybersecurity policy, like many others, reaches across many different stakeholder groups and sectors. Fewer and fewer industries and organizations in the world today are without some level of online footprint. Digital presence and marketing are now an integral part of the business cycle, along with utilizing digital resources for storage, collaboration, and governance. As cybersecurity grows in importance, stakeholders and those seeking policy changes need to mold their message to target different distinct audiences: businesses, governments, elected and appointed officials, the public, security professionals, and others. One on the larger issues remaining, however, is that cybersecurity does not generally fit neatly within the security or national security conversations and techniques utilized in the past. Cyberspace does not, to a large extent, recognize international borders, making it difficult for law enforcement or government agencies in one country to independently pursue foreign agents conducting cyberattacks. Reliance on militarization of cyberspace, or employing similar tactics, also runs into a few issues due to the public and private ownership of much of the infrastructure and the lack of oversight the government has in that realm (Lobato & Kenkel, 2015).

Cybersecurity policy development, as discussed earlier, relied heavily upon executive action between 2002 and 2014. In 2002, sweeping legislation passed Congress following the September 11, 2001 terror attacks that included numerous provisions for counterterrorism and cybersecurity. While both houses of Congress proposed several bills in the interim, it was 2014 before an agreement, with five separate pieces of legislation related to cybersecurity published in December of that year. As evidenced by the verbiage of the Presidential Actions over the last 15 years and the verbiage of the 2014 legislation, cybersecurity at the national level is frequently framed as a critical infrastructure issue. Within this larger debate, there are issues of technical knowledge, conflicting priorities of different stakeholders (consumers, governments, businesses, law enforcement and national security, among others), political considerations, and lack of a cohesive starting point or policy to draw from (Trautman, 2015).

Looking at the critical infrastructure protection (CIP) discussion, there are several factors relevant to cybersecurity. Many of the industries and sectors are increasingly controlling widely distributed networks using the Internet. Two types of components, supervisory control and data acquisition (SCADA) and distributed control systems (DCS), are the most vulnerable to cyberattacks. These are so vulnerable due to their function: providing command and control to flow in distributed systems and managing processes across entire facilities. The Stuxnet worm attack was a type of SCADA attack, infecting SCADA files across a network to eventually cause physical damage in an enrichment facility. The infrastructure across the United States relies on the same systems and exhibits similar vulnerabilities, increasing their vulnerability. Before the Internet, such systems were protected with physical barriers, but the inclusion of Internet protocols for backup, troubleshooting, and coordination also removed the need to physically enter a site to take control of such critical infrastructure. Adding to the complexity of securing critical infrastructure is the fact that many of it is privately owned, with only recommended cybersecurity protections and reporting in place. Even the latest legislation enacted placed voluntary protocols on CIP and prohibited federal authorities from requiring public and private partners from to adhere to specific standards. Authorities reported an almost 400% increase in cyberattacks on critical infrastructure around the country between 2012-2013, making it apparent that this is not an issue likely to abate without significant intervention (Pedersen, 2014).

To counter this trend, the federal government sought and seeks to create partnerships with public and private sector entities involved in critical infrastructure. Critical infrastructure in the United States covers a variety of elements, from nuclear energy and transportation to agriculture and cybersecurity. When developing a partnership, government agencies need to bring together disparate outside parties that may or may not see themselves as part of the infrastructure sector, or who may not wish to take part. There are also issues of oversight, accountability, and enforcement. It was noted earlier that the DHS is prohibited from requiring third parties from adhering to cybersecurity standards, so they must find alternate ways to bring partners to the table and convince them of the utility of cooperation. Public policy in this area applies funding to improve cybersecurity, but there is little evidence of improvement. In past reviews of CIP partnerships, the GAO concluded the lack of accountability to standards and fiscal expenditures may lead to a less secure environment (Koski, 2015).

While the current cybersecurity standards and policies from the federal government lack accountability and enforcement, there are indications the policies and frameworks from 2014 are making an impact. Several industry leaders in CIP and other industries incorporated these standards and some require them of their vendors, as well. Further, the NIST policy adopted in 2014 is considered the standard for due diligence when developing cybersecurity policies. With elected officials and industry leaders unable or unwilling to develop and enact wider-ranging and binding cybersecurity legislation, this type of voluntary, grassroots-type movement could be the best option for improving industry buy-in and security on a wider scale (Shackelford & Bohm, 2016)

Policy Analysis – Security policies and operations in Middle Tennessee

Cybersecurity at the state level in Tennessee falls mainly under the purview of two different departments: the Tennessee Bureau of Investigation (TBI) and the Tennessee Office of Homeland Security (TOHS), depending on the nature of the situation. The TBI focuses on the law enforcement issues, such as child victimization, child pornography, fraud, and hacking, malware, computer intrusion, and identity theft (Tennessee Bureau of Investigation, n.d.). The TOHS deals with homeland security issues, including responding to suspicious activities around the state, raising cyber awareness, protecting critical infrastructure, providing training for law enforcement, partners, and citizens, and management of emergency protocols (Tennessee Department of Safety and Homeland Security 3, n.d.).

The State of Tennessee has two major sections of its code addressing cybersecurity. The first is Title 39, Chapter 14, Part 6, the *Tennessee Personal and Commercial Computer Act of 2003*. This section of Tennessee law addressing computer hacking, malware, unauthorized access, trespass, and installation of viruses on private or commercial computers. This further specifies punishments for various cybercrimes, including theft, destruction of files, illegal access of networks, and use of computers or networks in connection with terrorism (Tennessee Personal and Commercial Computer Act, 2003). The second major piece of legislation within the Tennessee code is Title 47, Chapter 18, Part 52, the *Anti-Phishing Act of 2006*. This act addresses phishing activity within the state and establishes penalties for such actions (Tennessee Anti-Phishing Act, 2006).

Since the September 11, 2001 terror attacks, state-level security policies and procedures in Tennessee followed a similar path to that laid out at the federal level. In the immediate aftermath of the terror attacks, on October 2, 2001, the State created the Tennessee Homeland Security Council. The council was composed of “representatives from state and local departments and agencies who are tasked with helping plan and direct the statewide homeland security activities" (Tennessee Department of Safety and Homeland Security n.d.). The Council is headed by the Commissioner and Homeland Security Advisor from the Tennessee Department of Safety, and is members are tasked with coordination at higher and lower levels of government for homeland security purposes (Tennessee Department of Safety and Homeland Security n.d.). On October 1, 2002, the Governor of Tennessee issued Executive Order 36 on September 11, 2002, creating the Tennessee Office of Homeland Security, codified the Homeland Security Council, and created the Tennessee Governor's Citizen Corps Advisory Committee (State of Tennessee Executive Order 36, 2002).

In 2005, the State of Tennessee followed the lead of the federal government and established the National Incident Management System (NIMS) as the standard for all incident management in the State. As the NIMS system was the national standard and incorporated communication and operational considerations for state and local governments, it was the most effective option for the State, as well (State of Tennessee Executive Order 23, 2005). Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, established the NIMS program by tasking the Secretary of Homeland Security with developing and administering the Management system and a National Response Plan for all manner of domestic incidents. The NIMS program sought to create a single set of standards and practices for federal, state, and local governments and agencies for incident response and management. The description and standards set out for the program in HSPD-5 also consolidated crisis management and consequence management for domestic incidents into a single category. Prior to this, federal agencies and programs would have separate planning procedures for each side. HSPD-5 also noted the primacy of state and local governments in local disaster response and management and established certain situations where the DHS would assume control. In all cases, however, HSPD-5 directed response plans at all levels to be compatible and interoperable (Homeland Security Presidential Directive 5, 2003).

The Office of Homeland Security, Security Council, and Citizen Corps Advisory Committee were originally a subset of the Governor's office, but were transferred to the Department of Safety under Tennessee Executive order in June of 2007 "in the interest of economy, efficiency, and better coordination of the functions of state government" (State of Tennessee Executive Order 48, 2007). In 2012, the Governor's office issued Executive Order 16, dissolving the Tennessee Governor's Citizen Corps Advisory Committee based on direction from the U.S. DHS and in the interests of administrative efficiency (State of Tennessee Executive Order 16, 2012). These changes brought the Department of Safety and Homeland Security to its current functional structure and mission. Homeland Security in Tennessee is currently collocated in the Department of Safety, alongside the Tennessee Highway Patrol, Driver Services, and the Tennessee Highway Safety Office. The Office of Homeland Security is further broken down into three divisions: Analytics (Including the Tennessee Fusion Center), Operations, and Preparedness (Including Cyber and Special Programs) (Tennessee Department of Safety and Homeland Security 2, n.d.).

With the TBI focusing on the law enforcement side of cybercrime, the TN DOHS shoulders much of the responsibility for cybersecurity within the State of Tennessee. The

Governor laid out a plan to create a Cyber Security Advisory Council in the *Safer Tennessee* proposal for 2016-2018 to "establish and oversee implementation of a comprehensive cyber security plan for the executive branch of state government" (Tennessee State Government, 2016). Throughout the research for this project no information on this advisory committee was found online or in other related materials. The DOHS cyber awareness portal section of the website contains information on ransomware attacks, monthly security tips, phishing and social engineering, frauds and scams, cybersecurity awareness month, a cyber reference aid, cyber safety tips, and a scam alert. The monthly security tip links to a 2015 document, and of the two links in the frauds and scams, one is an up-to-date FBI link and the other is from 2013. The phishing and ransomware link on the site are also up-to-date, but the rest of the links all connect to forms and ages from 2013, with correspondingly dated information (Tennessee Department of Safety and Homeland Security 4, n.d.).

A search for cybersecurity and related legislation in the online archives for the Tennessee legislature do not reveal any notable action at the state level. There is a similar lack of information available on cybersecurity policies at the county and local levels. While governments at the county and local levels have their own sites, cybersecurity and assurance are not action items on the county of local government sites. The lower government sites also do not include any information on cybersecurity programs, policies, or procedures at these levels of operation. Additional information and clarification will be sought in these areas during the interview process.

In the following chapter, the role of the researcher, methodology, and trustworthiness of the proposed research will be discussed. The role of the researcher will cover any potential biases, conflicts of interests, or any relationships that could impact the proposed study. The methodology of the study will include an examination of the population and sample size to be used in the study, including selection criteria and explanation of saturation. The methodology section will also include descriptions of the proposed contacts with the participants, instruments to be utilized, and a discussion of the data collection methods. Finally, questions of credibility, transferability, dependability, and confirmability will be addressed.

Chapter 3: Research Method

Introduction

Over the past several decades, cyberattacks rose from a concern of IT departments and financial institutions to an issue of national prominence and seemingly part of the daily news cycle. Historically, public policy is a slow-moving process that requires significant investments in time, resources, and political will (Sabatier, 1988). In a technically complex and broad-ranging area such as cybersecurity, policy development faces additional challenges and roadblocks, slowing the process and requiring operational decisions on how to operate while awaiting guidance. Depending on the nature of the field agency in question, these gaps can be bridged by executive order or legislative guidance or governed by the mission of the agency itself. At the federal level, cybersecurity policies and procedures for intelligence and law enforcement evolved after the terror attacks of 9/11. The USA Patriot Act included changes across multiple areas, including cybersecurity, wiretapping, money laundering, and others (USA Patriot Act, 2011) As attacks increased in frequency, scope, and effectiveness, however, it became unclear whether updated policies and procedures kept pace and provided agencies with the tools needed in the current environment (Barnard-Wills & Ashenden, 2012).

This chapter includes detailed information on the research methodology and instrumentation. First, I will provide an overview of the research design and rationale, including the research questions, central concepts, and research traditions. Next, the role of the researcher will be defined, and relationships, potential biases, power relationships, and other ethical issues will be identified, along with plans for addressing these areas. I will then discuss the methodology, including the participant selection process; instrumentation; procedures for recruitment, participation, and data collection; and data analysis plan. Issues of trustworthiness and ethical procedures, including IRB documentation and participant protections, will then be discussed.

Research Design and Rationale

Cybersecurity at the federal and international level is in the news on a consistent basis. Executive orders and Congressional actions provide governance at the federal level, with different agencies enacting policies under that guidance to protect citizens and national assets (National Cyber Strategy, 2018). Below the federal level, the process is less clear as there is no mandate or standard for cybersecurity, with states and different sectors managing their processes according to individual preferences and governance (Glennon, 2012). Reviewing intended policy outcomes against what the emergency management officials and field agencies observe in their operational fields may help identify and define disconnects around cybersecurity. With this information, policy makers at the state and local level may be able to pursue policies or identify resources to assist with closing gaps or improving communications between partners.

The purpose of this study was to investigate the current state of cybersecurity policy at the state and local level, specifically in Middle Tennessee and its surrounding areas. The principal research question answered by this inquiry was whether cybersecurity policy at the federal level provides enough guidance and resources for state and local governments and agencies. I queried elected officials, agency representatives, subject matter experts, practitioners, and emergency managers to ascertain how the federal policies and procedures guide lower-level legislation and operations. Of interest were issues of resource allocation, authority, oversight, and coordination with public and private partners.

One additional question considered was whether there is a discrepancy in the established public policy on cybersecurity and the reality in the operational environment, along with what changes occurred from initial implementation to field readiness. Discrepancies can develop for a variety of reasons, including lack of understanding of a given policy or piece or legislation, limited funding, or conflicts in organizational mission with established policies (Hudson, Hunter, and Peckham, 2019). The lack of awareness between emergency managers or field agencies and the policy developers or elected officials of a gap in implementation creates an environment where neither side is really addressing the needs of the community, as both are working on different problems with different resources. Hudson, Hunter, & Peckham (2019) discussed some of the problem areas for implementation. These areas of concern include:

> complexity (underestimation of the delivery challenges); evidence base (insufficient objective, accurate and timely information on costs, timescales, benefits and risks); misunderstanding of stakeholders (optimism about the ability to align different views); behavior and Incentives (interested parties boosting their own prospects); and challenge and accountability (decision-makers seeking short-term recognition).(Hudson, Hunter, & Peckham, p.2)

If multiple policies require similar changes after implementation to make them acceptable or feasible for field operations, there may also be a systemic issue or lack of understanding on the part of the elected officials that needs to be addressed.

Research Tradition

Qualitative studies, such as this, encompass a range of designs. Creswell (2013) detailed the five primary types of qualitative research: narrative, phenomenological, grounded theory, ethnographic, and case studies. In the third edition of his work *Qualitative Inquiry & Research Design: Choosing Among the Five Approaches*, Creswell provided definitions, background information, examples, procedures, and challenges for each type (Creswell, 2013, pp. 69-107). The first of these designs, narrative inquiry, has a history reaching back into the mid-1800s, when researchers used narrative-type inquiries in social science studies with educational components (Connelly & Clandinin, 1990). The narrative description defines not only the structure of the study, but also the pattern of the study, as well. As humans recount experiences through a series of stories and experiences, the narrative inquiry lends itself to documenting human experience on a personal level (Connelly & Clandinin, 1990). Connelly and Clandinin (1990) provided an in-depth explanation and exploration of narrative inquiry for a variety of social sciences (Connelly & Clandinin, 1990). Authors of several studies on cybersecurity have used narrative inquiry, including Hopkins, Wilson, Silva, and Forsythe (2015). In their inquiry, Hopkins et al. grouped participants into two groups to track, solve, and identify possible suspects of cybercrimes. Participants in one group focused on narrative inquiry while participants in another group focused on association of elements of the crime

(Hopkins et al., 2015). The researchers found that the group focused on the narrative achieved more accurate results and identified more aspects of the crime, along with gaining better insights into possible suspects than the group focused on simple association of elements (Hopkins et al., 2015). The narrative inquiry model could be utilized for some studies on cybersecurity, but, this study involved consolidating a number of potentially conflicting viewpoints and missions. I opted against using the narrative model because I concluded that it might not allow me to grasp the complexity of the study phenomenon. In addition, I was worried about potential conflicts in incorporating conflicting narratives.

The second qualitative design, phenomenological, traces its roots to the beginning of the 20th century. At the beginning of the 1900s, Edmund Husserl published a series of treatises regarding a new philosophical approach to research, one that focused on the human experience as a method for collecting data. Husserl, and later Heidegger, expanded upon this theme, positing that the human experience and ego were the central driving force for behaviors (Carr, 1970). Phenomenologists seek to explore the individual lived experience of the participant to achieve a better understanding of the individual’s view of the world (Carr, 1970). Researchers have published several phenomenological dissertations on cybersecurity in recent years, from Caudle’s 2010 *Decision-Making Uncertainty and the Use of Force in Cyberspace: A Phenomenological Study of Military Officers* to Andrѐ’s 2016 *A Phenomenological Study of Frontline Hiring Professionals that Recruit in a Cybersecurity World*. The first study centered on the lived experiences and perceptions of the decision-making process of several military officers working at various cybersecurity commands in Washington, DC, to develop common themes, characteristics, and recommendations for future improvements in the process (Caudle, 2010). The second study focused on the experiences and perceptions of hiring and recruiting managers in the cybersecurity sector (André, 2016). André (2016) found that compensation was a primary driver in the ability to recruit and retain professionals in a limited pool and showed a significant increase in investment in cybersecurity resources across companies to protect infrastructures and assets. Phenomenology is an emerging research method in cybersecurity, with doctoral dissertations occupying most of the published research currently available. This study involved not only individual perceptions and experiences, but policy development as well; for this reason, I concluded that phenomenology was not well suited for my investigation.

The grounded theory arose from a perceived gap between empirical research and theory on the part of its creators. Those researchers, Glaser and Strauss first published *The Discovery of Grounded Theory* in 1965 as an introduction to their new approach. The pair believed their approach bridged the gap between theory and research left by the Columbia and Chicago schools of sociological research. Their approach significantly differed from more traditional research methodologies in that there is no predetermined problem or question at the outset of the study. Instead, the inquiry begins with a general research topic and the researcher collects data based on the research methodology (interviews, surveys, questionnaires, et cetera). The researcher begins forming the theoretical concepts at the outset of data collection, identifying themes and key phrases and reintegrating these into later collection and theory development efforts. The results are coded and further grouped together and compared to both a selected theoretical model and each other. This can provide either positive or negative correlation, depending on how well each data set fits the selected model and compares to others collected (Glaser & Strauss, 1965). As I previously identified both research questions to answer and theory before beginning research, the grounded theory was also not a fit for the proposed study.

Next is the ethnographic method, which can be traced to anthropological research conducted in the early part of the 1700s. As originally conceived, ethnography was a field of study concentrating on how cultural groups interact over time, both within and outside of the group. The expansion of the Russian Empire across Europe and eastward towards Kamchatka greatly impacted the development of ethnography. Gerhard Muller travelled from Germany to Kamchatka conducting anthropological research on the tribes and native groups encountered during the Russian expansion. During the Kamchatka expedition (1743-1753), Muller identified Volker-Breschreibung as a field apart from anthropology. Schlozer and Gatterer took this concept and further developed it into ethnography. As ethnography gained acceptance and usage in France in the mid-1800s, its usage shifted to "physical organization, intellectual and moral characteristics, languages, and historical traditions (Vermeulen, 1995, p. 50). As study did not deal as much with culture and tradition as policy and evolution, ethnography was not seen as a fit.

The final of the five principal qualitative research methodologies is the case study. The case study can be traced back hundreds of years in its current form and much further as a general process originating in the medical field, as the collection of data on individual cases and patients (McLeod, 2008). Case study research as it is currently known has roots in Western Europe and the University of Chicago School of Sociology. Chicago was an epicenter for the case study methodology in the first part of the 1900s due to the influx of immigration in the city. The case study method proved particularly well-suited to many issues related to immigration as it allowed an in-depth examination of the situation and cases studied. One of the most discussed criticisms of case study research is its limited applicability to different populations. The case study typically has a limited focus and provides an in-depth look at a phenomenon, decision-making process, or policy impact on the selected population (Tellis, 1997).

The case study research method has a two-tier definition dealing with the scope and features of a case study. According to Yin (2014), the scope of a case study method states: "a case study is an empirical inquiry that investigates a contemporary phenomenon (the 'case') in depth and within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident" (Yin, 2014, p. 16). This description helps the researcher separate case studies from other methods. Yin's second aspect outlines the characteristics of the case study:

> "a case study inquiry copes with the technically distinctive situation in which there will be many more variables of interest than data points, and as one result relies on multiple sources of evidence, with data needing to converge in a triangulating fashion, and as another result benefits from the prior development of theoretical propositions to guide data collection and analysis" (Yin, 2014, p. 17)

Taken together, the dual definitions of case study research show this methodology as one that returns a detailed and thorough examination of a limited subject field. Limiting the scope of the inquiry to a single case or subset of a larger population allows the researcher to investigate the selected problem at length and follow the research wherever it may lead. Such a design, as noted previously, can limit transferability of the results of a case study to other groups as the environment and behaviors, responses, and decision-making of the participants of the inquiry all impact the results (Yin, 2014).

The case study follows a linear process, but that process also builds upon itself and follows the data throughout the inquiry. The case study originates from a general plan for the inquiry, then the researcher develops questions to be answered by the investigation. Next the target population, instrument, and research design are selected and preparation for data collection begins. Once the collection phase begins, multiple stages may be impacted: analysis, sharing, design, and preparation. Depending on the nature of the results, the researcher may need to redesign part of the inquiry, adjust questions or instrumentation, or conduct secondary analysis based on emerging trends in the data. The researcher continues the collection, analysis, design, and preparation iterations until all data is collected and the final analysis can be conducted (Yin, 2014). I selected the case study method for the proposed inquiry based on its ability to follow emerging trends in current environments and the ability to incorporate many unknowns into the study. I collected and analyzed data from interviews with targeted individuals along with data from agency procedural documents and public policies.

Role of the Researcher

The role of the researcher in the study was to analyze data collected from interviews on cybersecurity policies and procedures at the state and local level in Middle Tennessee. During the interview process, I observed and documented responses and experiences of the interviewees for data collection. After each collection I conducted the iterative analysis/design/preparation process discussed in the previous section to capture emerging trends and prepare for subsequent interviews. I did not have professional connections to any individual participating in the inquiry, and my past personal interactions were limited to brief meetings with local politicians during community events. These interactions did not include any personal or individual contact outside of community forums or events open to the general population. As the individuals participating in the study were elected officials, appointed officials, subject matter experts working with the government, and emergency managers, there was no issue or subordinate workplace relationships.

