UNDERSTANDING THE BARRIERS TO ADDRESSING CYBERSECURITY CHALLENGES IN AMERICAN STATE AND LOCAL GOVERNMENTS

by

Mesut Karakoç

A thesis submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Master of Public Administration

Summer 2017

UNDERSTANDING THE BARRIERS TO ADDRESSING CYBERSECURITY CHALLENGES IN AMERICAN STATE AND LOCAL GOVERNMENTS

by

Mesut Karakoç

Approved: ____
Jerome Lewis, Ph.D.
Professor in charge of thesis on behalf of the Advisory Committee

Approved: ____
Maria Aristigueta, D.P.A.
Director of the School of Public Policy and Administration

Approved: ____
George H. Watson, Ph.D.
Dean of the College of Arts and Sciences

Approved: ____
Ann L. Ardis, Ph.D.
Senior Vice Provost for Graduate and Professional Education

ACKNOWLEDGMENTS

I would first like to express my gratitude to my advisor, Dr. Jerome R. Lewis, chair of my committee, for his advice and helpfulness throughout the process of my thesis. In addition, I would like to thank Troy Mix and Dr. Harvey White for their assistance, support, and encouragement. Thank you for keeping your office doors open and available for all the times when I needed it.

I would also like to acknowledge my loving and supportive girlfriend, Büşra Söylemez as the best supporter of this thesis, and I am gratefully indebted to her for her very valuable comments on this thesis.

I would also like to thank my life saver, Savannah R. Edwards. Thank you for helping me putting pieces together. I will always be in your debt.

Special thanks to my parents and my sister – Tuncer Karakoç, Nermin Karakoç, and Gamze Karakoç. Words cannot express how grateful I am to them for all of the support and sacrifices that they have made on my behalf.

Lastly, my sincere thanks to my best friends from Turkey - Ayhan Önen, Barış Beken, Barış Demirtaş, Ceyhun Çeliktaş, Doğukan Öztürk, Egemen Çetin, Ensar Topaloğlu, Erdi Tuna, Ferhat Altuntaş, Murat Güngör, Murat Yüksel, Onur G. Yıldırım, Özay Özaslan, Tufan E. Beken, and the others. Your deep friendship carried me through this process. This accomplishment would not have been possible without you.

Thank you.

TABLE OF CONTENTS

Chapter

LIST OF FIGURES

ACRONYMS

CIITC	Cybersecurity Investment Incentive Tax Credit
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CTIIC	Cyber Threat Intelligence Integration Center
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DISA	Defense Information System Agency
DoIT	Department of Information Security
DoS	Denial of Service
FFRDC	Federally Funded Research and Development Center
FY	Fiscal Year
IT	Information Technology
NASCIO	National Association of State Chief Information Officers
NCAP	National Consortium for Advanced Policing
NCCOE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OPM	Office of Personal Management
PII	Personally Identifiable Information
PPD-21	President Policy Directive 21
SSN	Social Security Number
US-CERT	United States Computer Emergency Readiness Team
USCYBERCOM	United States Cyber Command

ABSTRACT

We are living in the age of technology and the world is becoming more connected. This changing and dynamic world breeds many needs, including cybersecurity protections. While the federal government focuses on large-scale solutions to cybersecurity challenges, state and local governments cannot wait for the federal government to provide all responses and solutions before taking action. For this reason, states must take precautions to minimize cyber attacks and create a secure cyberspace.

Lack of sufficient funding, inadequate availability of cybersecurity professionals, lack of documented processes, increasing sophistication of threats, and lack of visibility and influence within the enterprise are the main barriers to addressing cybersecurity challenges in United States state and local governments. It is not possible to completely protect the cyberspace by creating a specific framework and applying stable strategies because those attacks and techniques are extremely dynamic. There are known strategies to reduce the effects of cyber attacks, but complete protection is not feasible. Building partnerships with the larger security community and outsourcing security needs, creating a cybersecurity strategic plan, and enabling more law enforcement are crucial steps in addressing cybersecurity challenges. Despite all these precautions, the local and state governments are inevitably going to face cyber attacks. The most important action to take is to develop sophisticated systems for early detection and rapid response to cyber attacks.

Chapter 1

INTRODUCTION

Technological changes and improvements have caused a significant increase in technology use in every stage of our lives. These changes and the usage of IT systems have revealed security problems for government agencies. In this paper, I examine barriers to addressing cybersecurity challenges in state and local governments and discuss what types of strategies state and local governments should adopt to be most effective in enhancing cybersecurity.

The world has been shaped through three major periods of technological improvement. First, the agricultural revolution of the 18th and early 19th centuries increased crop productivity. Second, the industrial revolution initiated fundamental changes in agriculture, textile and metal manufacture, transportation, economic policies and the social structure during the 19th century. Third, the information revolution, currently engulfing us, presages a new way of living (Webster, 2014). This new way of living is characterized by the usage and development of new technologies that are merging information and communication technologies in daily life. Technological changes and improvements have caused a significant decrease in the cost of processing, storing, and transmitting information in all forms (i.e. text, graphics, audio, and video.). According to PwC (2016), one of the largest professional services firms in the world, a terabyte of data storage cost $27 in 2016 whereas the same storage cost $3.5 billion in

1964. In addition, the cost of a Mbps of connectivity was $1200 in 1998 versus $0.63 in 2015.

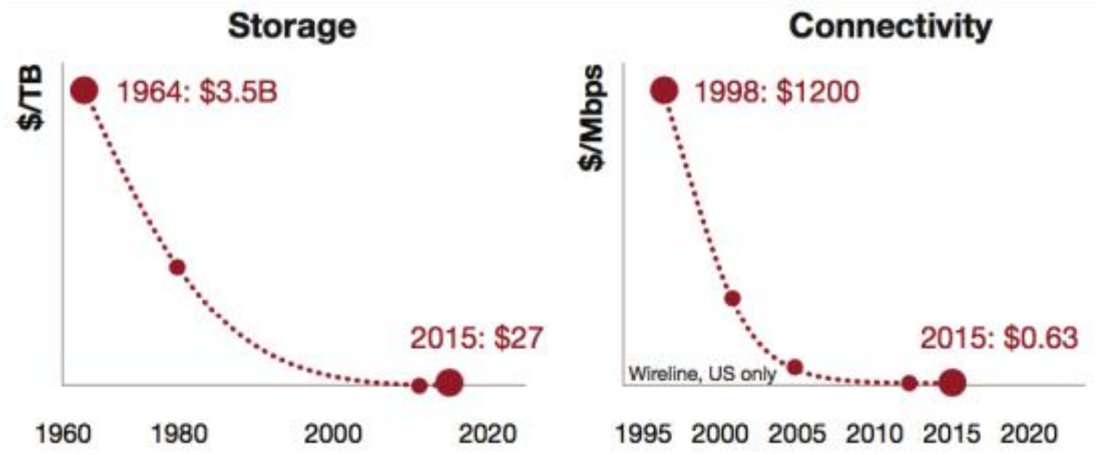

Figure 1.1: Technology costs are plummeting (and the reach is increasing) (PwC, 2016, p.3).

Plummeting technology costs and the development of technologies such as computers, digital communication, and microchips have caused a dramatic increase in the use of technological tools for both personal and organizational needs. This change created a non-physical space called '*cyberspace*'. The word cyberspace was first used in a science fiction novel, *Neuromancer* (1984), by William Gibson. Since then, it has been used by people in many walks of life—ranging from academics to government officials. According to one definition, cyberspace is:

> a new universe, a parallel universe created and sustained by the world's computers and communication lines. A world in which the global traffic of knowledge, secrets, measurements, indicators, entertainments, and alter-human agency takes on form: sights, sounds, presences never seen on the surface of the earth blossoming in a vast electronic night (Benedikt, 1991, p.1).

In this space, people can communicate with each other, save documents, conduct research, or shop. Cyberspace contains objects such as documents, communication exchanges, videos, graphics, and audio, as well as physical space. Organizations have significantly decreased their information transaction time, including the cost of processing and storage.

However, this increased use of cyberspace also causes an increase in security and privacy dilemmas because cyber attackers use this field to achieve their goals, which may include making profit, protesting, or creating an identity in the society. Any device that has a connection to cyberspace, such as a personal computer, a government data server, a computer used by a police officer, and a computer used by a federal agent, can be hacked and is vulnerable. In other words, any organization can be the target of cyber attacks in our age. Technology provides opportunities and conveniences for organizations, but it also augments cyber vulnerabilities. Since cyberspace is home to significant information for citizens, governments, and organizations these vulnerabilities pose significant threats to everybody involved in cyberspace.

Cyberspace, and technological developments within it, are not only used by individuals, but also by government organizations that aim to provide more transparent, accountable, efficient, professional, and ethical public services. All state and local governments have critical information technology (IT) systems which are directly connected to cyberspace. Increased use of cyberspace by government organizations for purposes like critical infrastructure, law enforcement, and human resources management systems can result in security and privacy dilemmas. Technological changes and the usage of IT systems have revealed security problems for government organizations as well as the private sector. While the federal government focuses on large-scale solutions to cybersecurity challenges, state and local government organizations are under pressure in cyberspace.

In Chapter 2, I discuss the transition to the information revolution from the agricultural and industrial revolutions. In this section, I explain the origin of the term ‘cyberspace’. Moreover, I clarify vulnerabilities of state and local law enforcement agencies: Personnel; Information Networks and Systems; Public-Facing Websites; Data Storage Devices; Social Media Accounts; Wireless Devices; Facility Systems and Physical Infrastructure. Next, I describe cyber attackers and provide explanatory accounts of their actions by delving into socio-psychological, economic, and political reasons motivating cyber attacks. Then, I mention a variety of hacking techniques used by cyber attackers to break into government organizations’ systems. Finally, I explain the importance of cybersecurity protection to federal, state, and local governments guided by statistics and research from Deloitte, the National Association of State Chief Information Officers (NASCIO), and Ponemon Institute.