As a result of my work experience with the military and in the transportation industry, I have experience and knowledge of typical interactions between state and local officials and their associated emergency managers in many different states and local areas. My current role is a university professor in Middle Tennessee, where I have little interaction with the elected officials or emergency managers. To eliminate potential bias based on previous experiences the proposed study focused on a geographic area outside territory I worked in previous positions. The subject matter of cybersecurity was also a significant departure from the operations and transportation focus of my previous experience, further insulating the study. The most important element to prevent personal bias was to focus on the opinions and experiences of the participants during data analysis and adhere to selected instrument during the interview process.

Methodology

A qualitative approach was selected for the proposed inquiry due to the nature of the information sought and the data to be gathered. According to Patton (2002), qualitative research typically derives from one of three types of data: interviews, observations, and documents. The data is generally collected through fieldwork, and the quality of the data, especially with interviews and observations, is directly related to the planning, skill, and quality of work by the researcher. Unlike quantitative research, where statistical analysis and other mathematical techniques define relationships, qualitative research seeks patterns in behavior, perspective, and experiences of the participants. Qualitative research has two principal purposes: research and evaluation. When using the qualitative method in a research capacity, the focus is on testing or generating new theories for a given scenario. Program evaluation, which I conducted for the study, "is the systematic collection of information about the activities, characteristics, and outcomes of programs to make judgments about the programs, improve program effectiveness, and/or inform decisions about future programming" (Patton, 2002, p. 10).

The qualitative method is especially well-suited to evaluate and capture localized differences within larger programs. Case study designs can further be used to evaluate whether the program in question is implemented in the manner intended, if the program deviates from the intended direction during evolution, or if different areas of local programs or entire local organizations are straying from the intended direction and goals of the original program (Maxwell, 2002). The research focused on these questions related to cybersecurity policy at the State and Local level in Middle Tennessee, making the qualitative case study an appropriate design.

Participant Selection Logic

For the proposed study, elected and appointed officials in four Middle Tennessee counties, along with their corresponding emergency managers, subject matter experts, and select officials at the state level were interviewed. The list of targeted offices and agencies across Middle Tennessee is located in Appendix C, along with the associated level of government, and potential number of interviews at each location. To gain access and assistance from Senators and Representatives, initial requests for cooperation were sent to the offices of the Chief Clerks for screening and processing. I selected the target area for the study based on lack of personal connections within the area, a range of socioeconomic and political perspectives and backgrounds within the target population, and a mix of technology-based, urban, and rural economies.

I targeted the Senators and Representatives at both the state and federal level for the state to gain insight into the current legislative mindset on cybersecurity. As noted in Chapter 2, cybersecurity is commonly described as a federal issue, but it has become more and more problematic for lower levels of government. Including state and federal legislators was an attempt to shed light into the proceedings and discussions behind the laws (or lack thereof) on the books in Tennessee. Each of the federal officials of the state was contacted for this study, but only a select few of the Senators and Representatives at the state level. At that level, those officials serving on State and Local Government, Transportation and Safety, Government Operations, Judiciary, Business and Utility, and Criminal Justice Committees were identified for potential participation. These legislators had direct insight into how cybersecurity is viewed within the state, how officials believe it impacts state business, and how it should be integrated into the state and local governments.

The information and insight provided by the lawmakers from the Congressional offices was then to be compared with the information provided by the Governor's office to determine the consistency of the message and vision of the cybersecurity program at the state level. Administrators and field managers at select state agencies (Tennessee Bureau of Investigation (TBI), Tennessee Emergency Management Agency (TEMA), and Safety and Homeland Security) were then targeted for interviews to gain insight into the instructions, missions, and priorities received and how well actions and programs in place match the intended and publicized policies in place. This first set of interviews served as the foundation for the remainder of the inquiry into the county and local behaviors and will be utilized to adjust interview questions and directions, as needed.

After completing the state-level interviews and data analysis, the inquiry shifted to the lower levels government and emergency managers in the four targeted counties. County mayors, county information officers, economic and development officers, and county-level emergency coordinators were contacted for interviews. These interviews shed light on the level of engagement with cybersecurity in the counties, ascertain how well the county's programs and policies align with the state, and investigated whether the emergency and field operating managers saw implementation in line with established policies and procedures, or disconnected. The inquiry also sought opinions and experiences that could correct areas that operate differently on the ground than the original or established concept, identify resources needed to implement changes, and/or identify gaps between existing and needed policies. At the local level, mayors, city information officers, city administrators, subject matter experts, and emergency managers comprised the last set of interviews requested. These interviews followed along the same path as those with the county described above, with the collected data providing a comprehensive view of cybersecurity policy at the state level and across the county and city levels in the targeted Middle Tennessee area.

The overall population identified for the study consisted of 100 individuals spread between Congressional seats and state, county, and city officials and emergency managers. This population represented elected and appointed officials from the federal to local levels in the target area, along with associated emergency managers, subject matter experts, and supporting practitioners that oversee cybersecurity operations in their assigned territories. I sent invitations to participate in the study to the offices for each of the potential participants, with a target response and participation rate of around 25% for the local and state locations and half of the counties. Sampling was not used for the target population prior to receiving commitments. If a significantly higher number of participants elected to participate than anticipated, a filter would be applied to balance the participants by levels of government and geographic location within the selected area.

The number of interviews required for a meaningful and valid study is not based on a mathematical formula but achieving saturation with the data. Collecting enough data to reach saturation is essential for the validity and replicability of the study. Saturation in qualitative research, particularly in one including interviews like this study, occurs when no new data is collected from additional participants, despite interviewees answering the same questions regarding the subject matter. Throughout the course of the data collection and analysis, additional interviews would be sought if either data saturation was not reached with the original interviewees or if alternate subject matter experts or critical stakeholders were identified in the process that were not included in the study (Fusch & Ness, 2015).

Selection of participant agencies for the proposed study focused on the elected and appointed officials in Middle Tennessee concerned with cybersecurity. I identified potential state Congressional participants based on their membership on committees that dealt with cybersecurity most directly. The same logic went into the selection of state agencies, with those coordinating with federal cybersecurity assets and addressing state issues chosen for the study. Geographic constraints on the area of the study constrained the potential participants at the county and city levels. Representatives from the four counties and nine major city governments in the region were contacted to participate in the study as each location has the potential to add unique perspective to the study. Smaller towns scattered throughout the geographical area were not included in the initial request for participation, as most of these locations rely on the surrounding counties for much of their infrastructure (fire and police protection, water treatment and waste collection, emergency response, et cetera).

I e-mailed the initial cooperation request letters to the appropriate clerk for each agency or congressional office. Upon receipt of letters of cooperation and approval from IRB to conduct the study, additional communications followed, including e-mail, phone calls, and face to face meetings. Different offices or agencies had additional protocols or permissions required, so process and procedures differed slightly depending on individual requirements. As noted previously, analysis took place as data collection occurred, allowing identification of emerging trends or stakeholders not captured in the original participant pool. Due the rural/suburban/urban mix within the geographic area, care was also be taken to incorporate participants from each category as well as the different levels of government. Saturation for the study occurred when subsequent interviews from an area return the same results or participants in each of the required categories were incorporated in the results, along with any emergent stakeholders.

Instrumentation

The primary focus of this study was to determine whether federal cybersecurity policies and procedures provide adequate guidance, resources, and oversight for state and local policies and agencies, especially within Middle Tennessee. Of interest was the level of engagement the state officials have with this area and how important or relevant they considered it to the governance of their state and location. Along with gauging the level of interest and engagement, it was also necessary to determine if federal policies and programs provide requisite resources and authority to carry out a cybersecurity program below the federal level. Most of the interview questions focused on these issues, working to define the operational environment for cybersecurity in Middle Tennessee. The secondary focus of the proposed study was whether the current policies and programs currently in place are being implemented properly in the field. To that end, part of the interview questions inquired about the level of engagement of each participant with cybersecurity operations. Those with firsthand knowledge were asked to compare the intent and published policies with the reality of the mission and focus of the operational units on the ground.

The instrumentation for the proposed study included use of a digital audio recording device for face to face interviews. The intent was to conduct face to face interviews with each of the participants using the digital audio device for transcription recordings. If there are willing participants that cannot conduct face to face interviews, Skype and telephonic options will also be offered to collect the data. As an option of last resort, the interview protocol (shown in Appendix D) was able set up in Survey Monkey for participants to complete asynchronously. I developed the data collection instrument to be used in the study based on the research questions. At the outset of the data collection process, the interviews were the primary source of information. Policy documents, guidance, and directives for emergency departments and other legislative committees were also utilized where they contributed to the study, as well.

With a researcher-created data collection instrument, a pilot study was needed to test the instrument. The pilot study was performed with a subject matter expert working in cybersecurity. This individual had similar knowledge and experience as the other individuals targeted for participation and will demonstrate whether questions need to be modified, removed, or additional added to gain insight. Feedback and commentary were also sought on the areas of potential bias, subject knowledge, and applicability to location-specific resources.

Procedures for Recruitment, Participation, and Data Collection

The data collection was conducted at the offices of each of the participants that volunteer for the study, or at an alternate location of their choosing. This included government buildings in the different counties, coffee shops, and other locations the participants deemed favorable. These included the state Capitol, County Seats, and city halls for the locations listed in Appendix C. Interviews were also conducted via telephone and through Survey Monkey. The procedures for participant selection, data collection, and data analysis follow. These will occur in separate phases: study development, recruitment, data collection, and analysis stages.

In the study development stage, I sent letters of cooperation out to the offices of the participants listed in Appendix C via e-mail. For the federal Congressional officials, letters were sent to their individual offices. State Congressional contact was made through the Office of the Clerk for both the Senate and the House for the initial cooperation. County and local official contacts went through their respective offices in their geographic locations. With e-mail serving as the primary method of contact for this initial contact, follow up communication followed two weeks after the initial e-mail for any office without a response. Based on the nature of the responses (positive and negative), the need for expansion of the study or participant population was examined six weeks after the initial contact e-mail. To assist in the cooperation process, I also contacted community partners to assist with introductions to potential participants. The next steps in the development process was completing the Walden IRB process. Once IRB approval was obtained, I conducted my pilot survey, examined the results, and moved on to recruitment. Next was the recruitment stage, where I reached out to the individual participants identified to gauge their interest. Interviews were then scheduled with the participants using their preferred method (face to face, telephone, Skype, or Survey Monkey).

The data collection stage of the study commenced with the first scheduled interview. Before each interview began, the participant received a copy of the Informed Consent form to sign for the interview, and a copy of the interview protocol. The interview opened with standard opening comments that provided an explanation of how the interview will run, the type and scope of the questions, and reminding each participant they were not obligated to answer any questions and that I would record the interview with their permission. Within a week after the interview each participant was provided with a copy of the transcription of the interview to verify for completeness and accuracy. The participants were given a week from receipt to make changes to the transcript before the data is coded for analysis. A lack of response after a week was taken as acceptance of the provided transcription, a fact that will also be explained during the interview process.

The interview protocol (shown in Appendix D) was designed utilizing McCracken’s questionnaire construction guidelines from *The Lone Interview*

(McCracken, 1988, pp. 34-38), and began by thanking the interviewee for their time and participation in the study. The structure of the interview was provided, along with topics of the different sets of questions. The participant was reminded that all responses are voluntary and they may choose not to answer any question or come back to a question later in the interview, if desired. Participants were also reminded that all responses are confidential and no identifying information would be included in the results of the study. The first set of questions served to establish the participant's background, expertise, and current role and responsibilities. Participants were asked to provide a brief synopsis of their professional and educational background, along with their time in current position and the primary responsibilities of that role. Next, each was asked about what issues are of greatest import to citizens, businesses, and special interest groups in their districts, as well as the issues of greatest concern among their peers (other legislators, mayors, emergency managers, et cetera). The final two questions in the opening section sought insight into the participant's comfort level with cybersecurity from both policy and technical perspectives and if the participant had any areas they wish to incorporate into the interview.

The main research question for the study asked if U.S. cybersecurity policy at the federal level provides enough guidance and resources for state and local governments and agencies to enact and implement cybersecurity policy. The data collection instrument contained eight questions designed to gain insight into legislative priorities in the targeted area and the current policy environment around cybersecurity. The first question asked the participant about what drives legislative priorities from year to year. Next, interviewees were asked to provide examples of issues that rose from either not on the legislative agenda or of marginal importance to a major issue during a session in the last decade. Taken together, these two questions provided insight into how lawmakers establish priorities, set their agendas, and the types of issues important enough to create a large enough consensus or grassroots support to demand immediate attention. Next, participants were asked their opinion on the responsibilities of the various levels of government with respect to cybersecurity. Question four asked which of the federal cybersecurity policies and procedures are most relevant and applicable to the policy environment at the state level in Tennessee.

The next question in this section asked how cybersecurity is viewed by the participant's peer group: as a need at the state level, a federal issue, or mixed, and if the opinions are divided, what is the composition of the opposing groups? Under this question, there were three additional inquiries regarding special interest groups and stakeholders in the cybersecurity discussion. These asked the participant to describe the belief structure and resources of the interest groups and stakeholders along with their preferred methodology. Participants were also asked how effective the special interest groups are at influencing opinions, topics of discussion, and decisions regarding their preferred interests. Question six asked what the main influences are for cybersecurity policies and procedures. Question seven inquired about how cybersecurity considerations have impacted emergency preparedness and planning at their level. The last question in this section asked the participant to define changes over the course of the last decade regarding cybersecurity: attributes of the problem, fundamental social values and structure, basic constitutional structure and laws, socioeconomic reform, systemic governing coalition, degree of consensus needed for policy change, overlapping societal cleavages, and general direction and focus of policy.

The second research question the study addressed is: how well aligned are current cybersecurity program implementation with the established policies and vision that created them? To address this inquiry, there were seven questions for each participant to answer in the second set of interview questions. The first question asked the participant to provide an overview of how cybersecurity is accounted for in policy and planning for the participant’s district. Question two asked about the major constraints and limitations for emergency planning and operations around cybersecurity. The third requested details about the authority and resources provided for the lower levels of government by higher government regarding cybersecurity. Question four asked about the clarity of the organization’s cybersecurity mission, focus, and goals and requests the participant provide an overview of each along with an explanation of how each is measured. Next, participants were asked if their agencies can fully accomplish their missions and objectives assigned with their current resources and authority. If a negative response was given, a follow-up question inquired what resources are needed to bridge the gap between current operations and the ability to meet expected standards. Question six asked the participant to compare the structure of their organization and operations in the field to the original vision and charter for the agency. The final question asked the participant to provide their opinion on how to address any issues regarding disconnects in mission creep, conflicting directives, implementation of policy, or lack of resources.

At the close of the interview the interviewee was thanked once again for their time and participation in the study. At this time, they were given the opportunity to revisit any topic they wish to provide any additional insight for or to provide information for topics not covered by the interview. I also reminded the participants they will receive a copy of the transcript within seven days for their review and editing. This process continued until all of the interviews are complete.

Data Analysis Plan

In the analysis stage of the study began after the transcript was reviewed and returned by the participant, or after a week with no response by the participant. The analysis stage followed each data collection stage for the individual interview, but the coding and initial analysis occurred either before or during the period that other interviews took place. This process, as noted previously, helped identify emerging patterns or items that need to be addressed or incorporated into future interviews. In this stage, the digital recordings taken during the interviews (or responses if Survey Monkey was utilized) were converted into an electronic transcript and then analyzed using qualitative software. Once the electronic transcripts were complete, they were coded and entered into Atlas.ti to analyze the data, trends, and patterns identified and discussed. Atlas.ti is a qualitative research program that assists researchers in organizing and analyzing large amounts of data across multiple media types. Atlas allows for systematic coding, linking of topics and ideas, visualization and other tools to better understand the collected data (Altas.ti, n.d.).

For the data analysis, I utilized McCracken's five-step process. This five-step process is part of a larger narrative McCracken wrote on the use of the long interview as a tool of qualitative research. McCracken utilized extended interviews of up to six hours (broken up into two- or three-hour segments) as an exploratory instrument. The five-step analytic process described by McCracken is one element of his four-step method of inquiry. The first step is the review of analytic categories and interview design, the second is the review of cultural categories and interview design, the third stage involves the discovery of cultural categories and the creation of the questionnaire and interview procedure, and the last includes discovery of analytic categories, analysis, and the write up (McCracken, p. 32-38).

The first step in this analysis process starts with identification of each useful utterance within the individual transcript. At this point, each of these observations will be considered on its own without relating it to other observations or other transcripts. This stage of analysis, per McCracken, is designed to determine if the utterances identified in the transcript can shed light on the underlying thought processes that led to its inclusion in the interview. The investigator utilizes themselves as an instrument of analysis during this stage, not just a collector of data from the participant. The investigator, per McCracken, should pay attention to not only what is included in the data from the interview, but also what context cues and additional information the data conjures for the investigator (McCracken, 1988, p. 32-34).

The second stage of the analysis takes the initial observations from the first stage and expands the analysis over a wider swath of the transcript to further develop relationships, both positive and negative. This stage has three levels within itself, first, the utterances by themselves, secondly with the transcript, and finally, based on the literature and policy review. In the third stage of analysis, the focus should now be the individual pieces of text specific ideas are lifted from and less the entire transcript. During this stage of analysis general themes and patterns are identified, along with general constraints and characteristics of the data (McCracken, p. 35).

The fourth stage in McCracken's analysis process is a major step in narrowing the focus of the analysis by eliminating redundant or repetitive theories or themes. During this stage, the most significant and robust themes are elevated and all residual themes set aside and categorized. At this point, it is imperative to ensure that these residual or seemingly less important themes or theories do not conflict with or contradict any of the main themes or theories. Once any conflicts are resolved and the remaining themes and trends are ordered, analysis moves into the final stage. In stage five, the responses and views of the interviews are combined to form larger, system-level theses not reliant on individual perspectives, but built on general observations and trends (McCracken, p. 35-36).

Issues of Trustworthiness

To validate the quality and trustworthiness of qualitative research, there are four tests typically used: construct validity, internal validity, external validity, and reliability. Construct validity for case study research utilizes multiple sources of evidence, establishes a chain of evidence, or incorporates a review of the report draft by critical participants (Yin, p. 45). The study relied primarily upon interviews for data collection, but also requested relevant and supporting documents from participants, as well. Bringing in multiple sources of data can assist with either corroborating the information provided by the participants during the interviews or providing possible points of departure to investigate (Yin, p. 107-110). With much of the data collection centering on legislators, public use files and organizational records from committee meetings and legislative sessions was examined for specific time periods or events discussed by participants during the interviews. For participants working in other agencies, similar information was sought depending on recording standards and availability.

For internal validity, typical case study tactics include pattern matching, explanation building, addressing rival explanations, and using logic models (Yin, p. 45). For the proposed study, I expended the most effort examining rival explanations for the data. Per Yin, the more rival explanations and conflicting interpretations of the data considered and rejected within the analysis, the better quality the results will be (Yin, p. 142). For the external validity, the theory embedded in the design of the case study served as the basis for analytical generalization of the study as the data is analyzed and findings are incorporated. The reliability of the study stemmed from documentation, construction of the data collection instrument, and use of accepted strategies by the researcher. The structure and evolution of the instrument was provided in the previous section, along with documentation and analytical strategies to be used throughout the study. The study is entirely replicable by subsequent researchers using the information and instrumentation provided.

Ethical Procedures

The recruitment process began by e-mailing an invitation to participate to the office of the prospective participants. This initial document outlined the proposed study and provided the initial opportunity for the individual to choose whether or not to participate. Participants had multiple opportunities to select their level of participation and engagement at several steps before the interview begin. As noted previously, each interviewee was advised during the data collection process that they have the option the decline to answer any question during the session or skip a question and return to it later if desired. Considering the target pool and measures taken, there was no known risk to the participants of the study.

Each agency and organization taking part in the study was contacted to ascertain if they have additional IRB requirements beyond that required for Walden University. During the data collection process, each participant was provided with a detailed explanation of their role in the interview process and asked to sign a consent form prior to beginning the interview. The participants received a copy of their consent form, along with a copy of the interview protocol at the outset of the session. Participant confidentiality was maintained and protected for all aspects of the proposed study, as only I have access to notes, recordings, and other materials associated with the data collection and analysis. Additionally, when not in use all materials remain secured in my home office. All digital materials were downloaded to and stored on my personal laptop, which is password-protected and secured in my home office when not in use.

Summary

A qualitative case study methodology was selected for the proposed study to collect and analyze data from elected and appointed officials and emergency managers in Middle Tennessee. Concerns about bias and research quality were mitigated through instrument construction, awareness of the researcher's place in collection and analysis, use of multiple sources of evidence, and addressing rival or conflicting explanations within the data. Confidentiality concerns were addressed by removing all identifying information about the participants and their organizations from the data after the transcript is confirmed by the participant. Data and materials collected for the study were stored according to requirements provided by Walden University to protect participants and maintain ethical handling of the material. Coding and analysis of the data followed McCracken's five-step analytic process, which took place in an iterative manner following each interview once the transcript was approved. This process allowed following interviews to incorporate emerging trends or concepts as needed. The next chapter will address the data collection, analysis, provide evidence of trustworthiness, and discuss results of the collection.

Chapter 4: Results

Introduction

In this chapter, I will review the data collected for the study and present the results derived from analysis of that data. The primary purpose of the study was to understand how federal cybersecurity policies, procedures, and guidance impact the cybersecurity operations at the state and local level, specifically in relation to the State of Tennessee and local governments in its midstate area. In this chapter I will also explain the pilot study, setting and demographics, data collection and analysis methods, and evidence of trustworthiness.

I sought to answer two research questions: first, whether the current cybersecurity policy at the federal level provides sufficient guidance and tools for the State of Tennessee, along with count and municipal governments in the midstate area, and, second, whether the current implementation of cybersecurity policies and programs match with the expectations and vision of the original plans that put them in place. In the first part of this chapter, I will provide information on the pilot study developed to validate the interview protocol created for this study. I will then discuss the environment surrounding the study, including emergent events relevant to the study and demographics of the target area. Other information framing the study, including evidence of trustworthiness and characteristics related to the study and data collection, will follow. The chapter concludes with the results of the study, a discussion of their relevance to the research questions, and a summary.

Pilot Study

I received Walden University IRB approval to begin collecting the data for this study on December 8, 2017. The original approval number for this study was: 2017.12.08.1:44:26-06’00’. I conducted the pilot study on December 21, 2017, using the proposed interview protocol and with an individual having both extensive information technology and cybersecurity experience, in addition to decades of work in both the public and private sectors. Based on the responses received from the pilot study and feedback on the setup of the study, I determined that the survey covered all of the elements in the research questions and elected not to alter the interview protocol.

Performing the pilot study provided a number of benefits prior to the start of data collection and analysis. First and foremost, it provided an outside perspective on the interview protocol and allowed me to determine efficacy and fit for the study. With the results of the pilot study, I was also afforded an opportunity to test data collection methods, transcription, and coding protocols. The individual selected for the pilot study was outside the geographic area for the study and not currently serving as an elected or appointed official, nor was the person serving as a subject matter expert for the public sector. The results of the pilot study were not included in the study. Using these results did, however, allow me to enter data into the Atlas.ti program, perform code analysis, and verify that the preliminary coding structure developed was also relevant and capable of capturing relevant aspects of the responses.

Setting

Throughout 2018 and in the first three months of 2019, as I conducted the data collection, several high-profile attacks, new policies and procedures in the United States, and some international cybersecurity events occurred that could have influenced participants. In examining data from the online reference site Hackmageddon.com, I noted 1,749 successful cyberattacks in the 15-month period encompassed by the data collection cycle, or approximately 117 per month. Of those attacks, 209, or approximately 14 per month, took place within the United States. Finally, of the 209 attacks taking place in the 15-month window, 89, or approximately six per month, were targeted against government agencies or facilities (Passeri, 2019). A report published by Symantec for 2018 noted that one in 10 URLs (uniform resource locators) was malicious, that malicious e-mail had been sent to an increased percentage of users during 2017, that the percentage of malicious e-mail containing Microsoft Office documents jumped from 5% in 2017 to almost 50% in 2018, and that employees with smaller agencies and organizations were targeted more than those at larger institutions (Symantec, 2019). Symantec also noted that the company alone blocked over 1.3 million web attacks per day by the end of 2018, blocking almost 350 million web attacks throughout the year (Symantec, 2019). The number of web attacks was up 56% in 2018 compared to 2017 (Symantec, 2019). The number of mobile ransomware infections also increased in 2018, by 33% over 2017 (Symantec, 2019). Not all the news was negative, however. Although ransomware infections and attacks increased in mobile devices in 2018, ransomware overall decreased by more than 20% in 2018 (Symantec, 2019). Phishing attacks also declined in 2018, but at a slower rate of 7% compared to 2017 (Symantec, 2019). The number of targeted attacks was also down slightly in 2018, but the largest attack vector remains spear-phishing (Symantec, 2019).

In addition, there were several significant data breaches in the news throughout 2018 and the early part of 2019. One of the largest, with the most news coverage, was the Facebook-Cambridge Analytica data breach. This breach initially derived from a third-party application downloaded by approximately 270,000 Facebook users (Wipersoft, 2019). From that original participant pool, the application gained access, through Facebook's data collection and privacy policies, to the friend lists and other connections of the users on Facebooks network. Facebook had knowledge of the data collection efforts of this application, and others, as far back as 2015, but declined to address the issue or make the information public (Wipersoft, 2019). The story broke on news outlets in 2018, with an estimated final compromise of 87 million users' data (Wipersoft, 2019). Hackers and hacking groups reportedly utilized the data to create profiles of users to determine targeted advertising for a range of products, including political campaigns (Wipersoft, 2019). The U.S. Congress deemed the breach and ensuing scandal significant enough to call Facebook's CEO, Mark Zuckerburg, to testify before Congress. Facebook also reported a second breach in 2018, notifying users and the public that around 30 million user accounts were compromised through a security vulnerability (Wipersoft, 2019).

Other large data breaches in 2018 and early 2019 included the Google+ data breach and closure. There was a discrepancy in the reporting of the breach by Google and in the news. Google, in 2018, stated that over 400 applications had an existing vulnerability, but that user data was not compromised, but instead immediately patched. Multiple sources reported, however, that user data was exposed as early as 2015 by this breach. A second data breach was announced by Google in December of 2018 that included more than 53 million users. Google announced the termination of this service as of August 2019 after the first breach. After the second, the service termination was advanced to April of 2019. Other major data breaches from 2018 include the Under Armor MyFitnessPal breach, which released data from over 150 million users, a Marriott hotels breach impacting data for over 500 million users, and a breach at the genealogy site MyHeritage that leaked data for over 92 million users (Wipersoft, 2019).

As previously noted, the public sector experienced scores of cyberattacks in 2018 and the early part of 2019. At least 89 attacks were categorized as targeting public agencies or organizations during this time period (Passeri, 2019). These data breaches and cyberattacks occurred across a wide range of targets in the public sector, including: candidates running for office, Republican and Democratic National Committees, Senate and Congressional sites and accounts, individual Representatives and Senators, the Department of Defense, individual branches and its contractors, State and Treasury Departments, the website for the Affordable Care Act, and agencies at the state, local, territorial, and tribal levels. These attacks ranged in impact from minor disruptions, such as changing verbiage on Department of Transportation signs, short-term disruptions in service on websites and/or services provided, to massive, including: widespread data compromise, leak of personally identifiable information, theft of classified and sensitive materials, significant disruption of government services, and ransomware attacks (Passeri, 2019).

Agency impact and response was mixed during this time period. Some locations and agencies felt it was more important to keep services up and running and paid the ransom demanded by attackers. Others refused and dealt with the loss of their data and the resulting impact to services and its related toll on the public. While the average ransomware ransom in 2018 increased to approximately $1,077, that figure includes individuals and small businesses (Dobran, 2019). When ransom demands are sent to government agencies and larger corporations, the demands can go significantly higher. A ransomware attack in 2017 requested $250,000 (unpaid) in bitcoin from the City of Spring Hill, Tennessee, a city with approximately 40,000 residents (Ervin, 2017). Spring Hill lost access to some of their data permanently, residents could not use electronic payments for over a month, and the city was forced to recreate the utility billing system and others using manual data entry. The estimated recovery cost for this attack currently tallies over $100,000, not including remediation efforts for risks going forward (Graciela, 2018). Hancock Health, a hospital based in Indiana, paid out $55,000 to restore their systems after a ransomware attack in early 2018, despite having security and backups in place. This decision was made based on the estimated timetable to restore their systems utilizing the backups. Administrators estimated it would take several days, if not weeks, to fully restore the data. In the aftermath of the attack, the hospital reverted to pen and paper for records keeping, further impacting its efficiency and operations (Osborne, 2018).

Some ransom demands in 2018 and the first quarter of 2019 were small and more manageable, including the City of West Haven, Connecticut, which had 23 systems locked by ransomware and elected to pay $2,000 in Bitcoin to restore service (Dillane, 2018). On the other side of the scale, Jackson County, Georgia suffered a ransomware attack and paid the $400,000 ransom demanded by the hackers to restore their files. This attack came a year after the city of Atlanta fell victim to a ransomware attack (Padgett, 2019). The attackers on Atlanta requested $50,000 in ransom, which the city refused to pay. This attack impacted not only the city of Atlanta computers, but had also potentially exposed those that conducted business with the city, as well (Blinder & Perloth, 2018). The total for Atlanta's recovery efforts is expected to be between $2-3 million dollars in direct costs for the city and could cost the taxpayers of Atlanta as much as $17 million (Deere, 2018). A cross-section of attacks over the fifteen-month period include shutting down the Massachusetts public defender system for weeks, and significant disruptions resulting from attacks on the Colorado Department of Transportation, the city of Sammamish, Washington, the city of Matanuska-Susitna in Alaska, Del Rio, Texas, and many others (Passeri, 2019). A potentially devastating, but narrowly avoided, cyber-attack of the year was against Harris County, Texas. This attack was a phishing attack by a supposed contractor working on a project for the county, where the county initially transferred almost $900,000 to the contractor. The agency reached out to the company that supposedly e-mailed them for clarification, but found the transfer instead went to hackers and the e-mail was a phishing attack. The money was recovered, but the attack made headlines across the country and demonstrated potential threats and costs (Zaveri, 2018). The State of Tennessee was not immune from these attacks during the period in question, either. Knox County's website was impaired by a distributed denial of service attack on election night in 2018, preventing the county from reporting election results for a period of several hours (Whetstone, 2018). Columbia State Community College in Tennessee was also forced to shutter operations for two days in the first part of 2018 due to a cyber-attack (Malafronte, 2019).

In the public sector during 2018, legislative changes regarding cybersecurity occurred across the country. During this period at the state level, at least 35 states, Puerto Rico and the District of Columbia introduced or considered more than 260 bills related to cybersecurity, with 52 bills enacted in 22 states. The primary areas for legislative activity during 2018 were: "Improving government security practices, providing funding for cybersecurity programs and initiatives, restricting public disclosure of sensitive government cybersecurity information, [and] promoting workforce, training, economic development" (National Conference of State Legislatures, 2019 (1)).

In Tennessee, this included one bill in the House and one in the Senate considered but not enacted, both bills requiring "the coordinator of elections to engage a cybersecurity firm to perform a study of the voter data system in this state and produce a report that details the risk to voter data posed by hacking" (National Conference of State Legislatures, 2019).

In 2019, more than three dozen states have introduced more than 150 pieces of legislation through the first four months of the year. The key areas thus far are improving government security practices, addressing the security of connected devices, relating to cybersecurity insurance or standards for insurance data and information security, addressing elections security, [and] creating cybersecurity commissions, task forces or studies. To this point in 2019, the State of Tennessee has not introduced any new legislation related to cybersecurity (National Conference of State Legislatures, 2019 (2)).

At the U.S federal level, there were also several changes in the last fifteen months. One area was the release of the United States' National Cyber Strategy, released in September 2018. This strategy outlined cyber policy and strategy for the first time in a decade and a half. Included in their strategy was a path forward, including:

> Defend the homeland by protecting networks, systems, functions, and data, promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation, preserve peace and security by strengthening the ability of the United States — in concert with allies and partners — to deter and, if necessary, punish those who use cyber tools for malicious purposes; and expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet (National Cyber Strategy, 2018).

In the federal arena, the Trump administration also oversaw the creation of the Cybersecurity and Infrastructure Protection Agency (CISA). CISA Director Krebs noted:

> The CISA Act elevates the cybersecurity mission within DHS and streamlines our operations to better secure the nation's critical infrastructure and cyber platforms," said CISA Director Christopher Krebs. "CISA continues NPPD's mission of leading the national effort to improve critical infrastructure security, coordinating the protection of the federal government's networks and physical

> infrastructure, and helping entities in the public and private sectors manage risk (Homeland Security Today, 2018).

This agency adds to the national defense posture and seeks to reach out to public and private partner to improve the cyber posture across the United States. This agency also works to coordinate and consolidate public and private responses to cyberattacks (Department of Homeland Security, 2018).

In the international arena, there were two significant cyber events during the targeted time period: implementation of the General Data Protection Regulation (GDPR) and the United Nations Educational, Scientific, and Cultural Organization's (UNESCO's) Internet Governance Forum (IGF). The GDPR is the result of years of planning, preparation, and debate across the European Union. The regulation was adopted on April 14, 2016 but was not enforced until May 25, 2018. This regulation sets forth data privacy laws for the European Union and replaces the previous privacy framework. The GDPR has three objectives:

1. This Regulation lays down rules relating to the protection of natural persons regarding the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons

> regarding the processing of personal data (Regulation 2016/679 of the European Parliament).

Under the terms for this agreement, citizens of the European Union (and those doing business with the EU) saw five significant changes in data protection. The first was a more clear and concise language for data privacy standards. Prior to this regulation, data privacy and collection efforts could be hidden behind complex legal documentation and language. Going forward, these policies and procedures are required to be in a clear and concise language so users can understand them. The next section requires affirmative consent from the users before data can be utilized by an organization. This closes gaps where silence or a lack of negative response from the user or consumer was previously taken for consent. Users also gained additional transparency into how their data is used by companies. Previously, users might not be aware whether their information was shared outside of the EU, how the data is used after it is collected, or whether certain actions and decisions are made using Artificial Intelligence or algorithms. Going forward, companies are required to provide clear information on data transfers, explain why data is being collected and for what purpose, and inform users which decisions are automated and provide an avenue to dispute them. The GDPR also provided for additional rights for the users. Previously, users may or may not know when a data breach occurred and their data was exposed, could have difficulties transferring data from one company to another, obtaining a copy of the information companies collected, or having their data deleted entirely. The new GDPR requires businesses to inform users when breaches occur, allow users to move or request data, and a right to have files deleted. The last provision provides for stronger enforcement. The previous regulation allowed for minimal means of redress, but the GDPR established a Data Protection Board that can adopt binding decisions and impose fines against businesses not adhering to the regulation (European Commission, 2018).

The other major international cyber event in 2018 was the Internet Governance Forum. The 2018 IGF was the thirteenth annual meeting of the Forum, and it was a part of France's 'Paris Digital Week' in November of 2018 that also saw the Paris Peace Forum and a Government Technology (GovTech) Summit. On November 12, 2018, French President Emmanuel Macron announced the Paris Call for Trust and Security in Cyberspace. "This high-level declaration in favor of the development of common principles for securing cyberspace has already received the backing of 547 official supporters: 65 States, 138 international and civil society organizations, and 344 entities of the private sector" (Paris Call, 2018).

The United States is not currently a signatory of the Paris Call, but many U.S. companies and interests signed. These companies and agencies declared support of the call and developing better policies and procedures to work together to improve safety and security of cyberspace. This call acknowledged and outlined many of the challenges facing the world at large regarding cyberspace, and called for increased collaboration between governments, private sector, and civil society to develop new standards, policies, procedures, and best practices to improve safety and security moving forward (Paris Call, 2018).

Demographics

In developing this study, I decided against relying on a partner organization to serve as an intermediary. This decision was driven by the disparate organizations and locations of the targeted participants. I felt that no single organization would be able to provide access across all levels of government and in desired locations, so direct contact with each of the individuals would yield better results. I sent the initial contact e-mails (see Appendix F) to elected officials at the federal level (senators and representatives from Tennessee) the same week I set up the pilot study. This included 11 potential interview targets. At the same time, I sent initial contact e-mails to elected and appointed officials at the state and county levels in Tennessee and the initial target area. This batch of e-mails included 65 potential targets. I targeted specific individuals based on their positions in certain agencies and committees in each house of the Legislature (and joint committees). The last set of e-mails went to officials at the city/town level in the target area and included an additional 24 potential participants. Altogether, 100 individuals were identified for potential interviews. At the outset of the study, and in my proposal defense, the expectation was that I would conduct a significant number of interviews, as I intended to interview every person who elected to take part in the study.

Approximately two weeks sending the original e-mails to potential participants, I sent a follow-up e-mail (see Appendix G). The follow-up e-mail generated the first responses to my requests for interviews, including several declinations and five individuals interested to participate. I subsequently sent additional communications to the interested individuals to obtain informed consent and schedule interviews. I received the first informed consent for the study on January 9, 2018 and conducted the first interview on February 6, 2018. The final e-mails (see Appendix H) were sent to the targeted participants 2 weeks after the second e-mail. Based on the study design, a lack of contact from the targeted participants at this point indicated a lack of interest.

Data Collection

During the data collection process, two obstacles added significant delays and barriers to success. The first involved getting potential participants to buy in to the study and its relevance to their respective levels of government and day-to-day operations. This was a challenge as multiple officials in smaller jurisdictions declined to take part in the study as they felt upper level governments could better answer the questions posed. Some officials replied that cybersecurity was not an issue they felt qualified to speak about and felt they could not offer value to the study. Part of the intent of this study was to gauge the level of engagement and understanding of cybersecurity issues across multiple levels of government. Interviews with individuals in position as elected or appointed officials, no matter their experience level or knowledge of cyber operations, or lack thereof, help to answer that question. The other major challenge was finalizing interview scheduling after potential participants agreed to take part in the study. Approximately a dozen participants expressed interest in taking part in the study but either changed their minds or stopped communicating altogether. With the study focusing on elected and appointed officials and practitioners working for the state, the time commitment to participate in the study was also an issue for several potential participants. Six individuals noted they would like to contribute to the study but did not have enough time to schedule. Alternative options were provided aside from the face-to-face interview (telephone and Survey Monkey) to try and solicit more participation, but those individuals still declined.

Due to the nature of the officials in the participant pool, there were no additional IRB requirements for this study beyond that required by Walden University. I submitted my initial IRB application on November 27, 2017 and received IRB approval to begin data collection on December 8, 2017. I submitted a continuing review to the IRB and a request to add two counties to my original three on November 23, 2018. The IRB approved the continuation of the study and the change in counties covered on January 8, 2019.

Interviews were conducted and data collected between February 6, 2018 and March 7, 2019. Of the interviews, two were conducted face-to-face, one over the telephone, and two more submitted using a SurveyMonkey survey. The 5 interviews conducted represent 5% of the targeted population for this study. There were 18 other individuals that initially expressed interest that did not complete the process. An additional dozen individuals were willing to speak with me in an informal capacity but declined to participate due to a range of factors, politics, confidentiality, and lack of technical expertise chief among them. The face-to-face interviews took place in one participant's place of employment and one was in a coffee house per the request of the participant. Voice recording was done for one of the face-to-face interviews, with the permission of the participant. This recording made transcription easier and ensured I did not miss any relevant data. I recorded data for the other face-to-face interview and the telephonic interview with notes. After I conducted each of the live interviews, I transcribed the data collected and provided a copy for the participants to review for accuracy. I did not receive any secondary documentation from any of the participants, but one participant returned the transcript with additional notes and clarifications. In order to maintain confidentiality, participants were assigned numbers 1-5, and those numbers were utilized during the transcription and coding periods. Participants in the study hold positions in Tennessee from the local to the state level and include practitioners that work with the state and public officials at multiple levels.

Data Analysis

As discussed in Chapter 3, I analyzed the data using McCracken's five-step process. This process begins with identifying each so called 'useful utterance' in the individual transcript. At this point in the process, these key words or phrases in the interview may help provide insight into the motivation of the participant to include them in the interview. According to McCracken, the researcher is not simply retrieving or collecting data in this step, but they should also seek to identify contextual references and other information that can be gleaned from the interview. In the second stage of analysis, the observations from the initial analysis step are expanded upon to determine positive and negative relationships among the data and utterances. The second step encompasses three levels: looking at the utterances individually, looking at the utterances in the context of the transcript itself, and finally, looking at the initial observations through the lens of policy and literature review (McCracken, 1988, p. 32-35).

The third stage of analysis focuses on ideas and the specific sections of text where they originate. This phase of the analysis process seeks to develop overall themes, patterns, constraints, and characteristics of the data. The fourth stage of analysis winnows out the minor and residual themes in the transcript and elevates those more significant. While working on this stage, it is imperative to check that the apparently less important or relevant themes are not at odds with the major themes. If a conflict exists, it must be resolved before moving on to the final stage of analysis. The last step in this stage is to order the themes in order of importance and relevance to the study. The fifth and final stage of data analysis combines the themes, responses, and viewpoints in the interviews to create system-level theses built on general observations and trends and not based on any one individual perspective (McCracken, p. 35-36).

I began the analysis phase of the study using the primary codes in the preliminary coding (see Appendix I) I developed before starting data collection. The primary codes were selected based on expected responses and to create a baseline for initial analysis. Using Atlas.ti software, I coded each interview and identified emerging trends and patterns. Interview questions were coded into cybersecurity and emergency preparedness in the initial pass. This differentiation allowed me to separate responses into separate areas to assist with theme development. The transcripts were coded sequentially as interviews were conducted and all transcripts were examined when all were complete to identify inconsistencies or inaccuracies in the coding. A second coding pass identified areas related to Advocacy Coalition Framework and its components. These codes included references to coalitions and opportunities, constraints, external events, governmental decisions, policy considerations, and stable system parameters. Finally, I went through the transcripts a third time and evaluated them based on recurrent themes as laid out in the tertiary code section (see Appendix J). Taking this tiered approach allowed me to develop themes in a systematic manner and identify other codes needed based on participant responses.

Evidence of Trustworthiness

To bolster credibility of the study, I sought to present all questions in the interview protocol in the same manner with each participant. Some of the questions could be leading, or misleading, depending on phrasing and the nature of the conversation at the time. It was also imperative to remain open to new avenues of inquiry as we progressed through the interview protocol. As I served as the primary instrument for this study, I limited discussions of my personal and professional experience as they relate to Cybersecurity and public policy during the interviews. This assisted in minimizing the bias or framing to guide how participants responded. When participants responded in a manner not anticipated but the preliminary coding, I worked to remain flexible and responsive to those emergent themes and topics. When these situations occurred, I asked follow-up questions to clarify responses and get a better understanding of the participant's perspective and thought processes and to improve confirmability (Creswell, 2013). During the data collection and analysis stages of the research, any information that could be used to identify the participant's position, location, or agency was sanitized and/or generalized for inclusion in the final paper. Within a week following each interview, I sent a copy of the transcript to each participant. The participants were given an opportunity to add or remove information obtained in the interview process. I reminded them at this point the study was voluntary and they did not need a justification to remove or edit responses. Of the participants, one made a few corrections and returned the transcript. The others stated the information contained was accurate and could be included in the study.