In Chapter 3, I examine the barriers to addressing cybersecurity challenges faced by state and local governments. This examination draws from on the 2016 Deloitte-NASCIO Cybersecurity Study and another research report entitled, “Cybersecurity Challenges to American State and Local Governments.”

Chapter 4 draws insight from a case study investigation of Maryland. The state of Maryland has well-developed practices for cybersecurity planning. Protecting its cyberspace is more significant for the states because it is a home of many government organizations related to national security. The state of Maryland is home to highly relevant cyber resources such as the Defense Information System Agency (DISA), the National Security Agency (NSA), United States Cyber Command (USCYBERCOM), and the National Institute of Standards and Technology (NIST). Even though the state government has recognized that cybersecurity is a vital issue, and it puts significant effort towards protecting cyberspace, it still faces many of the barriers that I discuss in Chapter 3. I argue that the lack of sufficient funding, inadequate availability of cybersecurity professionals, insufficient or under-enforced policies, and governance issues are the most relevant barriers that state and local governments in Maryland face in their attempts to secure cyberspace. In order to provide empirical evidence for my arguments, I use interviews conducted through focus groups that include IT and cybersecurity professionals from the state government and several local governments in the state of Maryland, as well as interviews published through online journals and local news. The most important findings from those interviews are discussed. Lastly, the fact that cybersecurity policies are underdeveloped, even in Maryland, reveals that the dynamic and unpredictable nature of cyber attacks are crucial barriers to implementing sufficient protections. Government officials and IT professionals agree on the significance of cybersecurity, but effective protective mechanisms remain elusive.

My concluding chapter proposes strategies state and local governments can employ to be most effective in enhancing their cybersecurity. This discussion and suggestions draws from literature, recommendations by federal government and NASCIO, and reflections extracted from interviews.

Chapter 2

NATURE OF CYBER RISKS

2.1 Cyber Vulnerabilities

The information revolution ushered in the rapid adoption of technological changes and improvements, causing a significant increase in the usage of electronic devices such as computers and smartphones. With these changes and the advent of the internet, a cyberspace was created which has hosted a new place to communicate online. Online communication is predominantly carried out via social media platforms such as Facebook, Twitter, LinkedIn, Instagram, and Flickr. Even most government agencies, according to Garcia (2016), use these platforms to drive citizen engagement, collect real-time data, transform public perception, maximize awareness of agency goals, and improve the constituent service experience. However, one government official on a social media platform can lead hackers and other bad actors to an entire network of officials. Therefore, social media accounts used by government agencies and officials can also be considered vulnerabilities.

Technology is improving rapidly and new forms of using networks continue to emerge. One of those developments is wireless technology, which gives mobile devices the ability to go where no Ethernet cables exist and still stay connected to the local network or the Internet. Wireless devices have the potential to be exploited because they receive and transmit data, command other systems, and provide information to other systems. Technologies such as radios, mobile-data systems, body-worn cameras, dash-mounted cameras, navigation systems, tactical gear, smartphones and tablets, and body-worn sensors use wireless technology to communicate with each other. In addition, many building management systems such as, water systems, heating and air conditioning systems, elevators, parking garages, lighting systems, security and access control systems, have a wireless component that make them vulnerable. All of those systems are critical to state and local government agencies. Furthermore, the ability to access a network without any physical connection makes it much easier for cyber attackers to do the same, as they don't have to worry about "plugging in" to the cable. Such wireless attacks can even be more effective since security experts identify wireless connections as more vulnerable than cables. Cyber attackers could take control of those facility systems and physical infrastructure because they have wireless components (NCAP, 2016; Shinder & Cross, 2008).

The consequence of these technologies is that as organizations innovate they face an increasing number and variety of cyber vulnerabilities. The National Consortium for Advanced Policing (NCAP) (2016) lists the most important cyber vulnerabilities of state and local law enforcement agencies: Personnel; Information Networks and Systems; Public-Facing Websites; Data Storage Devices; Social Media Accounts; Wireless Devices; Facility Systems and Physical Infrastructure.

One of the greatest contributors to vulnerability is human behavior. Many systems are vulnerable to an insider, someone who has an intent to harm the organization. There are two types of insiders: an accidental insider and a purposeful insider. Accidental insiders are people who make an unintentional misstep or fall victim to a social engineering scheme. For instance, opening or clicking on content in a phishing e-mail might cause the system the person uses to be hacked. Purposeful insiders are people who intentionally target an organization while working as an employee. For example, an employee who did not get a promotion while his/her colleague did could turn an enemy against the organization and use his or her authorization to damage the system.

Information and network systems are one of the most targeted public faces of an agency because of the sensitive data that they usually keep. Some of those information and network systems such as web applications, content management systems, and even database servers are still configured with weak or default passwords. In addition, mobile devices such as, phones, tablets, and unencrypted laptops pose some of the greatest risks to information and network system because people do their personal, or organizational jobs by using those devices. Furthermore, those systems are under the risk of cyber attacks when they have some missing patches and outdated system files. Weak or default passwords, unencrypted electronic devices, and missing and outdated system files are some of the most important cyber vulnerabilities because they are directly targeted by cyber attackers (Beaver, 2013).

When you compare websites viewable only by employees with public-facing websites of agencies, it is clear that public-facing sites are more vulnerable to cyber intrusions if they are directly connected to the rest of the agencies' network assets. Public-facing websites are more vulnerable because they offer e-government services to citizens and they have a direct connection to agencies' networks, which can be used to access servers. In addition, an agency's website that is not connected to the agency's network can be hacked and defaced in order to make a statement or protest. Security configuration of the hosting provider and relationship of the web server to other computer systems in the agency can cause technical vulnerabilities (NCAP, 2016).

Portable data storage and personal devices, such as thumb drives, internal and external hard drives, CDs/DVDs, computers and laptops, and smartphones, can be used to keep critical documents and sensitive information. Those devices can also present a significant security vulnerability if they are compromised or stolen (NCAP, 2016).

2.2 Who are those cyber attackers?

As shown in Figure 2.1, cyber attackers are categorized within 2 main categories: (1) Outsiders, and (2) Insiders. Insiders act from within the organization, while Outsiders attempt to penetrate it from the outside.

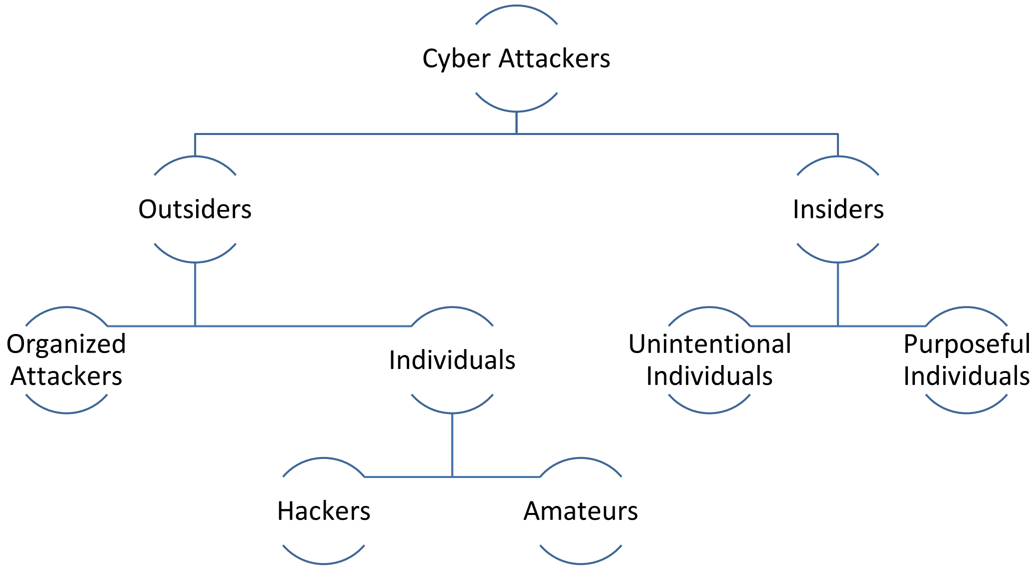

Figure 2.1: Categories of cyber attackers (adapted from Han and Dongre, 2014, p.40)

There are two types of outsiders. First, organized attackers are the larger part of outsiders. Terrorists, hacktivists, state actors, and criminal groups are organized attackers. Terrorists are members of extremist and radical groups that use cyberspace to spread propaganda, attack systems of their political enemies, and steal money for their cyber or real-life activities (Gandhi et all, 2011). Hacktivists use hacking techniques to disrupt services and bring attention to political and social issues. State-sponsored military or intelligence services, groups, and individuals are acting on behalf of foreign governments. These state-sponsored actors pose a threat to state and local law enforcement in the United States and have executed successful attacks (NCAP, 2016). Criminal groups target agencies by infecting computers with ransomware which encrypts files until the agency pays a specified amount, or ransom, to decrypt them again. In addition, there are many criminal organizations conducting credit card fraud.

Second, individual hackers are also categorized as outsiders. These individual attackers are dependent on their own hacking skills, which can run from extremely advanced to the very basic. As shown in Figure 2.1, they are divided into two categories, hackers and amateurs. Individuals that have extremely advanced hack skills are called hackers. Hackers use their creativity to overcome limitations of software systems and develop programs and scripts to break systems, in addition to finding security flaws. On the other hand, amateurs, generally called “lamers”, “script kiddies” (NCAP, 2016), or “noobs” (Han and Dongre, 2014), are less-skilled individuals that modify existing computer scripts, or codes. Those people use existing programs, scripts, and instructions that can be found on the internet because they lack the expertise to create their own.