One of the hallmarks of a properly designed and executed qualitative study is its ability to be replicated (Peng, 2012). While the study should be reproducible and provide similar outcomes, it can be difficult, if not impossible, to exactly replicate a study, particularly when the study includes interviews. A second researcher or research team can pull from the same population, or a similar population, but the individual dynamics and interpersonal communications can alter responses and data gleaned from the interviews. Barriers in communication, having multiple people present in the interview instead of one-on-one, a change in experience level, and environmental conditions at the time of the interview can all influence the results. If a second study is undertaken with the same population as the previous study, participants may respond differently based on their previous interviews or if they became more engaged in the subject matter after their previous interview. Changes in geographic location and participants can also drastically alter outcomes for interviews. If you conducted the same cybersecurity study utilizing officials in Michigan, Alabama, Research Triangle, or other high-tech corridor, those officials and practitioners would likely be better equipped to provide insight into cybersecurity policies and procedures. The basic outcomes of this study, however, should be transferable to an extent, as they show some of the challenges facing state and local governments in the current policy environment. Other locations may be more engaged or have a larger budget for security and/or training, but they still need to contend with similar issues as the counties chosen for this study in Tennessee. Additional studies across the State of Tennessee should result in outcomes close to this study, as well. The oversight provided by the State is uniform across all 95 counties, the major differences are socioeconomic, funding, and training.

Results by Code

Results in this section will first be discussed according to the coding conducted on the data, then by conceptual framework. Results will generally follow the sequence of questions to provide an understanding of the flow of the interviews and how each participant moved from question to question. In the following section, relevant codes will be reported as they relate to ACF. For each of the topics listed, I will discuss recurring topics, emergent trends, and any data in conflict from one interview to another. For a complete list of the codes, their grouping, and frequency across all interviews, see Appendix J.

Professional and Educational Background, Time in Position, and Role

At the outset of the interview, I asked each participant to provide a brief summary of their time in position, educational, and professional backgrounds. This information helped to frame the conversation, illuminate the qualifications of the participants, and create a more collaborative atmosphere for the interview. The participants hold at least a bachelor’s degree, two a masters, and one a doctorate. They average 20 years of experience in their fields, with a high of 28 years and a low of 12. The participants also average just under four years in their current positions, the most junior with just over a year for the most recent and over a decade for the longest-tenured. One of the earliest and most discussed trends across the interviews was the myriad of hats these individuals wear and the multitude of areas of sole or shared responsibility.

The role of the participants varies depending on the nature of the agency or locality, but the need to simultaneously see to needs across diverse populations is a constant. The participants not only have varying levels of education, but their backgrounds are similarly diverse. Another aspect each of the participants referenced with their roles was working across multiple levels of government. Participants in smaller locations manage their areas while interacting (to a point) with larger locations, counties, and the state. Those in large cities and at the state level are required to be able to work with those larger and smaller agencies and governments, with varying degrees of authority.

Special Interest Areas, Policy, and Constituent Concerns

I then asked participants about the main concerns of their constituents, special interest and policy issues in their community, and the most pressing legislative items at their level. Each of the participants referenced two areas: communication and dealing with multiple issues and concerns of their citizens. All volunteers noted multiple demands for their time and to some extent, conflicting demands on time and resources. One of the most common issues was improving efficiency and reliability while keeping costs and downtime to a minimum. Each participant also touched upon the desire of the public to have greater security and protections against cyberattacks and privacy protections, but also do not want the government to waste money chasing perfect protection or overly complicated systems. Communication between levels of government and government agencies with the general public and smaller population groups is another area of significant concern. Participants noted that some groups and citizens are better at providing communication when they disagree with a direction or would like to see a change. The governments, they noted, could do a better job of communicating back to the constituents of decisions being made, justifications, and broadening transparency.

In the special interest area, responses were mixed. Some participants saw robust special interest working to advance their point of view or preferred practices, while others saw little to no special interest or lobbying activity in their jurisdiction. From a cybersecurity standpoint, vendors seem to drive the special interest groups, setting up meetings and conferences where they can provide demonstrations and offer their goods and services. There were several policy areas participants felt more important than others. These areas of emphasis included: creating policies and procedures to deal with ransomware, cyberattacks, data governance and security, and providing additional resources to lower level governments.

Comfort Level with Cybersecurity, Emergent Issues, and Drivers of Policy

All the participants interviewed for this project felt they were well-versed in cybersecurity, which I expected based on their previously noted experience in the field and position. When asked about emergent issues, participants returned fewer examples than anticipated, noting most areas fall under one of the broad-ranging policies or standard operating procedures already in place. Participants stated that the policies they create to govern their locations are typically sufficiently broad to allow them leeway to address any issues that arise throughout the year. While there may be some unexpected bumps, most of the time emergent issues can be covered or at least addressed with policies and procedures currently in place.

When discussing the main drivers of policy; safety, resources, training and time were referenced by each participant. Participant 5 noted:

> "training, time, and money. Have a plan in place that will take a few years to fully implement. Deal with issues related to continuing requirements, interaction across multiple government levels, and continue to improve security and operations among customer agencies".

Each participant stated education, training, and resources to accomplish everything desired are all lacking to an extent in their organizations. With staffing and funds limited by government budget processes, agencies and localities have to get creative with how they address safety and security concerns, train staff, and hire and retain those with the requisite experience to guard against cyberattacks. The technical expertise is an ongoing issue across the state. Participant 2 noted:

> "Information and technology sharing also consumes a lot of time, pushing information from federal, DHS, and ISAC [Information Sharing and Analysis Center] down to lower levels of government. Some counties across the state have no IT staff. They have Emergency Managers, individuals that run the ambulance services or fire departments and they are told by the administrators that they are also in charge of IT…How do we find the talent and keep them? In some places,

> 60 or 70k to handle IT is good money, on other places, kids straight out of school are making that kind of money, or better. Makes it very hard for counties and small towns to recruit and retain qualified staff. How do you know what training is sufficient?"

Several participants referenced the budget process and not fully understanding who should be on staff or what the recommendations are from higher government levels or seen as appropriate for their agencies.

Responsibilities of Government in Cybersecurity

Next, participants were asked what responsibilities they believed different levels of government hold regarding cybersecurity. Respondents provided a range of responses as to what level is responsible for which actions, but the consensus (supported by established policies) was the federal government has the primary responsibility. While participants noted the federal primacy in the issue, differences arose when participants further discussed roles of government. At levels below the federal government, respondents felt strongly that state and local should all have a hand in securing the networks and improving safety for the entire system. One of the most significant themes arising from this study was the concept of *shared responsibility*. Four out of five respondents used a similar term and the fifth explained the same concept but used different terminology. This concept of shared responsibility manifests itself in several ways. First, the local, county, and state governments and agencies all utilize, at some level, to federal systems. If the lower government networks are compromised or a vulnerability exists, that in turn increases the risk and exposure for the federal networks and everything it touches, as well. Pushing out standards, policies, and procedures is part of a necessary cybersecurity plan, but that is not enough to provide protection.

Once the federal standards are in place and distributed, the respondents felt the state has the responsibility to ensure those standards are met, train users, and protect assets at the state level. The same goes for the county and local governments with federal and any state policies and procedures pushed down to their level. Again, all levels have a piece of securing the data and ensuring training is done and protocols are followed. Participant 3 provided a more detailed answer on the relationship between government levels with respect to cyber:

> “Federal government provides framework, outlines minimum standards, and protects federal resources. State will ensure compliance with federal and state mandates, user security training, and manage and protect state networks. State also provides credentials and access to state resources, provides resiliency and continuity of services and networks, facilitates communication and information sharing across networks and government levels, works to identify potential methods to streamline work and services and ease the burden on state agencies as they work with and answer to federal departments. The state agencies also provide continuous user support, sets policies and procedures at state level, conducts data analytics, provides professional support services, and manages vendors and requirements.”

The participants agreed upon the need for additional actions and the responsibility of the lower-lever governments and agencies, but disagreement remain. Participants had divergent ideas on where best practices, rules, and regulations should originate, and what actions are needed or recommended.

Federal Policies and Procedures Relevant to Tennessee Operations

When participants were asked which federal policies and procedures are most relevant and applicable to the current policy environment in Middle Tennessee, the results and responses differed depending on the agency level. When talking with individuals that operate beneath the state level, participants did not feel that many federal policies and procedures are relevant to their operations. At the local and county level, managers typically create their own protocols and come up with mitigation, remediation, and security standards for their organizations. The policies and procedures for the state and federal governments only come into play when lower level governments access their systems. Depending on the networks, certification or clearance may be required to access some systems, requiring lower level governments to maintain them for necessary employees.

Participants that work at the state level provided a range of federal policies and procedures that are relevant to their operations and environment. Participant 2 noted "multiple areas come into play, including FISMA, information sharing, user training, federal audits, and others." Participant 3 discussed FISMA and NIST standards that derive from the federal level. Participant 3 also noted that the federal government has a range of monitoring and information programs, but believed the information pushed can overwhelm lower level governments that may not understand how to utilize the information or translate it, so it is relevant for their agencies or operations. The concept of ‘shared responsibility’ was also mentioned regarding the federal policies and procedures. Weaknesses at the lower levels increase risk for upper levels of government. It makes sense, then, for upper level governments to push information, tools, and resources to lower levels to improve the system. However, based on insight, there appears to be a disconnect between levels of government. Much of the information provided from higher to lower is not actionable or is not provided to the appropriate people to act upon it. This renders much of the shared information irrelevant and can lead to additional workloads on staff to attempt to translate to their agencies.

View of Cybersecurity by Peers and Legislators

When I queried the participants about how cybersecurity is viewed by their peer group and legislators in their area, several strong trends emerged. First, all participants felt cybersecurity is not well understood by legislators. Participant 5 summed up the feelings of the group, noting “I don't think cybersecurity is viewed consistently because our legislators doesn't understand it. For the most part, I'm sure they have a concept of what cybersecurity is, but they don't fully understand what that means to them”. The issue of legislators struggling with the importance of cybersecurity is magnified by several factors. Participants noted the demands on time and budget and difficulty justifying additional resources in some areas, as well as the turnover and length of time it takes to appropriately develop, pitch, and enact programs and policies. Beyond the belief that cybersecurity is not well understood by legislators and how it pertains to the different levels of government, participants also noted viewpoints in their respective peer groups vary widely, depending on if their location (or one in proximity) recently experienced a cyber-attack.

Participants also noted that some type of coalition would at least be beneficial to the cyber sector, if not an absolute necessity. The participants put forward several different types of coalitions and interest groups they believed would be beneficial, each with its own strengths and weaknesses. The types of coalition participants referenced could enhance communication between layers of government, public and private partners, and provide common ground for similar locations and agencies to work together. Participants touched upon a few suggestions for partners and coalition members and added additional information in the following section.

Special Interest and Advocacy Groups and Views

In the discussion over advocacy and special interest groups, participants expanded upon their previous responses. While the participants felt a coalition would be beneficial to support and expand cybersecurity policies and procedures across the public sector, they had disparate views of the type of partners and who they felt would be better advocates. Participant 4 noted:

> “I feel that the main issue is that on a high level there are threats known by our government but that is as far as things go. local and state organizations that need to prepare or watch for these threats are often times left in the dark”.

Participant 4 felt that cyber is seen as an important aspect of operations across the board, but silos (limited sharing of information or intelligence) exist between different agencies and levels of government. On the topic of information sharing, Participant 2 felt one of the struggles facing information sharing was the lack of actionable intelligence. Just pushing threats or new vulnerabilities out to those tasked with cybersecurity and data integrity can be of little to no use if those individuals cannot translate the information to their level or provide patches and mitigation techniques to their agencies or constituencies. Participant 2 also noted: “there are a lot of groups that do not have resources to handle additional requirements or issues, so they wait until new legislation or policies come out and adjust as needed”. Developing an advocacy group could help translate this information, serve as a conduit, or provide expertise for implementation across multiple levels of systems.

Two major areas of consideration for advocacy and special interest groups are vendors and public private partnerships (PPP). Participant 2 discussed PPP in depth. In dealing with PPP in Tennessee he stated:

> “These PPP have not worked well in TN except for Knoxville. Whether the organization or its leader is motivated, and how they are motivated makes a lot of difference. In many cases, these organizations require a fee to participate. That excludes a lot of the smaller tech companies, the mom and pop locations cannot afford some of these fees. None of the governments can participate…Tried to build [one] for government and agencies, then wanted to build a portal. Had a lot of vendors that helped put events on and worked with them, but the conferences and meeting became sales pitches and charging for the online portal meant that some people and elements would then be excluded”.

Participant 2 noted that while the conferences or events sponsored by vendors might initially reach a wide range of people, but it can be exceedingly difficult to maintain participation and gain buy-in when the setting devolves into vendors making sales pitches, smaller organizations and public entities excluded, and limited opportunities for true information sharing and communication without pushing for a particular response or service.

Respondents also put forward some existing groups and specific organizations that could serve the public sector in a more formal capacity with respect to cyber operations. Among these groups were the Tennessee City Managers Association (TNCMA), the National Association of State Chief Information Officers (NASCIO), Chief Financial Officer groups, Infragard, technology councils, and the University of Tennessee Municipal Technical Advisory Service (UT-MTAS). Participant 1 spoke at length regarding advocacy groups and how they could best serve the public sector. The participant's point of view was neither the state nor advocacy groups should push mandates down to lower levels of government but should instead focus on developing best practices. Speaking of UT-MTAS, Participant 1 stated:

> "The Municipal Technical Advisory Service (UT-MTAS), they would be a group that could help to promote and manage those best practices. Once again, it's not mandates by the state but it's an advocacy for recognizing the dangers and here are a litany of things you can do at various cost levels and you do what you can afford to do and it's like how much insurance does a person buy? You buy what you can afford, and you just know that there are risks after that. And in my mind,

> that is the way it should go. And an MTAS or a Tennessee Municipal League those could be the carriers of the database if you will, they have the personnel that already do the training, that could just be one of the things that they could offer".

As further justification for the need for best practices and a strong coalition overseeing cyber operations, Participant 1 also noted:

> "I've had countless phone calls from peers that want to talk about what we went though and say 'OK, what happened and how do I avoid it [cyber-attack]'. Local agencies around here, not even cities but governmental/quasi-governmental agencies that I know the folks and they call and ask me to take a look at their plan and tell them if it is a good plan. I do not have the expertise to tell them if each plan is a good one for their specific department. It might look good, but I can't tell them if they are good plans. I can only tell them what we experienced and what we're going to do to keep it from happening again".

The disparity noted in attitudes and proactive measures taken between those impacted or near those impacted by cyberattacks is an area advocacy groups should seek to close.

Influences on Cybersecurity Policies and Procedures

The next question centered on what types of issues influence cybersecurity policies and procedures at the participants' levels. The two main influences discussed by the respondents were cyberattacks in the news and public consciousness and attacks occurring in the respondent's jurisdiction or surrounding areas. First, when considering news coverage, the participants split into two groups: one where current events and cyberattacks in the news raise awareness, help demonstrate opportunities, and help resource requests get approved; and one where participants felt their agency or organization already planned and understood threats and those events change public perception. The divide for the varying responses followed the level of the participant (state or below state level). Those operating below the state level felt news was beneficial in communicating risks to leadership and helping with funding and resource allocation. Participant 4 stated:

> “News stories and reports help, because that's what allows our executive staff to see what could happen. Recent cybersecurity issues in the City of Spring Hill, which is close by, and the City of Atlanta, which is a lot larger than us, also help to show that no one is exempt from cybersecurity issues. This helps with funding as well.”

Those working at the state level felt their agencies generally had policies and procedures in place to address many cyberattacks, so news is less relevant to their operations. The news can, however, influence public perception. Participant 3 noted:

> “At times these issues can raise the profile of policies and procedures in the public’s consciousness, but from the agency standpoint these areas generally have already been identified and addressed. Disconnect in how well an agency is handling an issue and what the public sees can be related to education, understanding, or what elements of practices are seen by the public.”

When discussing attacks occurring in their jurisdiction or one, they are familiar with, respondents felt practitioners, professionals, and officials in the impacted districts were excellent resources to help them identify potential vulnerabilities in their own systems and procedures. Participant 5 felt this was essential, noting: “I learn more from the professionals in the business and life lessons from those whom have been on the receiving end of cyberattacks”. Participant 1 echoed that sentiment and discussed previous efforts to understand cybersecurity risks and mitigation options in the past. Some conversations occurred between officials, but it did not take on a sense of urgency until they watched the City of Atlanta and other entities in Tennessee deal with cyberattacks over the last few years.

Cybersecurity and Emergency Preparedness and Planning

The next question in the interview asked participants how cybersecurity ties into the emergency planning and preparedness process at their level. All participants noted cyber is integrated into their emergency planning and preparedness, albeit to varying degrees. The state level participants documented a more complex and integrated version of cyber. Participant 3 provided an in-depth explanation:

> “[Cyber] is integrated into emergency preparedness and planning at the state level… From a practical standpoint, National Guard assets have been brought into the cybersecurity realm for prep and planning purposes. Tabletop Exercises (TTXs) have been held with multiple agencies and senior leaders and practitioners. These exercises provide communication and emergency planning outlines for different incidents… Additional training can further flesh out plans and procedures and these can be formalized when time and resources are available.”

Integration of cybersecurity considerations happens across state agencies, but this integration is a mix of policies, procedures, and best practices. In some areas, agencies advocating cyber do not have regulatory authority to enforce policies across all state agencies, forcing them to rely on best practices and working relationships instead of mandating changes.

In contrast to the state-level agencies, those working below the state level have more circumspect cyber integration. With the state-level agencies incorporating more cybersecurity practices and procedures, lower-level governments and agencies tend to focus on user impacts, needs, and efficiency. Participant 4 provided an overview:

> “Everything we do from an emergency preparedness aspect, has to be looked at from a cybersecurity standpoint as well. This brings in things, such as a screen lock policy. How does the screen automatically locking after so many minutes of inactivity, affect an officer that is on their way to an emergency? It is always a balance act to make sure we don't secure the system so much that it's not usable or make the system so usable that we can't secure it.”

Ensuring users have adequate training and that emergency and public safety systems are secure is a critical task. Cyberattacks, as noted by Participant 1, can impact public safety systems along with business and financial systems. Lower-level governments and officials can struggle to understand what networks are vulnerable or how they are tied together. Some governments have their police, fire, and rescue communications and computer systems linked to business networks. This can increase the exposure but may also help with efficiency and keep costs down. Seeing ransomware, DDOS, and other cyberattacks cause significant degradation of service in cities across the country has opened the eyes of leaders and officials and forced them to evaluate their posture and improve mitigation and recovery efforts.

Policy Changes over the Last Decade

When asked about how policies regarding cybersecurity changed over the last decade, participants identified several trends. First, policies changed significantly over the course of the last decade to decade and a half due in large part to the evolution of technology. The technology in place in the first part of the 2000s had much different security needs than the more interconnected world that exists today. As individuals increasingly telecommute, take work home with them, or continue to access networks on a variety of devices as they travel or are out of the office, additional policies and protections are required to protect against new vulnerabilities and reduce potential exposure. Participant 2 spoke in depth about one initiative of the last Tennessee governor, who left the office in 2019. That initiative moved a significant portion of workers in different state agencies to remote offices or allowed them to work from home. The state enacted several policies to mitigate potential risks. However, Participant 2 also noted:

> "Information is out there, there are a combination of problems. Boils down to information management. Cannot say 'do this and the risk goes away'. At the end of the day, the largest risk will always be the end user. That is where most of the problems exist. State mandates training, and numbers and breaches are coming down when efficiency tests are run. Where you run into challenges is that

> the risks and attacks are ever evolving, so you cannot create a policy or practice and expect the risk to zero out. The threat evolves, so your response and your users must evolve with the threat to stay safe and close loopholes and vulnerabilities."

Another trend noted by participants is that laws are not necessarily keeping up with the evolving cybersecurity landscape. Participant 4 stated: "I don't think the laws are keeping up. Again, our law makers don't fully understand the cyber security issues, so they don't know how to create laws against it". The agencies at the state level can implement policies and procedures to close some of the gaps, but again, agencies do not have the ability to force everyone to comply, particularly at the lower government levels. Getting policies enacted that are approved by agency leaders then issued by the Governor's office can help gain buy-in, but there are still training and communication needs to improve adoption and adherence.

The last major trend among responses to the question on policies is the need to create strong and broad policies to cover as many vulnerabilities as possible and improve the security of the networks in the most cost-efficient manner possible. With limited funding for lower governments available from the state, policies and procedures for the lower governments and partner agencies also need to consider the ability to fund compliance activities. A town or county with 15-20,000 citizens has a radically different stream of revenue than large cities and counties with millions of people and major commercial interests. The larger communities have integrated IT departments and agencies, where the small towns may not have staff or resources to address cyber questions in house. Where the large cities and higher governments employ certified cyber professionals, third-party vendors handle compliance and security programs for many counties and smaller cities and towns.

Accounting for Cybersecurity in Local Planning and Policies

When asked about cybersecurity planning at the local level, respondents noted two focus areas: user training, education, and testing internally and the widespread use of third parties. Most agencies in the higher levels of government have some form of an internal IT department with policies and protocols for user training and testing to one extent or another. Participant 5 stated: “We currently have two Network Admins who are responsible for monitoring our system and preventing attacks.” The training and education of users is critical, noted Participant 2:

> “At the end of the day, the largest risk will always be the end user. That is where most of the problems exist. State mandates training, and numbers and breaches are coming down when efficiency tests are run. Where you run into challenges is that the risks and attacks are ever evolving, so you cannot create a policy or practice and expect the risk to zero out. The threat evolves, so your response and your users must evolve with the threat to stay safe and close loopholes and vulnerabilities.”

Participant 1 discussed the need to have open dialogue with users regarding security posture and potential issues. If the users are afraid of getting into trouble if they click on a link that may contain malware the organization will likely only learn of the breach when found by IT or the system is locked, or the information shows up in the wild.

Participant 2 echoed this sentiment, noting that self-reporting of errors can drastically improve response time and allow for mitigation or isolation of an infected device before it has time to infect the entire system.