Insiders can be categorized under two labels, unintentional (accidental) individuals and purposeful individuals. On the one hand, accidental insiders who are unaware they have become the organization’s weakest link in the cyber chain. In other words, cyber attackers use employees lack of awareness to break into the computer network; those accidental insiders are indirect cyber attackers. On the other hand, purposeful individuals, employees, or contractors who intentionally cause harm to an organization by using permission such as database access given by the organization while working as a part of the organization. According to NCAP (2016), insiders may well be the most dangerous threat to state and local law enforcement agencies. Knowing the categories of cyber attackers helps us to understand the intentions behind their actions.

2.3 Why do cyber attackers attack?

There are three main reasons why hackers attack: (1) Socio-psychological reasons, (2) Economic reasons, and (3) Political reasons. Money is not the only motivator for hackers. Moreover, socio-psychological reasons can be the strongest motivating factor in some cases.

2.3.1 Socio-psychological Reasons

According to Shinder and Cross (2008), "many criminal offenses are committed out of emotional reasons: anger, rage, or revenge for real or imagined wrongs," (p. 95) or to satisfy their egos and show their abilities to others in the cyberspace. Other socio-psychological reasons also include entertainment, curiosity, desire for publicity, retribution, notoriety, misguided intentions to help someone, and attention seeking (Cross, 2008; Han and Dongre, 2014; NCAP, 2016). For instance, when considering hackers, one may not initially think of "the high school hacker who does not want his girlfriend to flunk calculus and have to go to summer school, so he breaks in to the school's computer system and changes her grade from an F to a C" (Cross, 2008).

2.3.2 Economic Reasons

Economic incentives are significant motivators for criminal organizations to break into financial institutions. Information ranging from personal records to case files on a law enforcement system is critical for malevolent people, as well as individuals and organizations. There is a significant private market for critical individual and organizational information. For this reason, “economic situations and personal or corporate financial greed often (serve as the primary) motives for cyber attackers [and] Cyber mercenaries and organized cartels also operate in cyberspace” (Gandhi et all, 2011). Economic incentives may also include theft of intellectual property or other economically valuable assets such as funds, and credit card information; fraud; industrial espionage and sabotage; blackmail; and tax records (Han and Dongre, 2014). In addition, an attack for profit often aims to lock the system and hold it hostage until a ransom is paid to return information, restore a system, or provide a new password. This is an example of a ransomware attack (NCAP, 2016).

2.3.3 Political Reasons and Hacktivism

The motivation behind hacking for political reasons can differ on a case-by-case basis. Some cybercriminals can be members of extremist and radical groups that use cyberspace to spread propaganda, attack systems of their political enemies, and steal money for their cyber or real-life activities (Gandhi et all, 2011). Others can use hacking as a tool for internet or online activism called Hacktivism. Loewengart (2012) defines hacktivism as an act of hacking, or breaking into a system, for a politically or socially motivated purpose. These perpetrators are called hacktivists. A hacktivist uses the same tools and techniques as a hacker but does so in order to disrupt services and bring attention to a political and social issue. In some cases such as a fight for social justice, human rights, and equality, political reasons for hacking may be considered ethical. For instance, in 2015, a group of cyber attackers temporarily prevented access to the State of

Indiana’s website to protest the governor’s signing of a controversial “religious freedom” bill. Many people exemplify this case as an illegal-but-ethical cyber attack because, according to those people who discuss the case in online platforms, attackers did not cause any lasting harm to the system.

These three motivations also demonstrate the evolution of process, in terms of the reason for hacking. Initially, hacking was a way to show strength or ability. In other words, in the past hackers may have attacked the systems to satisfy their egos or to show their abilities to others. However, currently, there are many reasons why hackers want to hack or attack a system. Early on, hackers attacked the systems as a means of boosting their ego, but after a while, they were making money from these attacks. Hacking can also be utilized as a protest tool, or a means of presenting a risk for socio-political issues.

2.4 Hacking Techniques

Hacking techniques have become more complex and sophisticated with technological development. Barber (2001) states that “the tools and techniques employed by hackers are extremely complex, utilizing a broad range of technologies. The number of mechanisms for breaking into systems, whatever the objective, is on the increase with new tools emerging continuously” (p.1). Some major hacking techniques used by cyber attackers include: Social engineering; Denial of Service (DOS) Attacks; Ransomware; Zero-day attacks; Phishing and other related variants.

Social engineering is one of the most widely used techniques used by cyber attackers. McQuade (2006) defines social engineering as the act of manipulating people into performing actions. Cybercrimes are not always thought of in terms of purely technical exploits (McQuade, 2009, p.168). People use social engineering to take advantage of people in order to obtain valuable information by using their ability of persuasion instead of technology alone. In other words, attackers obtain, or divulge personal information from someone by using his or her psychological manipulation ability. For instance, an attacker might use his social skills to obtain a government official's pet's name, favorite book, or favorite historic person which are generally used for resetting a password.

Kevin Mitnick, a formal cybercriminal and current security expert, explains how social engineering is critical for cybercriminals in his book *The Art of Deception*. He adds that people are the weakest link when it comes to security information. He confesses that many of his exploits were based on social engineering (Mitnick, 2012). A cybercriminal conducts research and collects intelligence on the target in order to discover security weaknesses after identifying the people, facilities, or information systems to be attacked. Then, the cybercriminal develops a rapport with the person who controls the targeted system to manipulate him or her into committing one or more crimes (McQuade, 2009).

McQuade (2009) started by citing Donn Parker, a computer security expert, who said that "effective social engineering techniques involve one or more of the following:

- Using appropriate, often official-sounding jargon, such as that used by a specific company or agency.
- Mentioning, or ''name dropping,'' persons in authority in such a way as to imply relationships with that party.

- Reading online bulletin boards and the like as a means of gathering intelligence on a victim or victims.
- Reading initial log on screens to learn basic contact information, such as help desk numbers.
- Mixing lies and truths to make requests seem more plausible.
- Exaggerating or minimizing the importance of receiving certain information.
- Asserting authority, ‘‘pulling rank,’’ or pretending to be someone in authority.
- Using intimidation and threats to manipulate subjects.
- Using praise, sympathy, and flattery to manipulate subjects.
- Repeatedly causing false alarms in order to get a subject to disable security safe guards” (p.169).

DoS and Distributed Denial of Service (DDoS) attacks are other common cyber attack techniques. According to the United States Computer Emergency Readiness Team (US-CERT) (2009), a DoS attack is a technique which prevents legitimate users from accessing information or services, whereas a DDoS attack is a technique which is used for controlling many computers in the same time to attack another computer system. A DoS attack may be able to prevent someone from accessing email, database systems, human resources systems, websites, and other services that rely on affected computer. A DDoS attack may be able to make the system non-functional for a certain period of time by sending a huge amount of data to a computer system. The attack is "distributed" because the attacker is using multiple computers that are hacked by the attacker, called zombies, to launch the DoS attack. Cyber attackers generally see these two techniques as a protesting tool and use them for hacktivism.

Ransomware is a harmful software that prevents organizations and users from accessing their computers or data, until the owner agrees to pay a ransom. In other words, it locks the computer or files, notifies the user of its presence, and requests payment (Mehmood, 2016). Ransomware is a relatively new technique for cyber attacks. Symantec (2016) first reported this type of attack in 2010 and blocked 100 million tech-support scams in the year 2015 alone. According to Lorhmann (2017), the number of ransomware attacks has grown by at least 50% in 2016. Even though the technique would seem to rely more on presumably more well-resourced private companies, Lorhmann says that private companies are less likely to pay the ransom. That is why cybercriminals have now begun to change their tactics and target government agencies. For instance, Jack Danhy, the former director of advanced security for IBM and a frequent writer and speaker on security and security issues, answers Lorhmann's question, "*What are some of the biggest ransomware incidents that you have seen affecting governments?*" by giving examples of ransomware attacks on government organizations. He says:

> In the Bingham County, Idaho, example, the attackers didn't rely on a traditional phishing attack or malicious link; they actively infected the system using brute force attack to gain access, then deployed a rapidly spreading version of ransomware that corrupted multiple systems, forcing the county to pay ransom on the few that could not be recovered (para.13).

He adds:

> Looking at their impacts, we have seen several that have actually shut down government services, like the example in Bingham County, another in Licking County, Ohio, and multiple events against police departments in places like

> Texas, Massachusetts, and even Washington, D.C. About a year ago, Department of Homeland Security (DHS) described the seriousness of this issue for the federal government in their response to a Senate request for information on ransomware's impacts (para.15).

Based on the given examples and predictions by security experts, it can be said that ransomware attacks have been affecting government organizations, and ransomware attacks will remain a very significant threat for government organizations in the future.

Phishing (pronounced the same as “fishing”) is another common technique used by cyber attackers, and is also a variation of social engineering. McQuade (2009) states that “phishing is a type of social engineering that cybercriminals use when attempting to deceive potential victims into revealing private information about themselves or their computer accounts, such as usernames, passwords, and financial or bank account numbers” (p.139). These types of cyber attackers typically use e-mail to acquire information from the recipient. For instance, a cyber attacker could send an e-mail to all the employees of a government agency asking employees to renew their e-mail passwords by sending a “fake” e-mail which may appear similar to the original password renewing link. If the employees are not educated enough to understand whether the e-mail and the link are fake or not, they could try to log into the fake system. After they type in their current password, it automatically sends that information to the attacker. Phishing is also used for identify theft.

2.5 How big is the cybersecurity problem?

Cybersecurity has become of the most significant challenges facing the world. Refsdal, Solhaug, and Stølen (2015) state that “cybersecurity is the protection of cyber-systems against cyber-threats”. It is one of the most significant issues facing the nation today because we are living in the age of technology and this is an increasingly-networked world. According to Bucci, Rosenzweig, and Inserra (2013), cybersecurity threats damage society’s critical infrastructure, limit the freedoms that Americans exercise online, and stifle the economic vitality of U.S. business.

Ponemon Institute conducted a study called *2016 Cost of Cyber Crime Study & the Risk of Business Innovation* in order to quantify the annual cost of cybercrime. The study is based upon a representative sample of 237 private organizations operating in six different countries. This study show the economic impact of cyber attacks and observes associated cost trends over time. According to the study, in 2016, US organizations have the highest average cost associated with cybercrime attacks, which is $17,360,000 per organization.

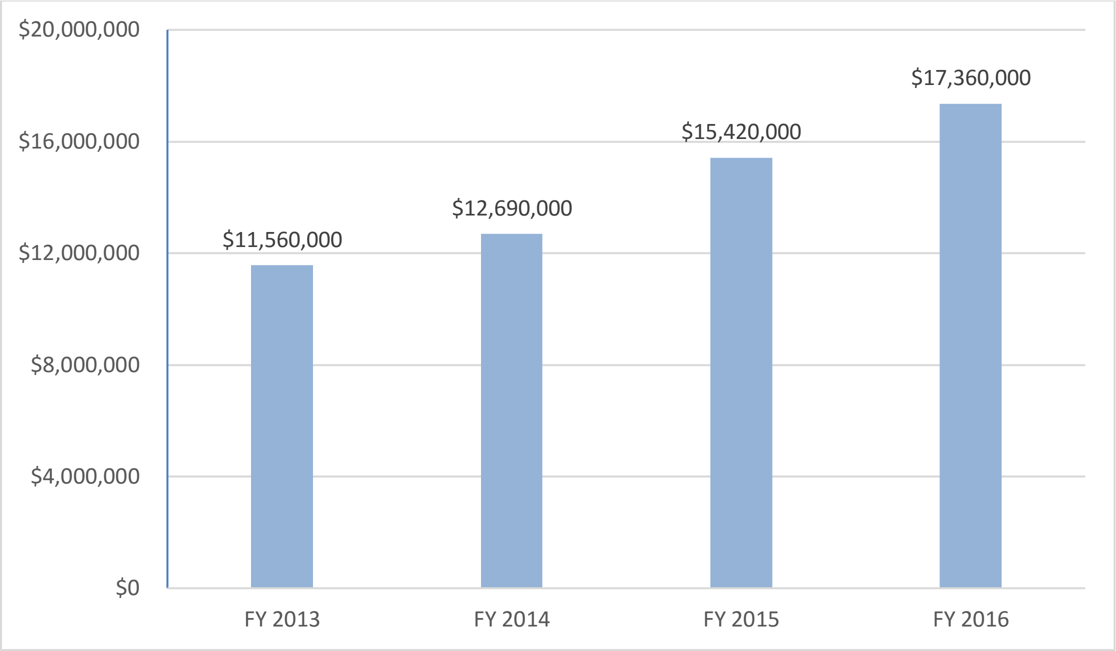

Figure 2.2: Avarage cost of cybercrime per company in the United States (adapted from Ponemon Institute, 2016, p.4).

Figure 2.2 presents the estimated average cost of cybercrime for companies operating in the US over a four year period. The figure illustrates that the average cybercrime costs to individual companies in the United States have increased from $11,560,000 in fiscal year 2013 to $17,360,000 in fiscal year 2016, an increase of 50.2%.

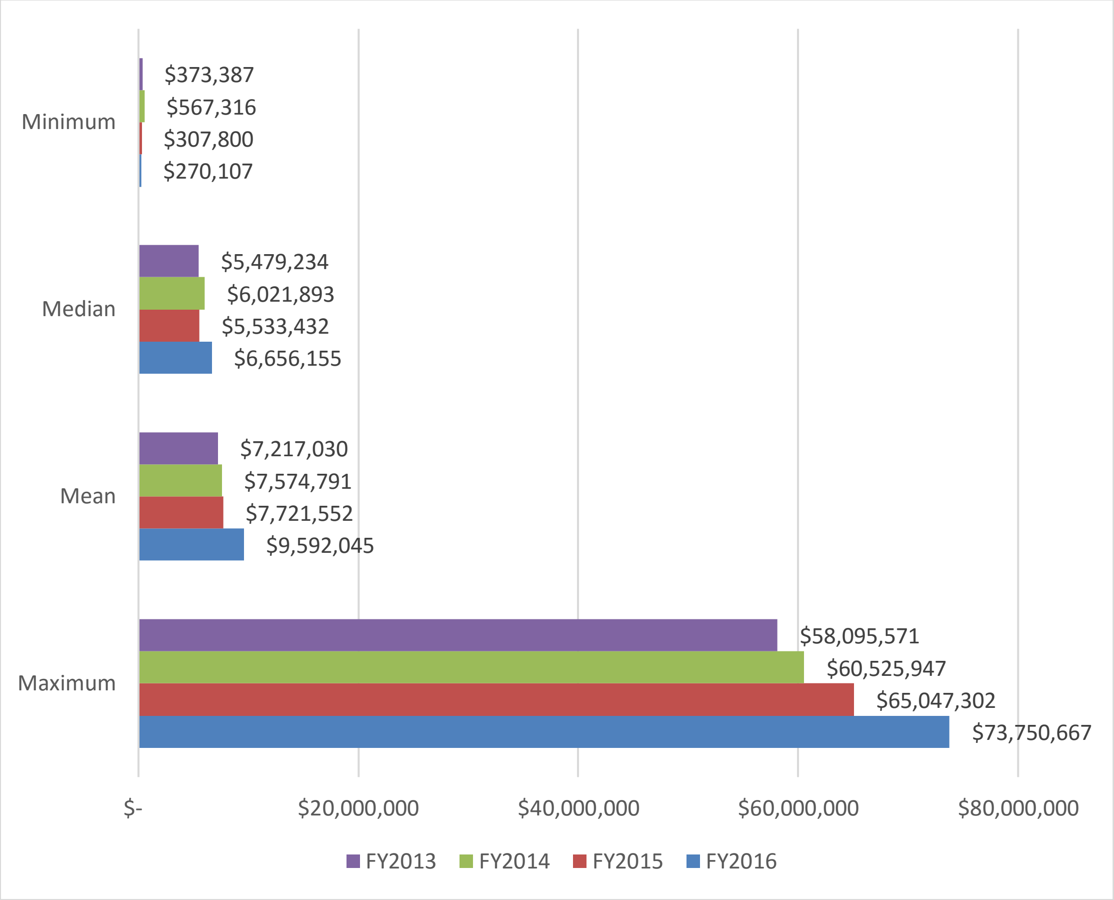

Figure 2.3: Global cost statistics of cybercrime (Ponemon Institute, 2016, p.5)

As shown in Figure 2.3, the total global annualized cost of cybercrime in 2016 ranges from a low of $270,107 to a high of $73,750,667 per company. The median annualized cost of cybercrime in the benchmark sample is $6.7 million—a slight increase from $5.5 million in 2015. The mean value is $9.5 million. An increase from 2015's mean of $7.7 million.

The data from figures 2.2 and 2.3 demonstrate that average cost of cybercrime per company in the U.S. ($17,360,000) is significantly higher than the global average cost per company ($9,592,045).

Cybersecurity Ventures, a firm that provides research and reports on cybercrime costs, conducted an inquiry into the cybersecurity market size. The study shows that cybersecurity market size, which consists of spending forecasts, cybersecurity jobs, and global annual cybercrime costs, will grow from $3 trillion in 2015 to $6 trillion annually by 2021 (Morgan, 2016).

The research noted above clearly shows that the economic cost of cybercrime has been significantly increasing, and that the U.S. has the highest average cost of cybercrime per organization. One example of such an attack was targeted at OPM. OPM discovered two separate but related cybersecurity incidents that have impacted the data of the federal government employees, contractors, and others. According to OPM (2015):

> Earlier in 2015, OPM discovered that the personnel data of 4.2 million current and former Federal government employees had been stolen. This means information such as full name, birth date, home address and Social Security Numbers (SSNs) were affected. In addition, in June 2015, Office of Personal management (OPM) discovered that the background investigation records of current, former, and prospective Federal employees and contractors had been stolen. OPM and the interagency incident response team have concluded with high confidence that sensitive information, including the Social Security Numbers of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, primarily spouses or co-habitants of applicants. Some records also include findings from interviews conducted by background investigators and approximately 5.6 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen (para 1-3).

Not only do cyber attacks have grave economic costs associated with them, but they also negatively affect the effectiveness and quality of governmental decisions. The US federal government urges the implementation of three principles for a state government: transparency, participation, and collaboration. According to the White

House (2009), “public engagement enhances the Government’s effectiveness and improves the quality of its decisions” (para. 8). Participation encourages public engagement by increasing opportunities for the public to be involved in policy making and to provide the government with the collective knowledge, ideas, and expertise of the population (Chun et al, 2010).

Trust in government is perhaps the most important variable for increased participation. Hacking public-sector information diminishes citizens’ trust in organizations (Deloitte, 2016). The government has to protect the cyberspace and take precautions to increase its effectiveness and improve the quality of its decisions.