As noted in the previous section, much of the cybersecurity planning and efforts at the local level is handled by third parties. The use of a vendor can provide technical expertise and fully integrated solutions for smaller organizations and lower-level governments, but their use holds other vulnerabilities. As Participant 2 noted:

> "Cities and counties do not have the resources to pay an IT manager with the needed credentials to run their systems. They hire a vendor that charges a set amount per month to provide security. Does that make them secure? We (the state) cannot tell them what to do, they are a private company. They do not always have the talent pool, or it gets mismanaged. Some of the counties are on shared servers with some really bad people – not necessarily bad in terms of ulterior motives or bad intent, but poor security practices or they think they know what they are doing – goes back to a lack of education on the part of the vendor and the county not having anyone on staff to ask the right questions and determine whether the vendor is providing the services and protection they say they are.
> Do not know if there is a magic bullet, there are NIST standards and others, but what a lot of people do not understand is that just because you meet the standards and are compliant does not mean you are not at risk and are protected.
> Goes back again to the talent pool and education. Compliance does not mean secure. Not by a long shot, if you do not know how to defend you are in danger.

> In some cases, compliance to a particular standard can be a godsend for hackers or malicious actors since agencies do not deviate from their established security protocols, leaving them open to 0-day issues or other emergent threats against the network. Meeting standards and nothing else can lead back in a circle."

Across all participants, the use of vendors and their potential for additional vulnerabilities was a concern. When the local governments do not have staffing or expertise to oversee cybersecurity in-house, they can develop blind spots, believing the vendor is handling security properly and protecting all their assets. Officials in this position may not understand how the vendor sets up their security or know the right questions to ask when soliciting bids for security or selecting the protection that is right for their setup and operations.

Constraints and Limitations for Cybersecurity

Questions regarding the constraints and limitations for cybersecurity returned three main trends across all participants: time, technical expertise, and money. The time constraint discussed included both a lack of time for proper and continuing training, but also the limited time leaders and officials must fully understand cybersecurity and its implications for their operations. Developing and maintaining a comprehensive and effective cybersecurity program requires a significant time investment, one that is continuous. As noted in previous responses, technology, threats, and laws are constantly evolving, and each new change requires study to understand its implications on the security program and posture. The larger the organization, the more complex the undertaking and the more time is involved.

The technical expertise required for cybersecurity planning and activities is also a moving target. As technology changes and threats evolve, those overseeing the cybersecurity program must keep abreast of changes and counters to mitigate threats. A lack of technical expertise on the part of the users opens a range of potential attack vectors across networks and systems. Participant 2 stated:

> “showing people that if they are all green and on open networks, they are giving their data and other information away for free. Sometimes at conferences it is possible to have people look at their settings and talk them through the process and show them how open they are to attack. Other times can set up a test network and show individuals how easy it is to gain access if they allow their phones to connect to such an open signal.”

A lack of technical expertise by those running the program or selecting a vendor, as previously noted, can leave the organization vulnerable, unprotected, or under protected. The same issue can arise if those in charge of the cyber program do not understand the difference in certifications and education of applicants for an IT position.

The last and most discussed constraint or limitation for cybersecurity is budget. Each of the participants provided examples of budget constraints. Lower level governments can have difficulty hiring and retaining certified and qualified IT professionals due to salary requirements. Larger organizations and cities have more flexibility, but adequate expertise in in high demand in today’s operating environment, so retention can still be problematic. Participant 1 discussed budget considerations in depth:

> “I do not think it should be an edict [to maintain a certain vendor or security protocol]. I think there should be best practices. For ultimate security, there are different levels of security, and it is basically what can you afford. And that’s why I do not think it needs to be a mandate by the state because it’s what can you afford. There are some municipalities… that have a shoestring budget, they are just breaking even and keeping everything going and they could not afford to spend $50,000 a year to have their e-mail run through third party servers. And they only have 30 employees and only 10-15 of those have e-mail access so they need a different operation than maybe a Spring Hill that has 250 employees and 300 e-mail accounts. Maybe we can afford the $50-70,000 it’s going to cost to run our e-mail through a third-party server and let them get rid of the URL links. I don’t think it should be a mandated policy by the state. I think it should be here are some best practices, but I am not sure that anybody with the state has figured out what those best practices are.”

Participant 2 spoke about the limited funding available from the state to lower level governments. The State can set requirements for access to its systems but has little recourse to require lower governments to adopt specific practices, procedures, or policies as they fund their operations and can acquire security and outside assistance to a point. There are a number of proposals in play at the state level, including providing additional training, possibly creating a Cabinet-level post for Cyber in the Governor’s office, working with technical schools to assist lower-level governments with penetration testing and security, along with possible grant programs and others.

Provisions, Authority, and Resources Provided for Cybersecurity

Inquiring about the provisions, authority, and resources the different levels of government and their agencies receive from higher sources revealed another state and lower than state differentiation. At the state level, agencies have duties, responsibilities, and authority provided by federal requirements and mandates, executive orders, and state legislation and mandates. The State of Tennessee has two main agencies overseeing cybersecurity, though there are cyber activities within many agencies. Strategic Technical Services (STS) serves as the IT department for the state. Participant 2 stated:

> "State IT is set up to handle big universities – UT, Memphis, Austin Peay, UTC. ETSU direct contact. Issues at smaller schools are handled by DoS and contact with local governments. STS handles all issues at the state level and while they have relationships with some of the local governments, they are largely on their own, with help from [the Department of Safety and Homeland Security]… [SHS is] Lead agency for terrorism related instances Identify, mitigate and apprehend – very broad. Cyber falls under that umbrella. Requirement with establishment of new cyber division at DHS – cannot hack or pen test, but everything else."

The Department of Safety (DoS) also serves as the bridge between larger government roles (state and federal) and county and local governments, along with smaller colleges and universities, public utilities and the private sector. Many of the functions of the department involve pushing resources and opening lines of communication with the populations they serve.

The participants involved with the lower levels of government all stated that state policies are sparse, requiring the lower level governments to develop their own cybersecurity programs, policies, technologies, seek, select, and hire vendors, and fund their activities on their own. There was a hesitation from participants at the lower levels to seek a single policy pushed from the state, especially if it required an unfunded mandate. One additional issue is that cyber and IT vendors do not all offer their services everywhere across the State. Some IT companies are small operations only covering a single city or town. Others may be more expansive but tend to stay within geographic regions. There may not be a vendor in Middle or West Tennessee providing the same services and expertise as on in East Tennessee. This limits options for pushing out broad-based policies from the state or federal levels. Regarding authority and policies from the federal government down to the State, Participant 2 stated:

> "Nothing in writing… Feds want the states to take charge and handle cyber. Instruction to states is almost limited to 'Do Cyber'… Every state very different… Would need a lot of money spent to have similar system [to other states with larger budgets and more integrated cybersecurity agencies]. [Tennessee has] no way to handle in real time."

Participant 2 also noted that some states, such as Michigan, have a larger budget for exercises and training than Tennessee has for its entire department. The difference in levels of support can cause extremely different programs and protocols.

Clarity of Cybersecurity Policy and Mission, and Organizational Vision versus Actual

When asked about the clarity of the of the cybersecurity policy and mission within their organization, the results were mixed. The issue is somewhat clearer at the state level. As discussed in the previous section, state-level agencies receive mandates and requirements from the federal and state levels. Even in those areas where policies and the mission cover a wide range of topics and organizations, the state agencies understand expectations and the end goal. Clarity regarding mission and policies is less clear and defined with the lower-level agencies and government offices. With many smaller cities and counties relying on third parties to secure their networks, mission and policies may be only vaguely understood. The expectations to maintain secure networks and not introduce vulnerability on higher-level systems are understood, but practical application and how this is achieved is less evident. Best practices or a set of norms for below state-level entities are recommendations made by multiple participants.

With clarity somewhat murky in less-than-state level organizations, it can also be difficult to determine whether the operations and programs in effect meet the expectations of the policies and vision that created them. Participants in lower-level organizations felt clarity was an area they could improve upon. Whether the program relies on conducting testing and evaluating the results or is more exhaustive and consists of multiple layers, communication and transparency are crucial for success. Responding to the question about its ability to fulfill its missions and obligations, Participant 3 stated:

> “The agency is able to fulfill its missions and objectives with some caveats. There are some federal mandates and requirements the agency is not able to fulfill (an issue across most states). Without funding for federal mandates, states must decide which areas can comply, which will be addressed at a later time, and which areas require an exception to policy or other mitigation. These areas can be addressed with federal authorities to maintain transparency and develop plans for current and future operations and expenditures. Some areas may be nonstarters, depending on the funding needs and how they mesh with local requirements. Additional resources could help but would have to take the form of additional manpower, funds, time, and other items. The environment is too large to be able to cover all eventualities and priorities.”

Additional Information

At the close of the interviews, participants were provided an opportunity to add any information not covered in previous questions. Four participants elected to add additional commentary. The topics raised included establishing a new process at the state level to identify trusted and preferred vendors for lower-level governments and agencies to employ. This type of program can reduce the number of contractors with access to local, state, and federal networks, theoretically lower the overall risk and number of potential points of attack. Other programs currently being evaluated include adding internships for university students at the state and larger city departments to get them real-world experience while in school. This would allow these agencies to expand their skill sets, train a new group of professionals, and allow students to identify their own strengths and weaknesses before they leave school and enter the workforce full time.

Participant 5 included the following: "The technology is ever changing and that does worry me. How do we keep up? We are all more vulnerable than we would like to think". Participant 2 discussed the role of political and legislative turnover in gaining traction for new policies, procedures, and programs. Participant 5 noted:

> "[There is a] lot of political turnover – working to learn players and important individuals. Attempting to use legislative partners to get buy-in for the council and see how to help – knows they cannot circumvent the process or individuals but need to try to find a way to increase buy-in and get things moving. Change in governors not helping continuity. Legislators many times more interested in pursuing issues that will help them politically and make them look good in the press than in effective leadership or helping with legislation needed by agencies. Issues of constitutionality and legality are wrapped up in the conversation, but it also distracts from worthwhile legislation and needed changes and improvements. Working to show free services and other options for those that have a budget. Can send things out, but easier for localities to filter what they want. Some counties simply do not want any assistance – feel they have everything in hand. At time conflicts between counties and cities or different cities can lead to individuals refusing to work with others to find solutions."

Summary

Federal cybersecurity policy in the United States is generally believed to provide enough guidance for state-level governments and organizations, with some exceptions. The federal government provides some resources, but action at the state level is largely funded through the state. This creates a network of dissimilar policies and protocols in states across the country, with state leadership in some locations better grasping what is needed and earmarking more resources to deal with the emerging cybersecurity needs or the public. Below the state level, however, federal policies and guidelines are viewed by Tennessee agencies as largely irrelevant to their day-to-day operations. Participants in the study felt some type of best practice or suggested policies and programs could help define outcomes and create a more cohesive network across the state. The same held for how well implementation of policy compared to actions on the ground. The state-level agencies feel they are meeting requirements and expectations to a greater or lesser extent, while lower-level governments and agencies feel clarity could be improved and standardization or streamlining the decision-making process could benefit their operations.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

In this chapter, I will discuss my interpretation of the study findings, consider the limitations and implications of the study, and offer recommendations for future research. The purpose of the study was to evaluate the effectiveness of the current cybersecurity policy environment in Middle Tennessee. I sought to answer two research questions, with the primary one being whether U.S. cybersecurity policy at the federal level provides sufficient guidance and resources for state and local agencies to enact and implement cybersecurity policy at their level. The secondary question regarded cybersecurity programs and how well aligned the current implementation and operations are with the established policies and the initial vision of the legislation that created them.

The first section of the chapter contains an interpretation of the results of the study, including discussion of limitations related to data collection and trustworthiness as noted during the data collection and analysis phases of the research. Recommendations for additional research opportunities, methodologies for improving the study, and additional considerations follow in the second section. Finally, I will delve into the implications of the study, including for social change, and provide a conclusion to the study.

Regarding the primary research question, participants working at the state level indicated that federal cybersecurity policy and programs provide adequate guidance for many of their areas of responsibility. State-level participants identified a lack of funding and resources from the federal to the state level to achieve expectations as the main weakness. At the agencies and governments below the state level, participants said that the policies and procedures did not translate well to their level or were irrelevant for their operation entirely. Participants at lower-level entities also described a struggle with technical expertise, funding, vendor management, and a lack of best practices or guidance from the state to their level. Participants at all levels did reference the concept of shared responsibility, or the idea that each level of government, and public and private partners, have a vested interest in secure networks and proactive communication and workflows.

The findings for the secondary research question indicated that the policies and programs undertaken did not always meet expectations. Participants at all levels stated that at times they needed to pick and choose which goals, mandates, or requirements to meet during a given time period. The lack of funding provided for mandates by higher-level governments and the wide range of support (or lack thereof) for cybersecurity at different locations and levels both had negative consequences on the ability to meet expectations, participants said.

There were eight recurrent themes with more than 100 references during the data analysis portion of the study. These themes were resources, challenges, education, technical expertise, best practices, impact, considerations, and relationships. Resources, challenges, impact, and considerations are closely related within this study as each participant brought up individual struggles to fund and maintain cyber security programs. Participants noted how the lack of adequate resources (including financial, staffing, and legislative support) require their agencies to pick and choose where and how they will comply with mandates or policies or how they need to adjust to mitigate risks caused by lack of resources. Education and technical expertise were two areas participants grouped together but also distinguished between the education of individuals about a topic or process and technical expertise of those designing and overseeing the cybersecurity programs themselves. The last two recurrent themes were best practices and relationships. When participants referenced the need for best practices or how they employ them, they also spoke about establishing and maintaining relationships among different levels of government, the public, and public and private organizations.

Interpretation of the Findings

As discussed in Chapter 4, the participant responses, coded in relation to characteristics of ACF and recurrent themes, confirmed the selected conceptual and theoretical framework as appropriate for this study. The findings derived from this study can be beneficial in multiple ways. First and foremost, this study expands the knowledge of the targeted discipline as there has not been a study conducted of this type and scope in at least the past decade and a half, according to my review of the literature. This study can inform cybersecurity leaders, officials in the targeted and surrounding areas, and legislators about the cybersecurity policy and program environment, specifically with regard to constraints, challenges, resource issues, and gaps in understanding. Leaders can then re-examine policies and procedures at multiple levels of government, look for gaps and vulnerabilities, and determine best practices or common ground to resolve identified issues and improve the overall security posture.

Primary concerns by the participants included a dearth of best practices from higher governments; resource constraints; challenges with education for users, leaders, and legislators; questions about technical expertise of potential employees, vendors, and those in charge of cyber programs; the ability to identify needed skills; the ability (or lack thereof) to retain qualified employees; and the need for improved communication and better relationships between different levels of government. Participants also noted that current events and cyberattacks in the news can drive some decisions and behaviors. Participants clarified, however, that their agencies and organizations have plans and procedures in place to protect against a variety of threats and mitigate risks posed by these threats. The news stories do add uncertainty to their dealings with the public, particularly when agency operations or procedures are not publicly available or transparent. Data breaches that expose personal data are the primary topics of concern for the public, but ransomware attacks that can disrupt operations and impact daily life is, as well.

The findings of the study also confirmed that the ACF framework is well suited to evaluate the cybersecurity policy environment. Areas of focus for the ACF include coalition and coalition opportunities, constraints and resources, external events, governmental decisions, policy beliefs, inputs, and outputs, and stable system parameters (Sabatier, 1988). During the interviews, each participant referenced each of these areas to some extent and discussed the change in cyber policies over a period of years. Researchers typically use the ACF to evaluate the impact of these elements on a given policy environment over time spans of a decade or more (Sabatier, 1988). With respondents averaging 20 years of experience in their fields, they were well positioned to understand how policy changed over the years and provide insight into those forces that drive, or fail to influence, cyber policy within their organizations and in more general terms.

Limitations of the Study

The most significant limitation of this study was the lack of participation by members of the target pool, with 5% of the targeted individuals eventually participating. I submitted a change to the IRB to add additional locations, but participation remained very minimal across the participant pool. The participants in the study represented state and local level governments, along with very diverse socioeconomic populations. The participants responded to the interview protocol in a similar enough manner that saturation occurred. The information collected achieved the goals of this study. However, increased participation could shed light on topics or themes not included in this study.

With the goal of maximum participation, I constructed the study with redundant communications and multiple avenues for participation, including face-to-face, telephone, and online survey options. The protocol included an initial e-mail, subsequent reminder, and a final attempt, each sent 2 weeks apart. During the design and preparation phases of the study, I felt no community partners were needed. In many studies, community partners can serve as advocates for the researcher, providing access to additional populations or assisting with communication. As cybersecurity such a prominent issue across multiple levels of government, in the news, and in both the public and private sectors, I concluded a partner would only add complexity and potentially influence the outcome of the research. After reaching out to 100 different potential volunteers and speaking with almost a third in one form or another, I found a lack of partners (advocacy groups or other organizations) in place that would have been able to help with the targeted population. The research revealed a variety of stakeholders and interested parties in the selected geographic area, but each lacked access, resources, and/or adequate relationships with other stakeholders to coordinate large-scale efforts or collaboration.

One other limitation of this study was the limited geographic area targeted. When selecting a target population, I opted for locations with wide socioeconomic and demographic variety. The targeted counties included disparate political environments, governments among the richest and poorest in the state, and some of the smallest and largest population centers. While four counties are represented in the data collected, participant responses during the study brought out other counties across the state that either have other programs, partnerships, or could otherwise add to the study. There have been several cyberattacks across the state in recent months and years, encompassing both public utilities, the private sector, and governments at multiple levels. All participants noted in their responses that cyberattacks are on the increase, and directly referenced the impact those had on localities, organizations, and agencies they work with, and on the public at large.

Recommendations

There are a number of ways future research could expand or build upon this study. At the local level, future research could expand to cover a wider number of counties, regions within the state, or attempt to touch all counties in the state at once.

With 95 counties in Tennessee, the most feasible next step would be to conduct a study using the Grand Divisions of Tennessee (East, Middle, and West). This study included counties in the middle of the state, so broadening the study to include all counties in the Middle Division would be logical. The inclusion of more counties could expand upon the results of this study and determine if there are trends, issues, or coalitions that are involved in the larger area. An additional option for expansion at this level is to reach out to other entities in the geographic region that are also impacted by cybersecurity policies of the government agencies. These include, but are not limited to, critical infrastructure sectors, third party cybersecurity vendors, and private sector organizations that touch government systems and resources. The inclusion of these partners would widen the participant pool, provide more diverse responses and shed light on issues and concerns of those dealing with lower level governments and their cybersecurity programs. Gathering responses and data from only the government agencies only provides one part of the picture of the nature of the cybersecurity environment at this level. On a larger scale, a future study could also examine the cybersecurity environment across multiple states or in a regional area. This study can also be replicated, in original or expanded form, in any geographic area across the United States. The results and data can shed light on cybersecurity policies and programs in alternate locations, with the results compared to findings for this study. If the study is conducted in other states or across state lines there will be some differences in state policies, procedures, and resources that will require additional consideration and documentation.

Another recommendation for future studies, and one I believe to be of most critical importance, is to obtain a community partner. The community partner can advocate for participation among the targeted population and help connect researchers to key individuals within those populations. This research project connected with 35% of the participants, but 30 out 35 of those participants eventually elected to not participate. For most of these, a range of explanations were given for declinations to complete the interviews after initial conversations, while the others stopped communicating entirely during the process. Community partners can provide initial introductions, opportunities to present the research project and request participants, and advocate for the importance of the study and participation. As I found no partners that reach across all branches of the state, there is an opening to create an advocacy group to fill this void.

Implications

This study could generate positive social change on multiple fronts. Beginning with the local level, the research shed light on some of the challenges and barriers government agencies below the state level face with regard to cybersecurity policies and operations. Participants at this level are not as clear on how their organizations fit into the cybersecurity environment, something that further research, collaboration, and communication could help improve. There is also a lack of understanding as to what resources and assistance is available for lower level entities. Organizations employing individuals with a cybersecurity background or training are better positioned in this area, but those reliant on vendors or individuals in roles without training and expertise can be overwhelmed by the scope of the issues and options for securing systems. Expanded studies incorporating wider participation and geographic range can also bring additional perspectives and expertise into the findings.

At the state level, additional research can lead to enhanced understanding of the policy environment, how state agencies create policies and seek to incorporate or support policies by lower level governments and agencies. The participants working at the state level provided information on a range of programs either in the planning stages or that they are working to expand. Additional research could help identify ways to support state efforts, procure funding, and enhance communication and collaboration among agencies, legislators, and practitioners across the state. The information developed by this study can also be utilized to enhance communication and collaboration between states and help develop regional working groups or policies to protect agencies and groups working across state lines. Looking above the state level towards the regional and federal levels, the information and findings of this study can help improve collaboration and crafting of policies and procedures to translate more effectively to a wider group of users. Some of the challenges and resource considerations identified can also be used to pursue grants and programs to help states better secure their systems and close potential vulnerabilities as they utilize federal and regional systems.

The research also proved the ACF framework as an effective method to examine cybersecurity policies and trends over time. Three of the codes for ACF were among the highest utilized in the coding process and represented three of the top six codes across the study. The lowest frequency code under ACF in the analysis still was more common across the responses than 25 of the recurring codes found. Each of the participants touched upon each of the ACF codes and commented on the nature and evolution of cybersecurity policy over the longer term. The applicability of ACF was particularly relevant regarding constraints and resources, governmental decisions, and policy beliefs. Further use of ACF in the study of cybersecurity could further illuminate how government decisions and policy change over time, how resources allocations shift, and what inputs and environmental considerations lead to changes over the longer term.

Conclusion

While cybersecurity is currently frequently in the news and much of the public are only recently beginning to understand the potential vulnerabilities and impacts on their lives, this field has roots going back decades. The data collected in this research demonstrate a variety of challenges and obstacles at the state and local level to a comprehensive, cohesive, and effective cybersecurity environment. Communication, education, technical expertise, collaboration, resource constraints, and conflicting priorities are all areas that complicate the cyber policy environment. Results from this study indicate a desire for best practices and procedures from the federal and state level to push down to lower-level governments to help them shore up vulnerabilities and weaknesses in their policies and programs. Cybersecurity is a shared responsibility, and the only way to reduce vulnerabilities and enhance the overall system is to create a more collaborative environment where leaders at all levels understand threats, vulnerabilities, and how to work with agencies at multiple levels of government and the public and private sectors as a team.