A highly safe cyberspace is critical for high-ranking government officials, government employees, and citizens and private companies. The U.S. federal government has outlined guidelines for precautions and protections concerning cybersecurity issues. For instance, President Obama (2015) stated at the White House Summit on Cybersecurity and Consumer Protection, “We have to build stronger defenses and disrupt more attacks. We have to make cyberspace safer. We have to improve cooperation across the board...not just here in America, but internationally” (para.36). In 2015, the federal government developed new policies and capabilities to identify, defend against, and counter malicious cyber actors such as

- the President directed the formation of the Cyber Threat Intelligence Integration Center (CTIIC),

- the Secretary of Defense released the new Department of Defense Cyber Strategy to guide the development of the U.S. military's cyber forces and strengthen the United States' cyber deterrence posture,
- the President issued Executive Order 13694 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities),
- and the President sent to Congress a new cybersecurity legislative proposal that included modernization of law enforcement tools to fight cybercrime.

In addition, according to the Cybersecurity National Action Plan (2016), released by White House, Office of the Press Secretary, the federal government plans to "invest over $19 billion for cybersecurity as part of the President's Fiscal Year (FY) 2017 Budget. This represents a more than 35% increase from FY 2016 in overall Federal resources for cybersecurity" (p.10).

Moreover, in 2013, the White House released Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience; this directive identifies 16 critical infrastructure sectors that are vital to the United States. Their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The 16 critical infrastructure sectors identified in PPD-21 are: Chemical; Commercial facilities; Communication; Critical manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities, Healthcare and Public

Health, Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems (The White House, 2013).

Even though the federal government has made it clear that cybersecurity is one of the most important challenges facing the nation, and taken some precautions, it is not enough to protect its citizens and critical infrastructure because these attacks are getting more localized, sophisticated, and individualistic. Precautions taken by the federal government could be very general in some cases, such as the protection of local infrastructure. However, state and local governments have increasingly noticed that they are the new targets of cyber attacks. In recent years, they have had to contend with increasing numbers and sophistication of cyber attacks. According to a study by the Center for Digital Government (2014), government agencies have lost more than 94 million citizens' records from 2009 to 2013, with each lost record representing a cost of $194. These attacks were directly targeted at state and local governments.

Of particular concern is that all U.S. elections are run by state and local governments. Across these many governments, elections use different types of voting equipment, with some making use of electronic devices and others using paper ballots to record votes. Whether the actual mechanism of voting is electronic or not, all state and local governments have a voter database which contains voter information. These electronic databases and electronic voting devices are significant targets for cyber attackers.

While cybersecurity activity garnered significant attention during the 2016 election, the largest cyber attack on a state agency in America's history happened to the

Revenue Department of South Carolina in 2012. It resulted in the theft of 3.8 million SSN and 387,000 credit and debit card numbers. In addition, the information of 1.9 million dependents and 700,000 businesses was stolen (Brown, 2012). Two days after this major data breach was recognized, the state of South Carolina signed a $12 million contract to work with an information services company to provide a year of credit monitoring and call center support for taxpayers.

Moreover, in March 2012, the hackers broke into a Utah Department of Technology Services computer server that stores Medicaid and CHIP claims data. There were 780,000 people whose SSNs, names, dates of birth, addresses, diagnosis codes, national provider identification numbers, provider taxpayer identification numbers, and medical billing codes were stolen by the hackers (Utah Department of Health, 2012).

In November 2016, international hackers called Cryptom27 hacked the transportation system of San Francisco. The hackers left a brief message on Muni ticketing systems: “You Hacked, ALL Data Encrypted.” However, they let passengers allow to get free rides rather than shutting down the network. The hackers left an e-mail address in their note. When the authorities contacted them, they said that all payment kiosks, internal automation systems and emails were compromised. They threatened to leak 30GB of the Municipal Transportation Agency's databases and documents, including employees' and customers’ contracts if the organization didn't accept to pay 100 Bitcoin, worth roughly $73,000 (Fox-Brewster, 2016). The authorities said they refused to pay the hackers. They eventually fixed the system by using their backup data. After two days, everything was back to normal. However, why the hackers have not leaked the data since the agency did not make a payment is still debated. These examples show that cyber attacks are getting more sophisticated and targeting state and local government agencies.

NASCIO has conducted a survey of state chief information officers (CIOs) to identify and prioritize the top ten policy and technology issues facing state governments since 2006. According to Lipman (2015), state and local governments are under tremendous pressure to secure critical data, infrastructure and services while the federal government works on big-picture solutions. In fact, state CIOs have ranked cybersecurity as their top priority since 2014, one year after PPD-21 was released.

Companies, governments, and social media tools we are using know all about our private lives once we disclose important, personal information which is a significant target for cyber attackers. For example, if a person wants to insure their car, they have to give their names, birth dates, social security numbers, income status, health status and many other details to an insurance company. Hence, companies and governments have large databases of sensitive personal information. This data is not only significant to every citizen, but also it is very valuable to companies in the advertising sector.

According to the 2014 Deloitte-NASCIO Cybersecurity Study, “within just the past few years, a number of high-profile attacks on states have resulted in loss of Personally Identifiable Information (PII) of millions of citizens, including SSNs, payment card records, dates of birth, driver’s license numbers, and tax data”. In addition, according to Levinson (2012), “Personal information is the currency of the underground economy” (para.6). In other words, hackers can sell it to a variety of buyers, including identity thieves, organized crime rings, spammers and botnet operators. The data that are sold by hackers are getting bigger and more public every day. Hackers are charging reduced prices for PII such as names, addresses, and social security numbers because of an "oversupply…from numerous data breaches” (Kharpal, 2015, p.4).

According to Abelson and Goldstein (2015), the personal information of tens of millions of Anthem’s (one of the nation’s largest health insurance companies) customers and employees, including its chief executive, was stolen by hackers. This data is being sold on the dark web. This sensitive personal information is not only used for making profits, but also to do other things such as serving time in jail with your identity or filing tax returns under your identity.

For all the reasons mentioned above, cybersecurity has become a serious issue that needs to be addressed at the state level as well. The precautions taken by the federal government are not sufficient by themselves, as the attacks continue to pose threats to the U.S. citizens’ daily lives. Therefore, state governments should improve their cyber defenses.

In the following chapter, I will discuss the barriers to addressing cybersecurity challenges in the state and local governments based on scholarly and professional literature, with particular attention paid to comprehensive research summarized in the 2016 Deloitte-NASCIO Cybersecurity Study.

Chapter 3

BARRIERS IN ADDRESSING CYBERSECURITY CHALLENGES

In this chapter, I discuss the top barriers to addressing cybersecurity challenges for state and local governments based on a comprehensive research report, the 2016 Deloitte-NASCIO Cybersecurity Study, done by Deloitte, and another research report entitled, Cybersecurity Challenges to American State and Local Governments[1]. State and local government strategies for protecting cyberspace are different from those of the federal government. While the federal government focuses on big-picture solutions to cybersecurity challenges, state and local government organizations are under pressure to protect critical data, infrastructure, and services. I will focus on the obstacles that local and state governments face in addressing cybersecurity challenges. After discussing these two research papers, I will explain the importance of each barrier.

According to the 2016 Deloitte-NASCIO Cybersecurity Study, a survey answered by 98 state business and elected officials, there are 5 major barriers in addressing cybersecurity challenges:

- Lack of sufficient funding.

[1] Cybersecurity Challenges to American State and Local Governments is a research done by Donald Norris, Anupam Joshi, and Timothy Finin from University of Maryland.

- Inadequate availability of cybersecurity professionals.
- Lack of documented processes.
- Increasing sophistication of threats.
- Lack of visibility and influence within the enterprise.

As Figure 3.1 shows, according to the survey data, lack of sufficient funding (80%), inadequate availability of cybersecurity professionals (51%), lack of documented processes (45%), increasing sophistication of threats (45%), and lack of visibility and influence within the enterprise (33%) put state governments at risk. Those barriers are the major sources of cybersecurity problems facing state and local governments.

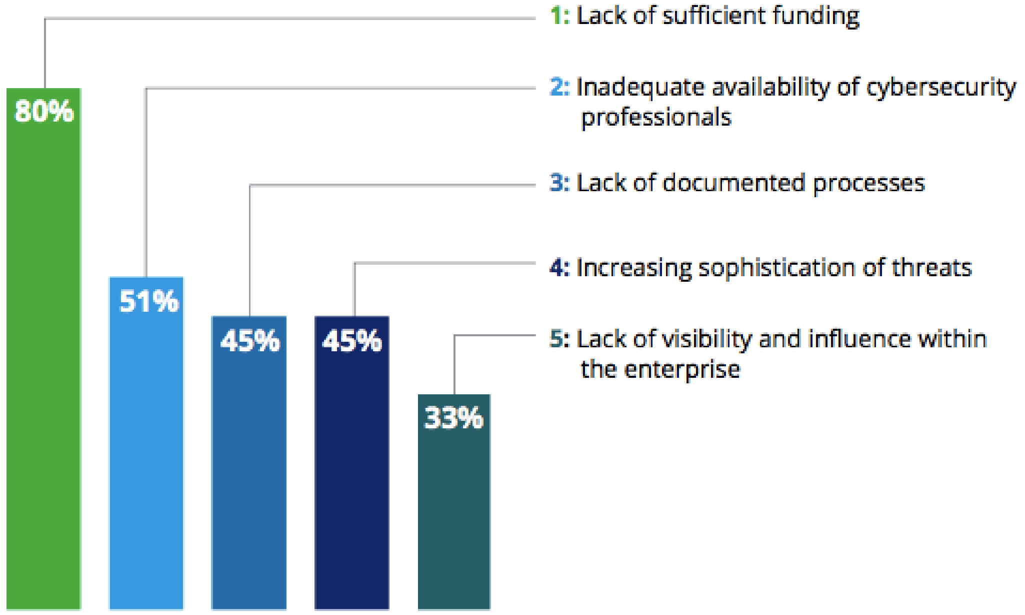

Figure 3.1: Five major barriers in addressing cybersecurity challenges (Deloitte, 2016, p7).

In addition to the 2016 Deloitte-NASCIO Cybersecurity study, there is a research project called *Cybersecurity Challenges to American State and Local Governments* done by Donald Norris, Anupam Joshi, and Timothy Finin from University of Maryland. They conducted a focus group in late 2013 that include IT and cybersecurity professionals from the state governments and several local governments in the state of Maryland. According to their research, there are 3 major barriers that state and local governments face in the area of cybersecurity:

- Insufficient funding and staff.
- Governance and federation.
- Insufficient or under-enforced cybersecurity policies.

Based on those two reports, I will discuss the most important barriers that state and local governments face in more depth below.

3.1 Lack of Sufficient Funding

Insufficient funding to combat cybersecurity issues is not a new concern for state and local governments. Dan Lohrmann (2017c), former chief information security officer (CISO) of the state of Michigan from 2002 to 2009, states that funding was always a problem in his days as the CISO. He said that it is very important to know how you spend the funding you have because the budget is limited.

According to 2016 Deloitte-NASCIO Cybersecurity Study (2016), 80 percent of state CIO’s surveyed indicated a lack of sufficient funding as their number one challenge in cybersecurity. Moreover, Greg Garcia (2016), the executive vice president at Signal

Group DC, states that most states budget between 0-2 percent of their overall budget for cybersecurity matters, compared with an average of more than 10 percent in large companies. For example, according to Mark Raymond, the state of Connecticut’s CIO, only about 1 percent of the state’s IT budget goes to cybersecurity (Bergal, 2017). Garcia (2016) adds, according to one DHS tally, only 30 states and 2 tribal territories spent a total of $27.3 million on cybersecurity with homeland security grants over a four-year period from 2011-2014.

Even large companies that spend approximately 10% of their overall budget on cybersecurity have been successfully hacked. Most of the state and local government agencies have technology older and less secure than those prominent enterprises. Furthermore, those agencies spend less than 2 percent of their budget on protecting themselves and remediating cybersecurity attacks. Those government organizations are faced with just as many security challenges as private companies. For this reason, it is alarmingly clear that state and local agencies’ cybersecurity efforts are woefully underfunded (Lipman, 2015).

State and local governments have been let down by the security industry. Cybersecurity has become too complex for state and local government agencies. As Lipman (2015) mentions, “multiple products from multiple vendors don’t readily integrate and require prohibitively expensive installation and ongoing management.” (para. 10). Because the field of technology and security is very dynamic. Every single exploit or security hole requires a new update, which requires updated technology and more money. A typical state or local government agency doesn’t have the budget to effectively deploy and maintain all the required components to protect itself sufficiently.

3.2 Inadequate Availability of Cybersecurity Professionals

In addition to budgetary concerns, state and local government organizations face a severe shortage of cybersecurity personnel. Two out of three states admit that their IT initiatives are hindered by a lack of qualified candidates. Furthermore, 85% of states cannot fill available IT positions. In addition, nearly 92% of states acknowledge that this shortage results from low salary rates and pay grade structures. It is very hard for a state or local government agency to compete with a private company in terms of IT professionals’ salary. For instance, state officials in Michigan report that their cyber salaries run about 20% below market rate. Private sector firms can offer salaries that are $25,000 higher than those paid by state governments. Cybersecurity experts are commanding top dollar, typically $120,000 and up, in the private sector. (NASCIO, 2015; Stone, 2014).

According to 2016 Deloitte-NASCIO Cybersecurity Study (2016), 51% of state CIO’s surveyed in the research indicated that there was an inadequate availability of cybersecurity professionals. As previously mentioned, there is a shortage of cybersecurity professionals, and by 2019 that gap will grow to reach 1.5 million (Morgan, 2015). The shortfall will have a direct impact on state and local governments. The size of the shortage of cybersecurity professionals is roughly proportional to the cyber attacks and data breaches because state and local governments spend more money to hire IT professionals when they face cybersecurity problems, rather than preemptively. As a result, lack of cybersecurity professionals is one of the most critical cybersecurity risks.

3.3 Increasing Sophistication of Cyber Threats

As discussed in Chapter 2, cyber attacks have become more sophisticated and they are targeting state and local government agencies. Those attacks are getting more sophisticated because the tools and techniques employed by hackers are extremely complex and utilize a broad range of technologies.

According to Senator Gary Peters (2017), a member of the Homeland Security and Governmental Affairs Committee, “our nation is facing an ever-growing threat from increasingly sophisticated cyber attacks, and we are only as strong as our weakest link.” (para.2). He also thinks that “state and local governments face unique cybersecurity threats that can endanger critical infrastructure, as well as residents’ sensitive personal and financial data.” (para.2). Moreover, according to the 2016 Deloitte-NASCIO Cybersecurity Study (2016), 45% percent of state CIO’s surveyed in the research indicated they believed that there was an increasing sophistication of cyber threats.

Cyber attacks are not only getting philosophically sophisticated such as improvements in social engineering techniques, discussed in Chapter 2, but also becoming more technically sophisticated and harder to detect. Rob Kraus, the director of security research and strategy at NTT Security says that “…the intensity and sophistication of these attacks are on the rise. Hackers are shifting their strategy from widespread attacks to a more focused effort to compromise specific targets they can leverage, opening the door for more malicious and potentially lucrative actions." (NTTSecurity, 2017, Para. 2).

As a result, changes and improvements in technology, such as the growth in web applications and compliance requirements, have added on to the complexities that state and local governments face. Cybersecurity is more than just safeguarding your network as it also requires securing data and users.

3.4 The Challenge of Governance

One of the most important barriers to addressing cybersecurity challenges in the state and local governments is the issue of governance. All state governments consist of three branches: executive, legislative, and judicial. These three branches are mostly separate, even though there are some exceptions such as county governments. By the nature of the organizational structure of state governments, comprehensive IT departments are located in the executive branch. This organizational structure causes some governance problems in terms of implementing cybersecurity policies.

According to Norris et al. (2015), there are four reasons for the governance problem in the sense of cybersecurity. First, state and local governments are federated among executive, legislative, and judicial branches. IT departments do not have authority over the legislative and judicial branches because they are generally located in the executive branch. Second, there are some departments or units such as police departments that have "special protection" and remain outside of the purview of IT departments. IT professionals are not allowed to access to the classified information protected by those special departments. Although it is crucial for these departments to not leak the classified information, it disables the cybersecurity professionals to supervise these specially protected departments. Third, differences among departments within the executive branch causes an issue to enforce a cybersecurity policy among different departments that are vastly different depending upon what their leadership thinks is important to them. Lastly, some state governments have too many networks that are connected to each other. Managing these networks simultaneously can be a governance barriers for state governments.

3.5 Insufficient or Under-Enforced Cybersecurity Policies

As is discussed in Chapter 2, one of the top cybersecurity vulnerabilities of state and local government law enforcement organizations is human behavior. Many IT systems are vulnerable to an insider. As we explained in the previous chapter, there are two types of insiders: accidental insiders, and purposeful insiders. On the one hand, accidental insiders are people who make an unintentional misstep or a part of social engineering scheme. On the other hand, purposeful insiders are people who intentionally target an organization while working as an employee. It is very hard to detect those purposeful insiders and protect the organization from inside attacks. However, organizations can be secured from accidental insiders in different ways. Norris et al. (2015) note that state and local government agencies combat those problems in two different ways: (1) training their workforce on cybersecurity best practices and (2) defining cybersecurity policies and implementing procedures to enforce them.

The problem is that many of the state and local government agencies do not enforce their cybersecurity policies. For instance, it not efficient to have a cybersecurity training policy if it is not mandatory. Norris at al. (2015) states that “a common example is not enforcing rules that require user to get cybersecurity training” (p. 200). The lack of sufficient cybersecurity policies and their enforcement can also be seen in requiring data breach notifications and to establish clear courses of action for companies and state agencies to follow in the event of a data breach, including reporting any such breach to the state’s IT Department or the state’s police department.

To investigate cybercrimes, fraud, IP theft, privacy breach, and other cyber activities, state and local government agencies that have had a data breach or any cybercrime need to collaborate with IT departments and report that the cybercrime has occurred. However, due to the absence of a mandatory clause to cooperate with IT officials and report incidents, the collaboration to detect cybercrimes and protect the organization from future attacks can fail. Sufficient cybersecurity policies should include a clear course of action in the event of a cybersecurity breach and require companies and state agencies to notify the state’s IT Department and the state’s police department if a data breach has occurred.

These major barriers in addressing cybersecurity challenges are present mostly because cybersecurity is a relatively new problem that state and local governments have not developed sufficient mechanisms or a framework to address. Although the history of cybercrime goes back to 1970s, state and local governments were not expected to address cybersecurity issues until the 2000s. As a consequence, state and local governmental cybersecurity capacity has only recently begun to develop. Some of these barriers occurred because of structural and statutory problems such as the challenge of governance, and insufficient or under-enforced cybersecurity policies. It is hard to overcome those barriers without legal reform. The organizational structure sometimes does not allow to take actions on cybersecurity problems. For instance, as I mentioned above, IT departments do not have authority over the legislative and judicial branches because they are generally located in the executive branch. The other barriers mentioned, a lack of sufficient funding, inadequate availability of cybersecurity professionals, and increasing sophistication of cyber threats, are managerial/administrative related. Those kinds of barriers might be overcome with an efficient management strategy. For instance, the challenge of increasing sophistication of cyber threats is related to management. It could be overcome with a good management mandate such as making IT system updates obligatory. Legal requirements are not needed to overcome those kinds of managerial problems whereas structural problems need legal reforms to be solved.