References

Abbate, J. (1999). Getting small: A short history of the personal computer. *Proceedings of the IEEE, 87*(9), 1695-1698. Retrieved from https://doi.org/10.1109/5.784256

Adams, C. (2016). *March 3, 1991: Rodney King beating caught on video*. CBS News. Retrieved from http://www.cbsnews.com/news/march-3rd-1991-rodney-king-lapd-beating-caught-on-video/

André, P. (2016). *A phenomenological study of frontline hiring professionals that recruit in a cybersecurity world* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global database. (Accession No. 10250990)

Atlas.ti. (n.d.) *What is Atlas.ti*. Atlasti.com

Retrieved from: https://atlasti.com/product/what-is-atlas-ti/

Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture, 15*(2), 110-123. doi:10.1177/1206331211430016

Baumgartner, F., & Jones, B. (1991). Agenda dynamics and policy subsystems. *Journal of Politics, 53(4),* 1044-1074. Retrieved from https://doi.org/10.2307/2131866

Berkowitz, B., & Hahn, R. (2003). Cybersecurity: Who's watching the store? *Issues in Science and Technology, 19*(3), 55-62. Retrieved from http://www.jstor.org/stable/43312327

Blinder, A., & Perloth, N. (2018). *A cyberattack hobbles Atlanta and security experts' shudder.* Retrieved from https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

Carr, D. (1970). *The crisis of European sciences and transcendental phenomenology: An introduction to phenomenological philosophy*. Northwestern University Press

Carr, D. (1987). Husserl's world and ours. *Journal of the History of Philosophy, 25*(1), 151-167. Retrieved from https://doi.org/10.1353/hph.1987.0011

Caudle, D. (2010). *Decision-making uncertainty and the use of force in cyberspace: A phenomenological study of military officers* (Doctoral dissertation, University of Phoenix). Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a534888.pdf

Ciluffo, F., & Cardash, S. (2013). Cyber domain conflict in the 21st century. *Seton Hall Journal of Diplomacy and International Relations*, *14*(1), 41-47. Retrieved from http://connection.ebscohost.com/c/articles/87977324/cyber-domain-conflict-21st-century. Accession No. 87977324

Clarke, J. (2004). The United States, Europe, and Homeland Security: Seeing soft security concerns through a counterterrorist lens. *European Security*, *13*(1-2), 117-138. Retrieved from https://doi.org/10.1080/09662830490484836

Committee on National Security Systems. (2010). *National information assurance (IA) glossary* (CNSS Instruction No. 4009). Retrieved from http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf

Connelly, F., & Clandinin, D. (1990). Stories of experience and narrative inquiry. *Educational Researcher*, *19*(5), 2-14. Retrieved from https://doi.org/10.3102/0013189x019005002

County Technical Assistance Service. (n.d.). Directory of county officials. Retrieved from http://gml.ctas.tennessee.edu/

Creswell, J. (2013). *Research design: Qualitative, quantitative, and mixed method approaches.* Thousand Oaks, CA: SAGE.

Cyber Security and Infrastructure Security Agency (n.d.). *Resources for State, Local, Tribal, and Territorial (SLTT) Governments*. Retrieved from: https://www.us-cert.gov/resources/sltt

Cyber Security & Information Systems Information Analysis Center. (2017). The DoD cybersecurity policy chart. Retrieved from https://www.csiac.org/resources/the-dod-cybersecurity-policy-chart/

Da Cruz, F. (2013). *Programming the ENIAC*. Retrieved from http://www.columbia.edu/cu/computinghistory/eniac.html

Deere, S. (2018). *Confidential report: Atlanta's cyber-attack could cost taxpayers $17 million*. Retrieved from https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K/

Department of Defense. (2011). *Department of Defense Strategy for Operating in Cyberspace*. Retrieved from: http://csrc.nist.gov/groups/SMA/ispab/documents /DOD-Strategy-for-Operating-in-Cyberspace.pdf

Department of Defense. (2015). *Cyber Strategy*. Retrieved from: http://archive.defense.gov/home/features/2015/0415_cyber-strategy/

Department of Defense. (2015). *The DoD Cyber Strategy*. Retrieved from: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Department of Homeland Security. (2009). *Office for State and Local Law Enforcement*. Retrieved from: https://www.dhs.gov/sites/default/files/publications/ plcy_directive_252-11_office_for_state_and_local_law_enforcement.pdf

Department of Homeland Security. (2016). *Department of Homeland Security Law* Retrieved from: https://www.dhs.gov/sites/default/ files/publications/Law%20Enforcement%20Cyber%20Incident%20Reporting.pdf

Department of Homeland Security. (2018). *About CISA*. Retrieved from: https://www.dhs.gov/cisa/about-cisa

Department of Homeland Security. (2018(2)). *SLTT Governance Guide*. Retrieved from: https://www.dhs.gov/safecom/blog/2018/04/04/2018-sltt-governance-guide

Department of Homeland Security Law Enforcement Cyber Incident Reporting Guide. (2016). *A Unified Message for State, Local, Tribal, and Territorial Law Enforcement*. Retrieved from: https://www.dhs.gov/sites/default/files/publications /Law%20Enforcement%20Cyber%20Incident%20Reporting.pdf

Department of Homeland Security Directive 252-11. (2016). *Department of Homeland Security Law*. Retrieved from: https://www.dhs.gov/sites/default/ files/publications/Law%20Enforcement%20Cyber%20Incident%20Reporting.pdf

Dillane, M. (2018). *West Haven officials pay ransom after cyber-attack disables 23 serves at city hall.* Retrieved from: https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/

Dobran, B. (2019). *27 Terrifying Ransomware Statistics & Facts You Need to Read*. Retrieved from: https://phoenixnap.com/blog/ransomware-statistics-facts

Eeten, M. and Bauer, J. (2009). Emerging threats to Internet security: incentives, externalities, and policy implications. *Journal of Contingencies and Crisis Management* 17(4), 221-232. Retrieved from: https://doi.org/10.1111/j.1468-5973.2009.00592.x\

Electronic Privacy Information Center. (n.d.). *USA Patriot Act.* Retrieved from: https://epic.org/privacy/terrorism/usapatriot/

Ervin, S. (2017). *City of Spring Hill computer system hit by ransomware.* Retrieved from: https://www.wsmv.com/news/city-of-spring-hill-computer-system-hit-by-ransomware/article_b4ef98c5-2617-566d-9846-ab3132c95e5c.html

European Commission. (2018). *A new era for data protection in the EU.* Retrieved from: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf

Executive Order 12333. (1981). *United States intelligence activities*. Retrieved from: https://www.archives.gov/federal-register/codification/executive-order/12333.html

Executive Order 12829. (1993). *National Industrial Security Program*. Retrieved from: https://www.hsdl.org/?view&did=457290

Executive Order 13010. (1996). *Critical Infrastructure Protection*. Retrieved from: https://clinton6.nara.gov/1996/07/1996-07-15-executive-order-13010-on-critical-infrastructure-protection.html

Executive Order 13011. (1996). *Federal Information Technology*. Retrieved from: https://clinton6.nara.gov/1996/07/1996-07-16-executive-order-13011-on-federal-information-technology.html

Executive Order 13231. (2001). *Critical Infrastructure Protection in the Information Age*. Retrieved from: https://www.hsdl.org/?view&did=620

Executive Order 13354. (2004). *National Counterterrorism Center*. Retrieved from: https://www.hsdl.org/?view&did=449324

Executive Order 13355. (2004). *Strengthened Management of the Intelligence Community*. Retrieved from: https://www.hsdl.org/?view&did=449323

Executive Order 13470. (2008). *Amendments to Executive Order 12333, United States Intelligence Activities.* Retrieved from: https://www.hsdl.org/?view&did=487886

Executive Order 13549. (2010). *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*. Retrieved from: https://www.hsdl.org/?view&did=19427

Executive Order 13587. (2011). *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*. Retrieved from: https://www.hsdl.org/?view&did=689795

Executive Order 13636. (2013). *Improving Critical Infrastructure Cybersecurity.* Retrieved from: https://www.hsdl.org/?view&did=731040

Executive Order 13691. (2015). *Promoting Private Sector Cybersecurity Information Sharing*. Retrieved from: https://www.hsdl.org/?view&did=762390

Executive Order 13702. (2015). *Creating a National Strategic Computing Initiative*. Retrieved from: https://www.hsdl.org/?view&did=768436

Executive Order 13718. (2016). *Commission on Enhancing National Cybersecurity*. Retrieved from: https://www.hsdl.org/?view&did=790114

Fusch, P. and Ness, L. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, 20(9), 1408-1416. Retrieved from: tent/uploads/2015/09/fusch1.pdf

Galeotti, M. (2012). The cyber menace. *The World Today* 68(7) 32-35 Retrieved from http://www.jstor.org/stable/41962876

Garfinkel, S. (2012). Inside Risks: The Cybersecurity Risk. *Communications of the ACM 55(6).29-32*. Retrieved from: https://doi.org/10.1145/2184319.2184330 t3FaYPkf6UWz_YWIA&bvm=bv.146094739,d.cGw

Garland, M. (2015). A brief history of IT acquisition reform. *Journal of Contract Management*. Retrieved from: https://www.ncmahq.org/docs/default-source/default-document-library/articles/jcm15---article-05

Gjelten, T. (2013). First strike: U.S. cyber warriors seize the offensive. *Current*, (522), 3. Retrieved from: https://www.jstor.org/stable/43554737

Glaser, G. and Strauss, A. (1967). *The Discovery of Grounded Theory*. Aldine Transaction. Piscataway, New Jersey.

Glennon, M. (2012). State Level Cybersecurity. *Policy Review (171)*. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997565

Graciela, M. (2018). *Ransomware Attacks hits City of Spring Hill*. Retrieved from: https://www.thepluglosangeles.com/ransomware-spring-hill/

Greengard, S. (2016). Cybersecurity gets smart. *Communications of the ACM 59(5)*. Retrieved from: https://cacm.acm.org/magazines/2016/5/201590-cybersecurity-gets-smart/abstract

Hartnett, R. and Stever, J. (2011). The New Policy world of Cybersecurity. *Public Administration Review 71(3)*, 455-460. doi: 10.111/j.1540-6210.2011.02366.x

Healy, J. and Jordan, K. (2016). Setting Priorities on Cybersecurity. *Democracy: A Journal of Ideas Vol. 40*. Retrieved from: http://democracyjournal.org/magazine/40/setting-priorities-on-cybersecurity/

Heclo, H. (1974). *Social Policy in Britain and Sweden*. New Haven, CT. Yale University Press.

Heidenreich, B., & Gray, D. H. (2014). Cyber-Security: The Threat of the Internet. *Global Security Studies*, 5(1), 17-26.

Homeland Security Council. (2007). *National Strategy for Homeland Security*. Retrieved from: https://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

Homeland Security Presidential Directive 5. (2003). *Management of Domestic Incidents*. Retrieved from: https://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf

Hopkins, S., Wilson, A., Silva, A., and Forsythe, C. (2015). Factors Contributing to Performance for Cyber Security Forensic Analysis. In: Tryfonas, T., Askoxylakis

I. (eds). *Human Aspects of Information Security, Privacy, and Trust, HAS 2015. Lecture Notes in Computer Science, vol. 9190.* Springer, Cham

Hudson, B, Hunter, D., and Peckham, S. (2019). Policy failure and the policy-implementation gap: can policy support programs help? *Policy Design and Practice* 2(1). 1-14. Retrieved from: https://doi.org/10.1080/25741292.2018.1540378

International Strategy for Cyberspace. (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Retrieved from: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Kaiser, R. (2015). The birth of cyberwar. *Political Geography (46), 11-20. Retrieved from:* https://doi.org 10.1016/j.polgeo.2014.10.001 /

Kallberg, J. & Thuraisingham, B. (2013). From Cyber Terrorism to State Actors' Covert Cyber Operations. *Strategic Intelligence Management*. (229-233). Retrieved from: https://doi.org/10.1016/B978-0-12-407191-9.00019-3

Kennedy, M. (2017). *Volkswagen to plead guilty, pay $4.3 billion in emissions scheme settlement*. Nashville Public Radio. Retrieved from: http://www.npr.org/sections/thetwo-way/2017/01/11/509318791/volkswagen-to-plead-guilty-pay-4-3-billion-in-emissions-scheme-settlement

Koski, C. (2015). Does a partnership need partners? Assessing partnerships for critical infrastructure protection. *American Review of Public Administration, 45(3).* Retrieved from: https://doi.org/10.1177%2F0275074013494754

Leeuw, F. and Leeuw, B. (2012). Cyber society and digital policies: Challenges to evaluation? *Evaluation, 18(1)*, 111-127, doi: 10.1177/1356389011431777

Leiner, B., Cerf, V., Clark, D., Kahn, R., Kleinrock, L., Lynch, D., Postel, J., Roberts, L, and Wolff, S. (2009). A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review* 39(5). Retrieved from: https://doi.org/10.1145/1629607.1629613

Lin, H. (2016). Attribution of malicious cyber incidents: from soup to nuts. *Journal of International Affairs* 70(1). Retrieved from: https://jia.sipa.columbia.edu/attribution-malicious-cyber-incidents

Lobato, L. and Kenkel, K. (2015). Discourses of cyberspace securitization in Brazil and in the United States. *Revista Brasileira de Politica Internacional* 58(2) 23-43. Retrieved from: https://doi.org/ 10.1590/0034-7329201500202

Malafronte, K. (2019). *Malware Attack Shuts Down Columbia State for 2 Days.* Retrieved from: https://www.campussafetymagazine.com/university /malware-attack-columbia-state/

Malone, E. and Malone, M. (2013). The “wicked problem” of cybersecurity policy: analysis of United States and Canadian policy response. *Canadian Foreign Policy Journal. 19(2),* 158-177, doi: 10.1080/11926422.2013.805152

Maxwell, J. (2002). *Qualitative Research Design: An Interactive Approach (3d edition)*. Sage Publications. Thousand Oaks, California.

McLean, I. (1991). Rational Choice and Politics. *Political Studies (39, 496-512).* Retrieved from: https://doi.org/10.1111/j.1467-9248.1991.tb01625.x

McCollum, T. (2015). The cybersecurity imperative. *Internal Auditor*. Retrieved from: https://iaonline.theiia.org/2015/the-cybersecurity-imperative

McCracken, G. (1988). *Qualitative Research Methods: The long interview.* SAGE. doi: 10.4135/9781412986229

McLeod, S. (2008). *Case study method*. Retrieved from: Retrieved from: https://www.simplypsychology.org/case-study.html

Morris, T., Vandriel, M., Dries, W., Perdew, J., Schulz, R. and Jacobsen, K. (2015). Securing Operational Access. *The National Interest* (136). https://www.jstor.org/stable/44028370

National Archives. (2016). *Presidential Libraries*. Retrieved from: https://www.archives.gov/presidential-libraries.

National Conference of State Legislatures. (2019). *Cybersecurity Legislation 2018*. Retrieved from: http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx

National Cyber Strategy. (2018). *National Cyber Strategy*. Retrieved from: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

National White-Collar Crime Center & the Federal Bureau of Investigation. (2002). *IFCC 2002 Internet Fraud Report, January 1, 2002 – December 31, 2002*. Retrieved from: https://pdf.ic3.gov/2002_IFCCReport.pdf

National Initiative for Cybersecurity Careers and Studies. (n.d.). *Explore terms: a glossary of common cybersecurity terminology*. https://niccs.us-cert.gov/glossary

National Institute of Standards and Technology. (2017). *The Cybersecurity Framework: Implementation Guidance for Federal Agencies* (NISTIR 8170). Retrieved from: http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf

National Security Decision Directive 97. (1983). *National Security Telecommunications Policy*. https://reaganlibrary.archives.gov/archives/reference/Scanned %20NSDDS/NSDD97.pdf

National Security Decision Directive 113. (1983). *Security of Communications Systems Used by Key Government Officials.* https://reaganlibrary.archives.gov/archives /reference/Scanned%20NSDDS/NSDD113.pdf

National Security Decision Directive 145. (1984). *National Policy on Telecommunications and Automated Information Systems Security*. https://reaganlibrary.archives.gov/archives/reference/Scanned%20NSDDS/NSDD 145.pdf

National Security Directive 42. (1990). *National Policy for the Security of National Security Telecommunications and Information Systems.* https://bush41library.tamu.edu/files/nsd/nsd42.pdf

National Security Presidential Directive 54. (2008). *Cybersecurity Policy*. http://fas.org/irp/offdocs/nspd/nspd-54.pdf

O'Hara, J., Murphy, J., Vreeburg, J., Giaier, S., Maurer, D., Geffroy, M., and Lowe, T. (2015). Turf Wars: How a jurisdictional quagmire in Congress compromises Homeland Security. *New York Journal of Legislation & Public Policy*, 18(1), 1-44.

Office of Homeland Security. (2002). *National Strategy for Homeland Security*. Retrieved from: https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf

Osborne, C. (2018). *U.S. Hospital pays $55,000 to hackers after ransomware attack.* Retrieved from: https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/

Padgett, L. (2019). *Jackson County paid online criminals $400,000 to stop cyber-attack officials say*. Retrieved from: https://www.11alive.com/article/news/crime/ jackson-county-paid -online-criminals-400000-to-stop-cyber-attack-officials-say/85-bcb02d83-b607-4128-aae4-750b4a91fc50

Paris Call. (2018) *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*. Retrieved from: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity - paris-call-of-12-november-2018-for-trust-and-security-in

Passeri, P. (2019). *2018: A year of cyberattacks*. Retrieved from: https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyberattacks/

Passeri, P. (2019). *1-15 January 2019 Cyberattacks Timeline.* Retrieved from: https://www.hackmageddon.com/2019/02/04/1-15-january-2019-cyberattacks-timeline/

Passeri, P. (2019). *16-31 January 2019 Cyberattacks Timeline.* Retrieved from: https://www.hackmageddon.com/2019/02/14/16-31-january-2019-cyberattacks-timeline/

Passeri, P. (2019). *1-15 February 2019 Cyberattacks Timeline*. Retrieved from: https://www.hackmageddon.com/2019/03/12/1-15-february-2019-cyberattacks-timeline/

Passeri, P. (2019). *16-28 February 2019 Cyberattacks Timeline.* Retrieved from: https://www.hackmageddon.com/2019/03/20/16-28-february-2019-cyberattacks-timeline/

Passeri, P. (2019). *1-15 March 2019 Cyberattacks Timeline.* Retrieved from: https://www.hackmageddon.com/2019/04/09/1-15-march-2019-cyberattacks-timeline/

Passeri, P. (2019). *16-31 March 2019 Cyberattacks Timeline*. Retrieved from: https://www.hackmageddon.com/2019/04/15/16-31-march-2019-cyberattacks-timeline/

Patton, M. (2002). *Qualitative research & evaluation methods (third edition).* Sage. Thousand Oaks, CA.

Pedersen, C. (2014). Much Ado about Cyberspace. *Pepperdine Public Policy Review*, *71-21*. Retrieved from: https://digitalcommons.pepperdine.edu/ppr/vol7/iss1/3/

Pellerin, C. (2016). *DoD Cyber Strategy Defines How Officials Discern Cyber Incidents from Armed Attacks.* Defense Media Activity. Retrieved from: https://www.defense.gov/News/Article/Article/841043/dod-cyber-strategy-defines-how-officials-discern-cyber-incidents-from-armed-att

Peng, R. (2012). Reproducible research in computational science. *Science,* 2011;334(6060):1226-1227. doi:10.1126/science.1213847.

President's Information Technology Advisory Committee. (2005). *Cyber Security: A Crisis of Prioritization*. Retrieved from: https://apps.dtic.mil/dtic/tr/fulltext/u2/a449192.pdf

Presidential Decision Directive 5. (1993). *Public Encryption Management.* Retrieved from: https://clinton.presidentiallibraries.us/items/show/12737

Presidential Decision Directive 63. (1998). *Critical Infrastructure Protection. Retrieved from:* https://clinton.presidentiallibraries.us/items/show/12762

Presidential Directive 24. (1977). *Telecommunications Protection Policy*. Retrieved from: https://www.jimmycarterlibrary.gov/documents/pddirectives/pd24.pdf

Presidential Directive 53. (1979). *National Security Telecommunications Policy*. https://www.jimmycarterlibrary.gov/documents/pddirectives/pd53.pdf

Presidential Policy Directive 21. (2013). *Critical Infrastructure Security and Resilience*. Retrieved from: https://www.hsdl.org/?view&did=731087

Presidential Policy Directive 41. (2016). *Directive on United States Cyber Incident Coordination*. Retrieved from: https://www.hsdl.org/?view&did=797544z

Public Law 89-306. (1965). *Automatic Data Processing Act of 1965.* Retrieved from: http://uscode.house.gov/statutes/pl/89/306.pdf

Public Law 100-235. (1987). *Computer Security Act of 1987. Retrieved from:* https://www.gpo.gov/fdsys/pkg/STATUTE-101/pdf/STATUTE-101-Pg1724.pdf

Public Law 102-194. (1991). *High Performance Computing Act of 1991*. Retrieved from: https://www.congress.gov/bill/102nd-congress/senate-bill/272?q=%7B%22search%22%3A%5B%22PL102-194%22%5D%7D&r=1

Public Law 104-191. (1996) *Health Insurance Portability and Accountability Act of 1996.* https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

Public Law 106-102. (1999). *Gramm-Leach-Bliley Act*. Retrieved from: https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

Public Law 107-56. (2001). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001.* https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

Public Law 107-296. (2002). *An Act to establish the Department of Homeland Security, and for other purposes*. Retrieved from: https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

Public Law 107-305. (2002). *Cyber Security Research and Development Act.* Retrieved from: https://www.congress.gov/107/plaws/publ305/PLAW-107publ305.pdf

Public Law 107-347. (2002). *E-Government Act of 2002*. Retrieved from: https://www.congress.gov/bill/107th-congress/house-bill/2458/

Public Law 113-274. (2014). *Cybersecurity Enhancement Act of 2014*. Retrieved from: https://www.congress.gov/bill/113th-congress/senate-bill/1353?q=%7B%22search%22%3A%5B%22cybersecurity%22%5D%7D&r=6

Public Law 113-282. (2014). *National Cybersecurity Protection Act of 2014*. Retrieved from: https://www.congress.gov/bill/113th-congress/senate-bill/2519?q=%7B%22search%22%3A%5B%22cybersecurity%22%5D%7D&r=1

Public Law 113-283. (2014). *Federal Information Security Modernization Act of 2014*. Retrieved from: https://www.congress.gov/bill/113th-congress/senate-bill/2521?q=%7B%22search%22%3A%5B%22federal+information+security+modernization+act%22%5D%7D&r=5

Pugh, E. and Aspray, W. (1996). Creating the Computer Industry. *IEEE Annals of the History of Computing*. 18(2). Retrieved from: https://doi.org/10.1109/MAHC.1996.490112

Rutkowski, A. (2011). Public international law of the international telecommunication instruments: cyber security treaty provisions since 1850. *Digital Policy, Regulation and Governance* 13(1) 13-31. Retrieved from: https://doi.org/10.1108/14636691111101856

Sabatier, P. (1988). An advocacy coalition framework of policy change and the role of policy-oriented learning therein. *Policy Sciences* 21: 129-168.