The challenge of governance is the most important barrier in addressing cybersecurity challenges in the state and local governments. Even if state and local governments were able to reserve a large budget to fix cybersecurity issues, structural challenges would prevent effective and successful strategies. For this reason, there should be legal reform to give IT departments' authority over all state and local governments' branches for the enforcement of cybersecurity best practices. If structural and statutory challenges could be precluded, funding would be used more efficiently because it does not matter how much you spend, it matters how you spend the fund on cybersecurity issues. State and local governments should overcome structural problems to use their funds more efficiently and effectively.

In Chapter 4, I examine a case study of the State of Maryland to discuss their barriers. I argue that the lack of sufficient funding, inadequate availability of cybersecurity professionals, insufficient or under-enforced policies, and that their governance issue are the most relevant barriers for the state to face in their attempts to create a secure public cyberspace.

Chapter 4

THE CASE OF MARYLAND

In this chapter, I will examine the state of Maryland as a case study to explain the barriers that I discussed in Chapter 3. In order to provide empirical evidence for my arguments, I use interviews conducted through focus groups, which include IT and cybersecurity professionals from the state government and several local governments throughout the state of Maryland. These interviews constitute secondary data which was originally collected by three researchers[2] from the University of Maryland. In addition, I use interviews published through online journals and local news for the state of Maryland.

4.1 Case Justification

The state of Maryland has become a significant contributor nationally on cybersecurity, and it is one of the trendsetters among states leading cybersecurity strategies to protect its cyberspace (Spidalieri, 2015). Some of the premier cyber-related federal agencies and military installations are located in Maryland. According to the Federal Laboratory Consortium for Technology Transfer, there are 74 federal

[2] Donald Norris, Anupam Jashi, and Timothy Finin.

laboratories, more than twice as many as any other state, in Maryland. In addition, it is home to four highly relevant cyber resources: (1) the Defense Information System Agency (DISA), (2) the National Security Agency (NSA), (3) United States Cyber Command (USCYBERCOM), and (4) the National Institute of Standards and Technology (NIST). Those agencies are critical in supporting national security. For instance, the NSA is responsible for protecting U.S. national security information systems and collecting and disseminating foreign intelligence signals.

Moreover, Maryland was the first state in the country to establish a commission dedicated to cybersecurity, called the Maryland Commission on Cybersecurity Innovation and Excellence. The commission's purpose is to develop comprehensive, coordinated, and rapid response strategies for proactively protecting the state against cyber attacks and promoting cyber innovation and job creation. Furthermore, it was also the first state to create a National Cybersecurity Center of Excellence (NCCoE) to help businesses secure their digital infrastructure, and a Federally Funded Research and Development Center (FFRDC) exclusively dedicated to enhancing cybersecurity and protecting national information systems (Spidalieri, 2015).

Not only does Maryland present a great case study because it is the home to several critical agencies for national security, but also because it is one of the foremost practitioners applying the suggestions of NASCIO, NIST, and federal government to their own state's cybersecurity issues.

The state of Maryland has made significant investments to create incentives such as the Cybersecurity Investment Incentive Tax Credit (CIITC) on cybersecurity issues.

Even though it has significantly focused on addressing cybersecurity issues, it also has experienced the challenges and barriers that I discussed in Chapter 3. In the following section, I will analyze these challenges and barriers by looking at the case of Maryland.

4.2 Lack of Sufficient Funding and Cybersecurity Professionals in Maryland

There are many reasons why state and local governments cannot find or hire qualified cybersecurity or IT staff, such as inadequate availability of cybersecurity workforce, insufficient human resource departments, and lack of sufficient funding. First and foremost, they cannot hire those uniquely skilled individuals because there is insufficient funding for hiring qualified cybersecurity and IT employees. In other words, insufficient funding and lack of cybersecurity professionals are related with each other. For this reason, I would like to discuss these two barriers under the same section to analyze the case of Maryland.

Without enough funding, it is not possible to provide the needed level of cybersecurity protection and employ qualified IT and cybersecurity employees (Norris et al., 2015, p.199). In addition, the lack of sufficient funding and staff are also the top two barriers reported in the study of 2016 Deloitte-NASCIO Cybersecurity.

The lack of adequate budget and highly trained employees constitute important barriers in addressing cybersecurity challenges in the state of Maryland. Although it is one of the best examples and role models of state level cybersecurity management, it still faces an inadequate budget and staffing capacities. The fact that these problems constitute an important barrier in addressing cybersecurity challenges in the state of Maryland is supported by interviews with the IT and cybersecurity professionals from the state government and several local governments in Maryland.

For instance, one participant noted:

> ...less than two percent of the overall budget. Less than two percent. Yet 100 percent of the people in [the county] are using IT. So, you know, you're right, you know, we don't have the resources, we don't have the manpower. [We]... try and use our money the best way we can and...you're right, sometimes things can be solved with money (quoted from Norris et al., 2015, p.199).

Establishing and operating a secure server, hiring the best IT and cybersecurity staff, and having an information technology system is not a cheap way to protect the cyberspace for state and local governments that have limited budgets dedicated to addressing cybersecurity challenges. For this reason, state and local governments have tried to figure out alternative solutions to tackle cybersecurity problems. For example, one county represented in the focus group reported that its programs and data were already 90% running on cloud computing infrastructure. In other words, they outsource a service to store and protect data. In this case, the cloud service providers are responsible for securing the data and services. In addition, other professionals from different government organizations in Maryland noted that "they are beginning to view cybersecurity as a commodity or a service that they purchase on the market" (Norris et al., 2015, p.199). Some of the participants noted that, in addition to potential cost savings, outsourcing reduces staffing needs (Norris et al., 2015).

An adequate budget and trained staff are necessary conditions for an effective cybersecurity management, but they are not sufficient by themselves. Because of the sophistication of cyber threats, governments seem to face cyber threats even if they have enough budget and qualified staff. The state of Maryland is no exception. Because the techniques of cyber attacks are very dynamic, the increasing sophistication of cyber threats is a greater barrier, which I will discuss next.

4.3 Increasing Sophistication of Cyber Threats in Maryland

Increasingly sophisticated technology is allowing hackers to also develop increasingly sophisticated strategies for extracting protected data. For instance, system developers can create new codes that improve current systems; however, these new improvements can also create new cyber vulnerabilities. Cyber attackers exploit these vulnerabilities to find new security holes in the system. Even if an information system looks secure today, eventually, cyber attackers will find deficiencies in the system through new developments. The cyber attackers are always improving their strategies by using updated technological developments.

The state of Maryland is also exposed to sophisticated cyber threats. As opposed to the previous professionals that argued an adequate budget and qualified staff would overcome the barriers in addressing cybersecurity challenges, others argue that those precautions will not be sufficient because of the dynamic nature and increasing sophistication of cyber threats. Norris et al. (2015) cites from the interviews that "…even with greater funding and more staff, their systems will continue to be attacked and will probably, eventually, be a victim of a successful attack." (p.199). For this reason, state and local governments need to invest in responding to cybercrimes as well as investing in updated and secure systems and qualified IT and cybersecurity professionals.

4.4 The Challenge of Governance in Maryland

In the previous chapter, I discussed the four problems that stem from governance in regards to cybersecurity. To summarize these problems: First, IT departments do not have authority over the legislative and judicial branches because they are generally located in the executive branch. Second, IT professionals are not allowed to access to the classified information in all departments because some departments have special protections. Third, differences among departments within the executive branch causes an issue to enforce a cybersecurity policy. Last, there are multiple networks to manage. All of those governance issues can be seen in the case of Maryland. In this section, I will discuss these problems for the state of Maryland by using the interviews conducted by Norris et al., which present a clear understanding of Maryland's cybersecurity related governance challenges.

One of the participants of the *Cybersecurity Challenges to American State and Local Governments* stated, "I've got responsibility over all three branches of government. However, I can't legally enforce policy, due to the pesky constitution, over the legislative and judicial branches. But I am responsible for their security." (quoted from Norris et al., 2015, p.200). Even though the participant, a cybersecurity professional in Maryland State Government, does not have authority to enforce a policy over legislative and judicial branches, he is responsible for protecting their cyberspace and systems.

Another participant told his opinion based on his experiences:

> And well, even within the executive branch we've got 35 different departments, each with varying levels of risk tolerance. So being able to enforce a policy on department X versus department Y is vastly different depending upon what their leadership thinks is important to them. And what their mission is. Recreation feels

> like they have to provide services for ball fields and for swimming pools, etc., etc., that’s what their mission is but then…you start thinking about the millions of dollars that they get in credit card transactions every year and that then becomes a big potential security risk. (quoted from Norris et al., 2015, p.200).

Based on the participant’s interview, it looks like it is not easy to enforce a cybersecurity policy even when the departments are under the same government branch. In this case, the executive branch has 35 different departments, each with different responsibilities. Their management techniques, leaders, and level of risk tolerance are very different than each other. As a result, differences among departments within the executive branch cause an issue with enforcing cybersecurity policy.

Another governance issue, mentioned by an IT professional from Maryland, is an example of the managing multiple networks issue. This participant noted that “there are eleven, I stopped counting at eleven, different data networks…over the years, well-meaning people patched weird connections to them that we may or may not understand and we’re trying to untangle that...” (quoted from Norris et al., 2015, p.200).

The governance issue is a structural barrier that creates difficulties in the policy making process. The barrier of insufficient or under-enforced cybersecurity policies is an administrative problem that can hinder implementation of effective cybersecurity policies. In the next section, I will discuss this barrier.

4.5 Insufficient or Under-Enforced Cybersecurity Policies in Maryland

It is not enough to just have cybersecurity policies to block cyber attacks. These policies should be effective and feasible to implement. However, it is not easy to create a completely effective and feasible cybersecurity policy that fits into every state and local government because each agency has different management methods and responsibilities. Nevertheless, each state and local government needs to fulfill common requirements at a very basic level, which can be more general. For instance, collaboration among IT departments and law enforcement agencies are very crucial for feasible cybersecurity policies. In addition, mandatory training is the other critical precondition of the effective cybersecurity policy implementation.