Saldaña, J. (2016). *Theories of the policy process (Second edition)*. Boulder, Colorado. Westview Press.

Shackelford, S. and Bohm, Z. (2016). Securing North American Critical Infrastructure: a comparative case study in cybersecurity regulation. *Canada-United States Law Journal Vol. 40.*

Simon, H. (1964). On the concept of organizational goal. *Administrative Science Quarterly* 9(1).

Slayton, R. (2016). Framing computer security and privacy: the 1960s and 1970s. *Computers & Society* 26(3). Retrieved from:

http://dx.doi.org/10.1145/3024949.3024954

State of Tennessee Executive Order 8. (2003). *An order Constituting the Tennessee Office of Homeland Security, the Homeland Security Council, and the Tennessee Governor's Citizen Corps Advisory Committee.* Retrieved from: http://share.tn.gov/sos/pub/execorders/exec-orders-bred8.pdf

State of Tennessee Executive Order 16. (2012). *An order dissolving the Tennessee Governor's Citizen Corps Advisory Committee as constituted by Governor Phi Bredesen's Executive Order No. 8, dated April 3, 2003.* Retrieved from: http://www.tn.gov/assets/entities/safety/attachments/exec-orders-haslam16.pdf

State of Tennessee Executive Order 23. (2005). *An order establishing the National Incident Management System as the basis for all incident management in the State.* Retrieved from: http://share.tn.gov/sos/pub/execorders/exec-orders-bred23.pdf

State of Tennessee Executive Order 36. (2002). *An order constituting the Tennessee Office of Homeland Security and the Homeland Security Council and establishing the Tennessee Governor's Citizen Corps Advisory Committee*. Retrieved from: http://share.tn.gov/sos/pub/execorders/sundquist%20executive%20order%20no.%2036.pdf

State of Tennessee Executive Order 48. (2007). *An order transferring the Tennessee Office of Homeland Security, the Homeland Security Council, and the Tennessee Governor's Citizen Corps Advisory Committee from the Governor's Office to the Department of Safety*. Retrieved from:

http://share.tn.gov/sos/pub/execorders/exec-orders-bred48.pdf

Symantec. (2019). *Internet Security Threat Report*. Retrieved from: https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf

Tellis, W. (1997). Introduction to case study. *The Qualitative Report* 3(4). Retrieved from: http://nsuworks.nova.edu/tqr/vol3/iss2/4/

Tennessee Anti-Phishing Act. (2006). *Anti-Phishing Act of 2006. Retrieved from:* http://www.lexisnexis.com/hottopics/tncode/

Tennessee Bureau of Investigation. (n.d.). *Tennessee Bureau of Investigation Home Retrieved from:* https://www.tn.gov/content/tn/tbi.html

Tennessee Department of Safety and Homeland Security. (n.d.). *About us. Retrieved from:* http://www.tn.gov/safety/article/about_us

Tennessee Department of Safety and Homeland Security 2. (n.d.). *Directory*. Retrieved from: http://www.tn.gov/safety/article/directory

Tennessee Department of Safety and Homeland Security 3. (n.d.). *Homeland Security*. Retrieved from: http://www.tn.gov/safety/section/homelandsecurity

Tennessee Department of Safety and Homeland Security 4. (n.d.). Cyber Awareness. Retrieved from: http://www.tn.gov/assets/entities/safety /attachments/A_Safer_Tennessee.pdf

Tennessee Personal and Commercial Computer Act of 2003. (2003). *Tennessee Personal and Commercial Computer Act of 2003*. Retrieved from: http://www.lexisnexis.com/hottopics/tncode/

Tennessee State Government. (2016). *A Safer Tennessee: Highlights of the Governor's initial public safety action plan, 2016-2018 with key performance indicators.* Retrieved from: http://www.tn.gov/assets/entities/safety/ attachments/A_Safer_Tennessee.pdf

Trautman, L. (2015). Cybersecurity: what about U.S. policy? *University of Illinois Journal of Law, Technology & Policy*. Retrieved from: https://dx.doi.org/10.2139/ssrn.2548561

Tripathi, S. (2015) Cyber: Also a Domain of War and Terror*, Strategic Analysis, 39:1,* 1-8, DOI: 10.1080/09700161.2014.980549

United States Code. (2009). *Title 44, Public Printing and Documents Section 3502*. Retrieved from: https://www.gpo.gov/fdsys/pkg/USCODE-2009-title44/pdf/USCODE-2009-title44-chap35-subchapI-sec3502.pdf

United States Census Bureau. (2017). *Quick facts: Brentwood city, Tennessee.* Retrieved from: https://www.census.gov/quickfacts/fact/table/ brentwoodcitytennessee /PST045218

United States Census Bureau. (2017). *Quick facts: Columbia city, Tennessee*. Retrieved from: https://www.census.gov/quickfacts/fact/table/ columbiacitytennessee /PST045218

United States Census Bureau (2017). *Quick facts: Davidson County, Tennessee*. Retrieved from: https://www.census.gov/quickfacts/fact/table/ davidsoncountytennessee /PST045218

United States Census Bureau. (2017). *Quick facts: Fairview city, Tennessee.* Retrieved from: https://www.census.gov/quickfacts/fact/table/ fairviewcitytennessee /PST045218

United States Census Bureau. (2017). *Quick facts: Franklin city, Tennessee.* Retrieved from: https://www.census.gov/quickfacts/fact/table/ franklincitytennessee /PST045218

United States Census Bureau. (2017). *Quick facts: Giles County, Tennessee.* Retrieved from: https://www.census.gov/quickfacts/fact/table/ gilescountytennessee /PST045218

United States Census Bureau. (2017). *Quick facts: Maury County, Tennessee*. Retrieved from: https://www.census.gov/quickfacts/fact/table/ maurycountytennessee/ PST045218

United States Census Bureau. (2017). *Quick facts: Nashville-Davidson (balance), Tennessee*. Retrieved from: https://www.census.gov/quickfacts/fact/table /nashvilledavidson balancetennessee /PST045218

United States Census Bureau. (2017). *Quick facts: Pulaski city, Tennessee*. Retrieved from: https://www.census.gov/quickfacts/fact/table/ pulaskicitytennessee/PST045218

United States Census Bureau. (2017). *Quick facts: Spring Hill city, Tennessee*. Retrieved from: https://www.census.gov/quickfacts/fact/table/ springhillcitytennessee /PST045218

United States Census Bureau. (2017). *Quick facts: Williamson County, Tennessee.* Retrieved from: https://www.census.gov/quickfacts/fact/table/ williamsoncountytennessee /PST045218

United States Census Bureau. (2018). *Quick facts: Tennessee*. Retrieved from: https://www.census.gov/quickfacts/fact/table/tn/PST045218

United States Cyber Command. (2015). *Beyond the build: delivering outcomes through cyberspace. The commander's vision and guidance for US Cyber Command.* Retrieved from: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf

United States Office of Homeland Security. (2002). *National Strategy for Homeland Security*. Retrieved from: https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf

United States Strategic Command. (2016). *U.S. Cyber Command (USCYBERCOM)*. Retrieved from: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. (2001). Pub. L. No. 107-56.

Vermuelen, H. (1995). Origins and Institutionalization of Ethnography and Ethnology in Europe and the USA, 1771-1845. *Fieldwork and Footnotes: Studies in the History of European Anthropology*, 39-59.

Walden University Center for Research Quality. (n.d.). *Research Ethics & Compliance: Welcome from the IRB.* https://academicguides.waldenu.edu/researchcenter/orec

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

Warner, M. (2015). Notes on the Evolution of Computer Security Policy in the United States, 1965-2003. *IEEE Annals of the History of Computing* 37(2). Retrieved from: https://doi.org/10.1109/MAHC.2015.25

Weible, C., Sabatier, P., and McQueen, K. (2009). These and variations: taking stock of the advocacy coalition framework. *Policy Studies 37(1).*

Whetstone, T. (2018). *Knox County election night cyberattack was smokescreen for another attack.* Retrieved from: https://www.knoxnews.com/story /news/local/2018/05/17/knox-county-election-cyberattack-smokescreen-another-attack/620921002/

Wingfield, T. and Sharp, R. (2014). Tanks in cyberspace. *International Policy Digest* 1(4). Retrieved from: https://intpolicydigest.org/2014/04/14/tanks-cyberspace/

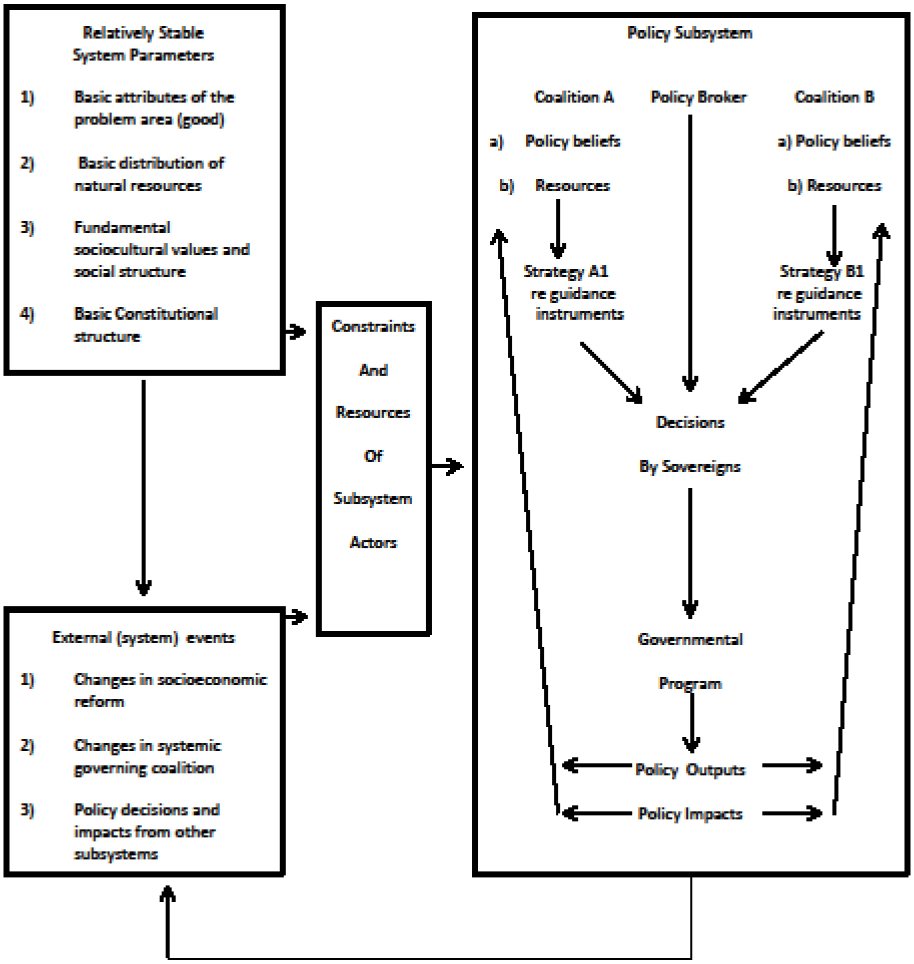
Wipersoft. (2019). *The biggest data breaches of 2018.* Retrieved from: https://www.wipersoft.com/the-biggest-data-breaches-of-2018/

Wolfe, M., Jones, B., and Baumgartner, F. (2013). A Failure to Communicate: Agenda Setting in Media and Policy Studies. *Political Communication* 30(2).

Yin, R. (2014). *Case study research; design and methods (fifth edition).* Thousand Oaks, California. SAGE

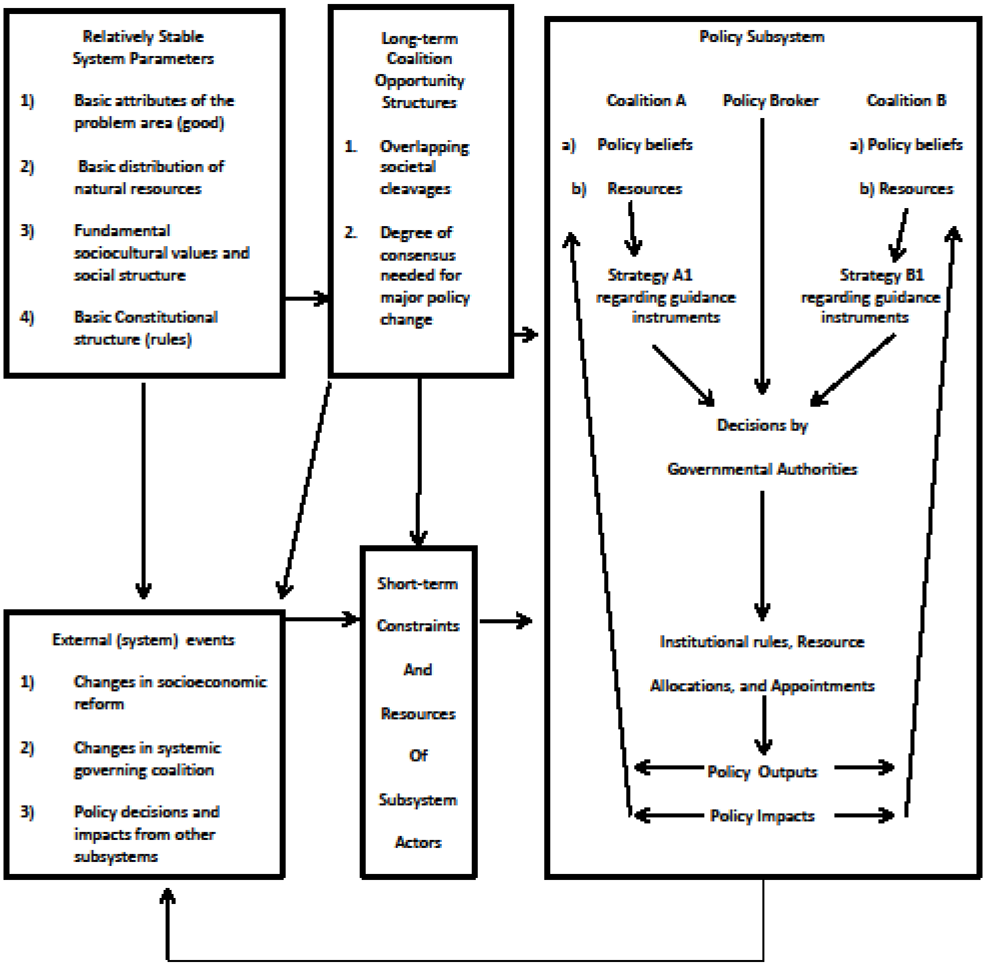
Zaveri, M. (2018). *Harris County tightens cybersecurity after almost losing $900K in phishing attack.* Retrieved from*:* https://www.houstonchronicle.com/news/houston-texas/houston/article/Harris-County-looks-to-boost-cyber-security-after-12524738.php

Appendix A: Advocacy Coalition Framework Outline From 1988


Relatively Stable
System Parameters
1) Basic attributes of the problem area (good)
2) Basic distribution of natural resources
3) Fundamental sociocultural values and social structure
4) Basic Constitutional structure
Constraints
And
Resources
Of
Subsystem
Actors
External (system) events
1) Changes in socioeconomic reform
2) Changes in systemic governing coalition
3) Policy decisions and impacts from other subsystems
Policy Subsystem
Coalition A
Policy Broker
Coalition B
a) Policy beliefs
b) Resources
a) Policy beliefs
b) Resources
Strategy A1 re guidance instruments
Strategy B1 re guidance instruments
Decisions
By Sovereigns
Governmental
Program
Policy Outputs
Policy Impacts

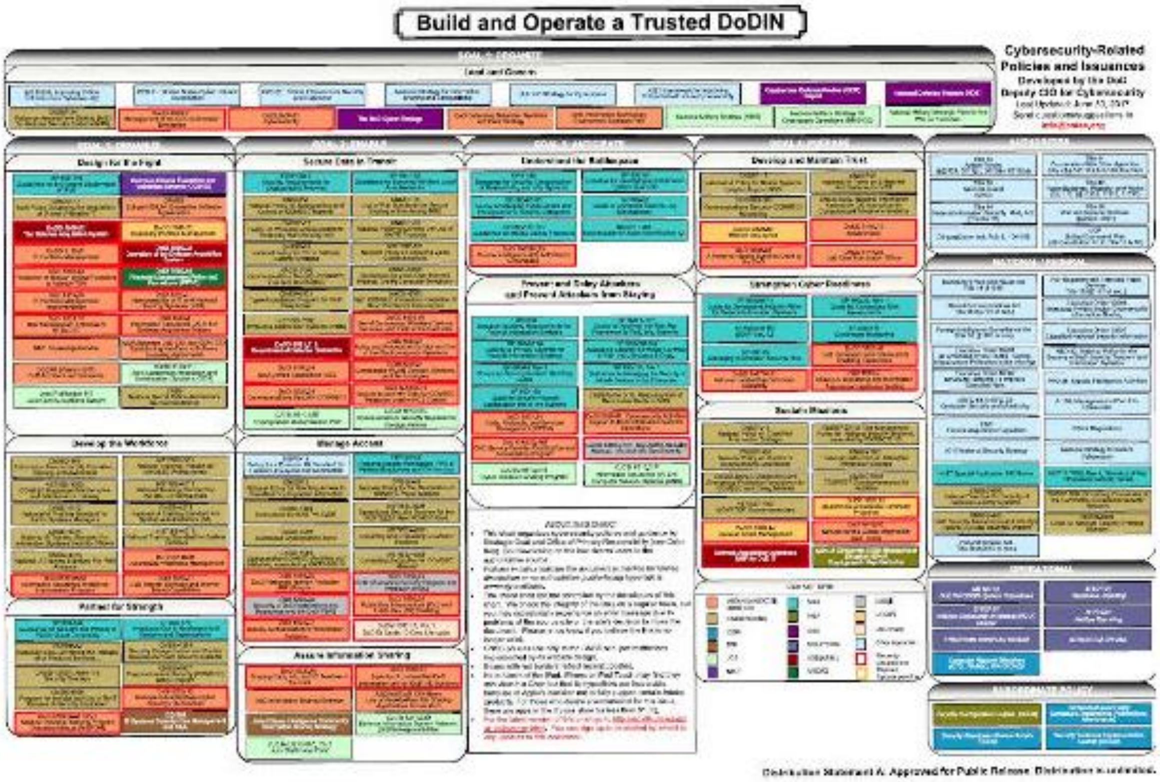
From "An Advocacy Coalition Framework of Policy Change and the Role of Policy-Oriented Learning Therein," by P. Sabatier, 1988, *Policy Sciences, 21*, p. 132. Copyright 1988 by Springer.

Appendix B: Advocacy Coalition Framework Outline From 2009


Relatively Stable System Parameters
1) Basic attributes of the problem area (good)
2) Basic distribution of natural resources
3) Fundamental sociocultural values and social structure
4) Basic Constitutional structure (rules)
Long-term Coalition Opportunity Structures
1. Overlapping societal cleavages
2. Degree of consensus needed for major policy change
Policy Subsystem
Coalition A
Policy Broker
Coalition B
a) Policy beliefs
b) Resources
a) Policy beliefs
b) Resources
Strategy A1 regarding guidance instruments
Strategy B1 regarding guidance instruments
Decisions by Governmental Authorities
Institutional rules, Resource Allocations, and Appointments
Policy Outputs
Policy Impacts
External (system) events
1) Changes in socioeconomic reform
2) Changes in systemic governing coalition
3) Policy decisions and impacts from other subsystems
Short-term Constraints And Resources Of Subsystem Actors

From "Themes and Variations: Taking Stock of the Advocacy Coalition Framework," by C. Weible, P. Sabatier, & K. McQueen, 2009, *Policy Sciences*, *37*, p. 123. Copyright 2009 by Springer.

Appendix C: The Department of Defense Cybersecurity Policy Chart


Build and Operate a Trusted DoDIN
Cybersecurity-Related Policies and Issuances Developed by the DoD Deputy CIO for Cybersecurity
Design for the Fight
Secure Data in Transit
Understand the Battlespace
Develop and Maintain Trust
Develop the Workforce
Manage Access
Prevent and Delay Attackers and Prevent Attackers from Staying
Strengthen Cyber Readiness
Sustain Missions
Partner for Strength
Assure Information Sharing
Distribution Statement A: Approved for Public Release. Distribution is unlimited.

Reprinted from "The DoD Cybersecurity Policy Chart (Formerly the IA Policy Chart," by Cyber Security and Information Systems Information Analysis Center, 2017 (https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/). In the public domain.

Appendix D: Agencies and Offices Targeted for Interviews in the Study

Office	Government Level	Potential Interviews
U.S. Senate	Federal	2
U.S. House	Federal	9
TN Senate	State	19
TN House	State	25
TN Governors Office	State	3
Safety and Homeland Security	State	2
TBI	State	2
TEMA	State	2
Davidson County	County	3
Giles County	County	3
Maury County	County	3
Williamson County	County	3
Brentwood	City	3
Columbia	City	3
Fairview	City	3
Franklin	City	3
Mount Pleasant	City	3
Nashville	City	3
Pulaski	City	3
Spring Hill	City	3

Appendix E: Interview Protocol

Date:
Time:
Office/Agency:
Interview Candidate: ________________________________

Opening Comments:

Thank you again for agreeing to meet with me today. Our discussion should last approximately 90 minutes. Our discussion topic is cybersecurity policy and management, particularly how federal policy influences state policies and procedures, if adequate resources exist, and where this issue ranks among other priorities on the legislative and operational priority matrix. For those with working knowledge of agency operations in the state, we will also discuss how well programs and policies are implemented in the field and whether they meet the expressed vision and goal of published policies.

I will begin the interview with some background questions regarding your personal and professional background, responsibilities, and level of engagement with cybersecurity in your current role. The second set of questions will focus on the current policy environment around cybersecurity. In the final section, questions will explore the relationship between established policies in the state and their implementation in the field.

As a reminder, you do not have to answer any questions you choose and we can skip over a question and return to it later in the interview to address, if desired. All responses provided are anonymous and no identifying information will be provided to anyone or included in publication. I will conduct the collection and analysis myself, so there is no risk for data exposure.

I will be digitally recording the audio portion of the interview to assist with transcription and data capture. Do you have any questions before we begin?

I would like to begin with some general questions to establish your background and experience, along with your engagement level with cybersecurity in your current role.

Opening Questions:

- What is your professional and educational background?
- How long have you been in your current position?
- What are the primary responsibilities of your current role?
- What issues do your constituents (if applicable) communicate with you most about?
- What special interest areas or policy subjects do you feel are most important to the business, social, or political environment of your home territory?
- What are the most pressing legislative/policy items at your peer level?

- What is your comfort level with the field of cybersecurity from both technical and policy perspectives?
- Are there any unique considerations or emergent issues I need to take into consideration for the interview today?

Research Question 1:
Does U.S. cybersecurity policy at the federal level provide sufficient guidance and resources for state and local agencies to enact and implement cybersecurity policy at their levels?

Interview Questions 1:

1. What are the main drivers of the most important legislative issues on your agenda year to year?
2. Can you provide some examples of emergent (unplanned) issues that elevated beyond their assumed importance during a given session over the last decade?
3. In your opinion, what are the responsibilities of the various levels of government with regard to cybersecurity?
4. Which federal cybersecurity policies and programs are the most relevant and applicable to the current policy environment in Middle Tennessee?
5. Based on your experience, is cybersecurity viewed consistently (as a need, as an issue for the federal government, or mixed) by your peers or is support divided? If divided, are the coalitions divided along party lines or other groups?
    a. Are there special interest groups or other outside parties expressing interest in cybersecurity policy within the State of Tennessee (either for or against) and contributing to advocacy or coalitions on either side of the discussion? If so, can you provide groups or other major stakeholders involved, along with their belief structure and resources?
    b. How effective are these coalitions at influencing legislative opinions on topics up for discussion and the eventual direction and decisions made by the governor?
    c. What methods are used by these coalitions to further their agenda (resource allocation, appointments, rules and regulations)?
6. What are your main influences when considering cybersecurity policies and procedures (do news stories or reports of hacking and other activity raise the issue to an actionable level if it was not previously there)?
7. How (if at all) have cybersecurity considerations impacted emergency preparedness and planning at your level?
8. Over the course of the last decade, how have the following policy areas changes around cybersecurity:
    a. Attributes of the problem
    b. Fundamental social values and structure
    c. Basic constitutional structure and laws
    d. Socioeconomic reform
    e. Systemic governing coalition

f. Degree of consensus needed for policy change
g. Overlapping societal cleavages
h. General direction and focus of policy

Research Question 2:
Regarding cybersecurity programs, how well aligned is the current implementation with established policies and the initial vision of the legislation that created them?

Interview Questions 2:

1. Please provide an overview of how cybersecurity is accounted for in the planning and policy of your locality (higher government responsibility, emergency manager in charge, CIO, et cetera).
2. What are the major constraints and/or limitations on emergency planning and operations regarding cybersecurity?
3. What provisions, authority, or resources are provided by higher government entities to you around cybersecurity?
4. How clear are your organization's mission, focus, and goals around cybersecurity?
    a. Can you provide a brief overview of each?
    b. How are these measured in your organization?
5. With your current level of resources, oversight, and authority, are you able to fully accomplish all the missions and objectives set out for you by policy, charter, and directive?
    a. If not, what resources are needed to bridge the gap between your current state and fulfillment?
6. How do your operations and field agencies compare on the ground to their vision on paper and in the charter for your organization (compare the implementation and continued finding and operation of ED and CS to the original concepts, budgets, and strength and mission on paper)?
7. In your opinion, what is the most effective method to address concerns of a disconnect in implementation, mission creep, conflicting directives, or lack of resources to perform critical tasks?

Closing Comments:
This concludes our interview today. Thank you once again for your participation in and contribution to this research project. Within the next seven days I will provide you with a written transcription of the interview question and responses from this session via e-mail for your review. Please review the transcription and let me know if there is anything that needs to be revised, edited, or revisited.

Appendix F: Invitation E-mail for Participants

Good Afternoon:

My name is Daniel Scherr and I am a doctoral candidate at Walden University. I am conducting a research study focused on public officials and cybersecurity in Tennessee. This study will occur in the form of interviews that I will facilitate. Each participant's confidentiality will be protected during the collection of data and the reporting of results. This e-mail is meant to serve as a request for participants for this voluntary study related to cybersecurity. If you are interested in participating in the study, please e-mail me directly at [redacted] and I will provide the necessary paperwork for informed consent for your review and completion.

If you need any additional information prior to deciding as to whether to participate, please feel free to contact me at the e-mail address noted below.

As a reminder, participation is voluntary and confidential.

Thank you for your time and consideration and please feel free to contact me with any questions.

Most Sincerely,

Daniel Scherr, MBA, CFE

[e-mail address redacted]

Appendix G: Reminder E-mail for Participants

Good Afternoon:

This e-mail is meant to serve as a reminder that there are two weeks remaining to communicate interest in participating in the voluntary study related to cybersecurity.

If additional information is needed prior to making a decision as to whether or not to participate, please feel free to contact me at the e-mail address noted below.

As a reminder, participation is voluntary and confidential.

Thank you for your time and consideration and please feel free to contact me with any questions.

Most Sincerely,

Daniel Scherr, MBA, CFE

[e-mail address redacted]

Appendix H: Final E-mail for Participants

Good Afternoon:

This e-mail is meant to serve as a reminder that there is one week remaining to communicate interest in participating in the voluntary study related to cybersecurity.

If additional information is needed prior to deciding as to whether to participate, please feel free to contact me at the e-mail address noted below.

In the event in which I do not receive a response within the next week, it will be understood that you are not interested in participating. This e-mail will be the last communication that is sent to individuals who do not respond.

As a reminder, participation is voluntary and confidential.

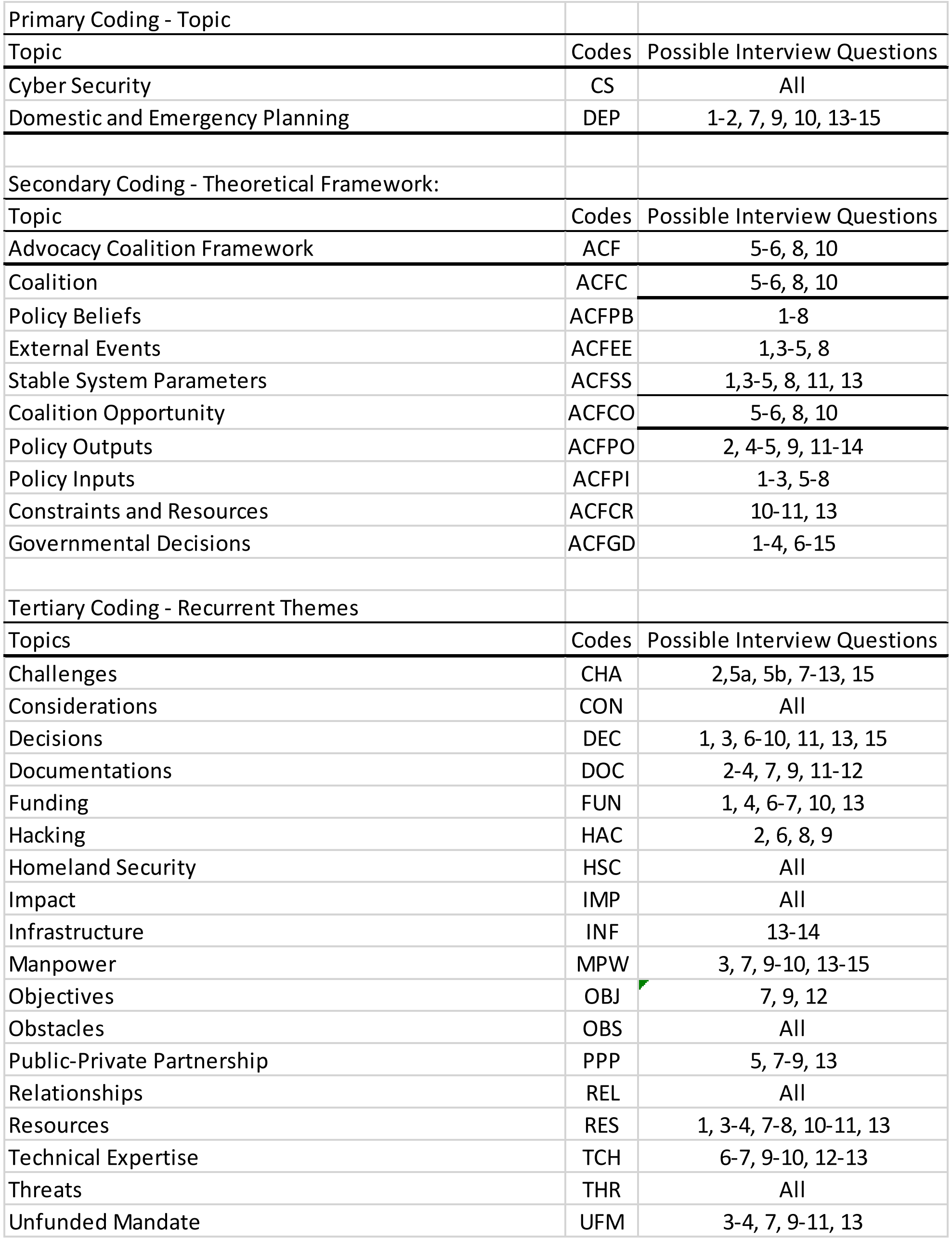
Thank you for your time and consideration and please feel free to contact me with any questions.

Very Respectfully,

Daniel Scherr, MBA, CFE

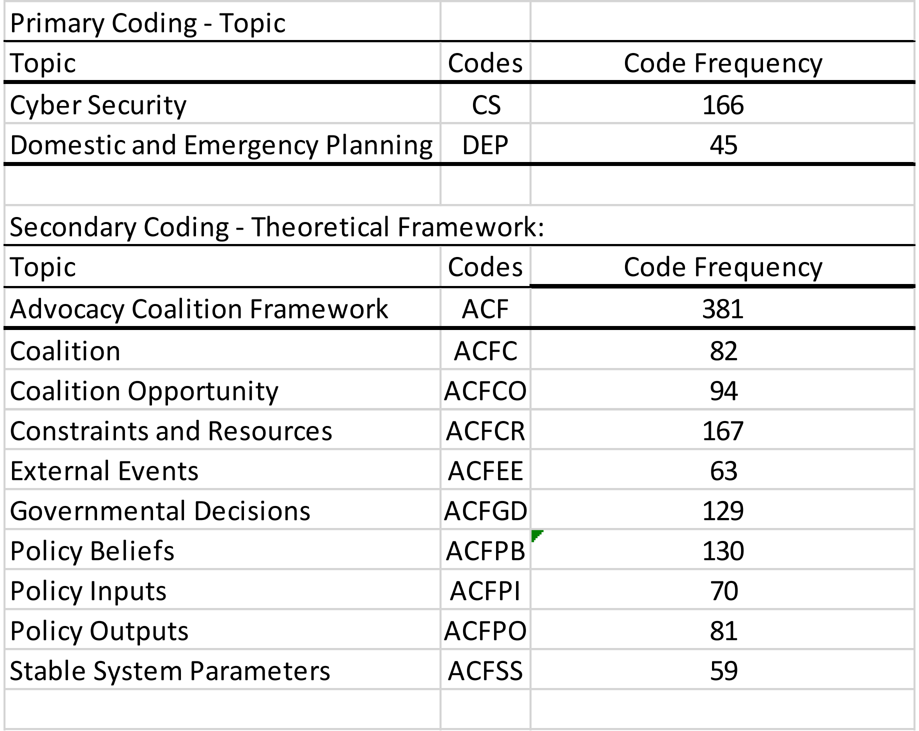
[e-mail address redacted]

Appendix I: Preliminary Coding

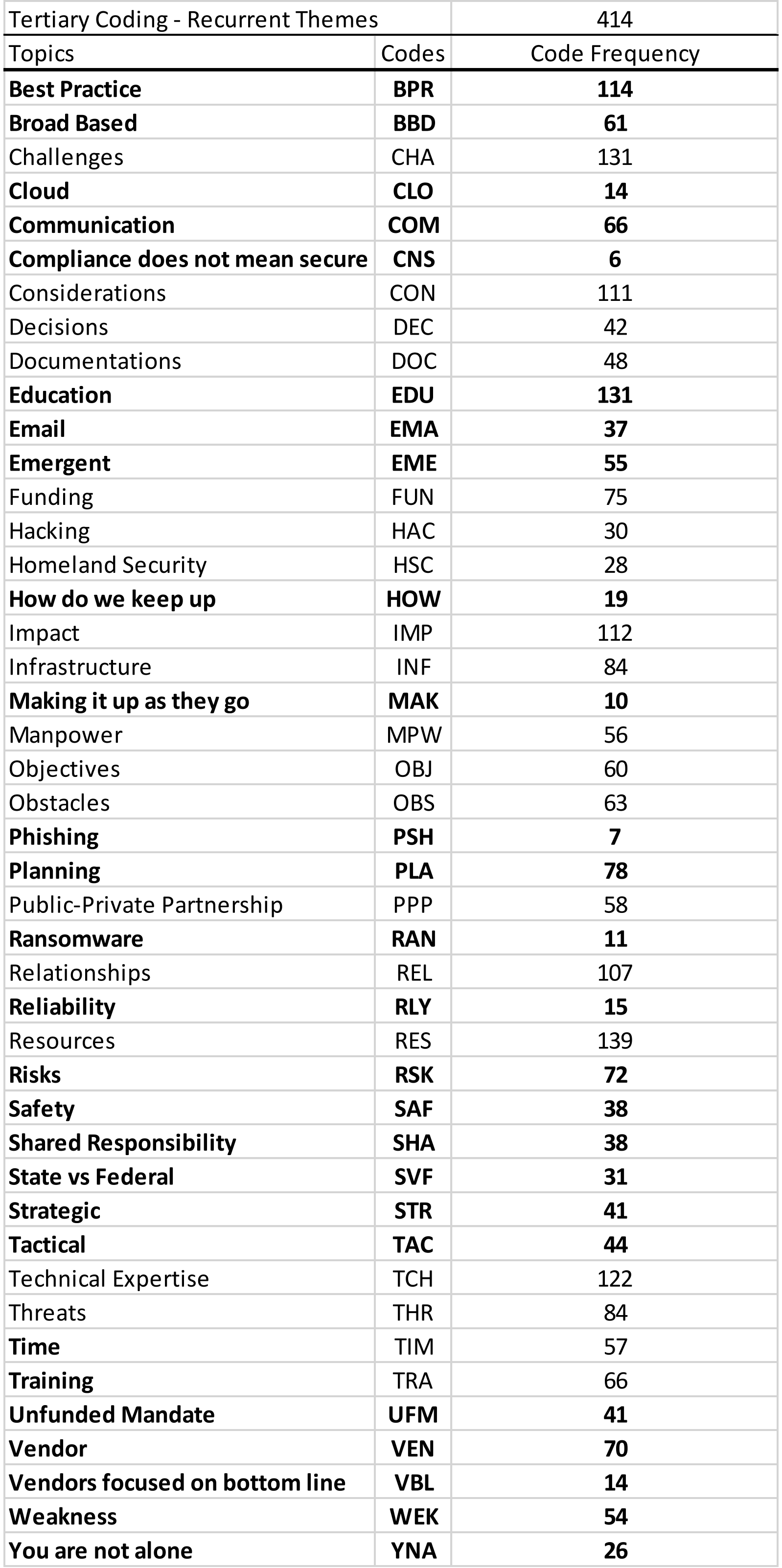


Primary Coding - Topic		
Topic	Codes	Possible Interview Questions
Cyber Security	CS	All
Domestic and Emergency Planning	DEP	1-2, 7, 9, 10, 13-15
Secondary Coding - Theoretical Framework:		
Topic	Codes	Possible Interview Questions
Advocacy Coalition Framework	ACF	5-6, 8, 10
Coalition	ACFC	5-6, 8, 10
Policy Beliefs	ACFPB	1-8
External Events	ACFEE	1,3-5, 8
Stable System Parameters	ACFSS	1,3-5, 8, 11, 13
Coalition Opportunity	ACFCO	5-6, 8, 10
Policy Outputs	ACFPO	2, 4-5, 9, 11-14
Policy Inputs	ACFPI	1-3, 5-8
Constraints and Resources	ACFCR	10-11, 13
Governmental Decisions	ACFGD	1-4, 6-15
Tertiary Coding - Recurrent Themes		
Topics	Codes	Possible Interview Questions
Challenges	CHA	2,5a, 5b, 7-13, 15
Considerations	CON	All
Decisions	DEC	1, 3, 6-10, 11, 13, 15
Documentations	DOC	2-4, 7, 9, 11-12
Funding	FUN	1, 4, 6-7, 10, 13
Hacking	HAC	2, 6, 8, 9
Homeland Security	HSC	All
Impact	IMP	All
Infrastructure	INF	13-14
Manpower	MPW	3, 7, 9-10, 13-15
Objectives	OBJ	7, 9, 12
Obstacles	OBS	All
Public-Private Partnership	PPP	5, 7-9, 13
Relationships	REL	All
Resources	RES	1, 3-4, 7-8, 10-11, 13
Technical Expertise	TCH	6-7, 9-10, 12-13
Threats	THR	All
Unfunded Mandate	UFM	3-4, 7, 9-11, 13

Appendix J: Final Codes and Frequency of Usage



Primary Coding - Topic		
Topic	Codes	Code Frequency
Cyber Security	CS	166
Domestic and Emergency Planning	DEP	45
Secondary Coding - Theoretical Framework:		
Topic	Codes	Code Frequency
Advocacy Coalition Framework	ACF	381
Coalition	ACFC	82
Coalition Opportunity	ACFCO	94
Constraints and Resources	ACFCR	167
External Events	ACFEE	63
Governmental Decisions	ACFGD	129
Policy Beliefs	ACFPB	130
Policy Inputs	ACFPI	70
Policy Outputs	ACFPO	81
Stable System Parameters	ACFSS	59



Tertiary Coding - Recurrent Themes		414
Topics	Codes	Code Frequency
Best Practice	**BPR**	**114**
Broad Based	**BBD**	**61**
Challenges	CHA	131
Cloud	**CLO**	**14**
Communication	**COM**	**66**
Compliance does not mean secure	**CNS**	**6**
Considerations	CON	111
Decisions	DEC	42
Documentations	DOC	48
Education	**EDU**	**131**
Email	**EMA**	**37**
Emergent	**EME**	**55**
Funding	FUN	75
Hacking	HAC	30
Homeland Security	HSC	28
How do we keep up	**HOW**	**19**
Impact	IMP	112
Infrastructure	INF	84
Making it up as they go	**MAK**	**10**
Manpower	MPW	56
Objectives	OBJ	60
Obstacles	OBS	63
Phishing	**PSH**	**7**
Planning	**PLA**	**78**
Public-Private Partnership	PPP	58
Ransomware	**RAN**	**11**
Relationships	REL	107
Reliability	**RLY**	**15**
Resources	RES	139
Risks	**RSK**	**72**
Safety	**SAF**	**38**
Shared Responsibility	**SHA**	**38**
State vs Federal	**SVF**	**31**
Strategic	**STR**	**41**
Tactical	**TAC**	**44**
Technical Expertise	TCH	122
Threats	THR	84
Time	TIM	57
Training	TRA	66
Unfunded Mandate	**UFM**	**41**
Vendor	**VEN**	**70**
Vendors focused on bottom line	**VBL**	**14**
Weakness	**WEK**	**54**
You are not alone	**YNA**	**26**

Appendix K: Demographic Profile for Selected Counties and Localities

Location	Population	Median Income	Median Home Value
State of Tennessee	6,770,010	$48,708	$151,700
Davidson County	691,243	$53,419	$194,800
Giles County	29,401	$43,925	$120,400
Maury County	92,163	$52,080	$156,000
Williamson County	226,257	$103,543	$388,400
Brentwood	42,667	$151,722	$582,800
Columbia	38,266	$41,673	$126,000
Fairview	8,763	$63,125	$191,000
Franklin	78,321	$92,589	$362,300
Nashville	667,560	$52,858	$191,400
Pulaski	7,676	$34,241	$96,200
Spring Hill	39,602	$86,538	$237,700

Data collected from Census data at census.gov/data