In the case of Maryland, there are clear deficiencies in terms of creating sufficient and effective cybersecurity policies. As we discussed in Chapter 2, one of the greatest contributors to vulnerabilities of state and local government agencies is human behavior. State and local governments try to protect themselves from cyber attacks that are related to human behavior by training their workforce. However, this training is not always mandatory for agencies. Norris et al. (2015) argue that “a common example is not enforcing rules that require users to get cybersecurity training.” (p.200). IT and cybersecurity professionals from Maryland agree. They ask for a mandatory training class because they think it is the only way to effectively implement cybersecurity policies and protect cyber safety. “Well, as far as security awareness is concerned, our struggle it getting it to be mandatory” (quoted from Norris et al., 2015, p.200). Another cybersecurity professional shared that in his county they managed to make the training mandatory with the support of the executive branch. “The county executive backed it up. People had to come to training centers.” (quoted from Norris et al., 2015, p.200).

The barriers of insufficient and under-enforced cybersecurity policies are very significant administrative issues in addressing cybersecurity challenges. Without feasible cybersecurity policies and effective implementation of them, it will not be possible to fully address cybersecurity challenges and combat cyber attacks.

In Chapter 5, based on the literature and research presented in previous chapters, I will discuss what types of strategies state and local governments should use to prevent and overcome the barriers explained in Chapter 3.

Chapter 5

POLICY RECOMMENDATIONS

As discussed in previous chapters, while the federal government focuses on big-picture solutions to cybersecurity challenges, state and local government organizations are under pressure to protect critical data, infrastructure, and services. I discussed the obstacles that local and state governments face in addressing cybersecurity challenges. Simply being aware of those barriers is not enough to protect the cyberspace. For this reason, state and local governments should take some precautions towards providing better cybersecurity because cybercrimes cause loss in the economy, threaten sensitive personal information, and hinder online freedom. There are three main ways to reduce cyber attacks on the local level:

- Building partnerships with the larger security community and outsourcing security needs
- Creating a cybersecurity strategic plan
- Creating more law enforcement

5.1 Building Partnerships and Outsourcing Security Needs

Outsourcing is a practice used by different organizations to reduce costs and organizational risks by transferring portions of services to outside suppliers rather than running them internally. Even though it is mostly used in the private sector, government organizations have been outsourcing services since the 1970s, New Public Administration traces. Building partnerships with the larger security community and outsourcing security needs provide two significant benefits to state and local governments: providing a talented workforce and reducing costs.

Organizations need skilled professionals to setup and run their cybersecurity systems. Private sector opportunities and salaries are undeniably better than those offered by state governments. Deloitte and NASCIO (2014) state that outsourcing is one way to compensate for talent gaps. They add that "the most frequently outsourced functions include forensic and legal support, risk assessment, and threat management and monitoring" (p.20). In addition, building partnerships with the larger security community creates a standardized security protocol which provides a more secure cyberspace. In other words, using similar firewalls, programming languages, and data logging techniques helps create a safer and unified cyberspace. Lastly, Brasso (2016) suggests that "government organizations, with partial funding from the private sector, could offer professional training and experience to recent graduates. After several years, these experienced workers could transition to a sponsoring company if they so desire" (para.13). Through this strategy state and local governments could take advantage of a highly qualified workforce.

The sophisticated and dynamic nature of cyber threats demands that state and local governments develop and participate in public-private partnerships focused on sharing information about threat characteristics, response options, and workforce needs.

For example, fusion centers can provide a good opportunity for state and local governments to access cybersecurity expertise that is only attainable through cost-sharing arrangements across public and private sector organizations. According to DHS (2016b), "a fusion center is a collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity" (para.1). According to National Governors Association (2015) "they are owned and operated by state and local governments and serve as focal points for state, local, federal, tribal, and territorial partners to receive, analyze, and share threat-related information" (p.1). Involvement from multiple sectors and industries promotes more robust information-sharing efforts that promise to yield an understanding of threats that is not possible without a coordinated approach.

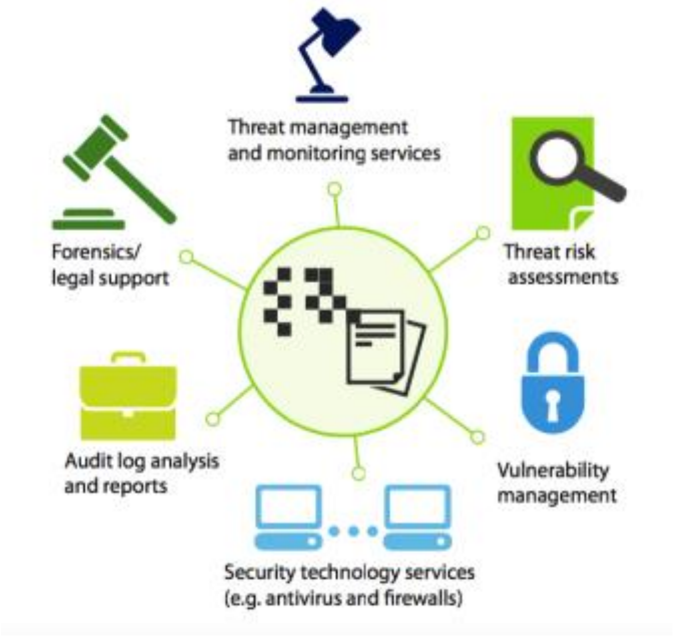

Figure 5.1: Leading Outsourcing Cybersecurity Functions (Deloitte, 2014, p.20)

Additional outsourcing targets include system setup, as it is extremely expensive to setup security systems that need to be updated almost every 6 months. It does not always make sense to setup and run them internally because they are expensive and short-term investments. State and local governments cannot easily update those systems even if they set them up because they have a restricted budget in addressing cybersecurity challenges. They can often reduce expenses by outsourcing these systems.

In 2015, Ponemon Institute published a research report named *State of Cybersecurity in Local, State & Federal Government*. 443 federal government respondents and 402 state and local government respondents participated in the survey. According to the report, as shown in Figure 5.2, “a lack of skilled personnel is a challenge at the local, state and federal organizations. However, the challenge is more severe at the state and local level (62 percent say this is a major challenge)” (p.8).

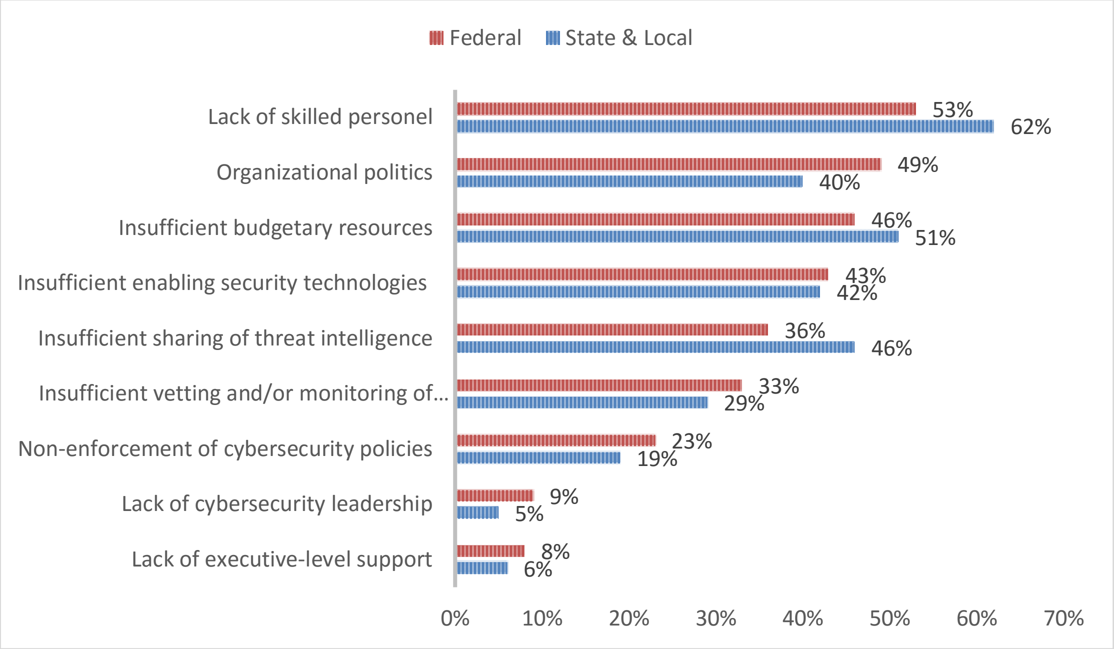

Figure 5.2: What are the main challenges to achieving a strong cybersecurity posture within your organization? (Ponemon Institute, 2015, p.8).

Consequently, if state and local governments build partnerships and outsource security needs, this helps to reduce costs, secure their own networks, and create a safe place for businesses.

5.2 State Cybersecurity Strategic Plan and Chief Security Officer

A state cybersecurity plan establishes states' visions, principles, goals, and objectives about cybersecurity precaution steps.

Melissa Hathaway, an expert in cyberspace policy and cybersecurity, states that an effective cybersecurity strategic plan includes:

> Specific cyber threats to the state and necessary steps, programs, and initiatives that should be undertaken to address identified cyber threats and increase resilience; competent authority—the responsible and accountable entity—that ensures the implementation and execution of the plan, and the adoption of well-

> established standards and policies; annual threat assessment to government agencies and critical infrastructure networks; adoption of well- known benchmarks, standards, and policies developed by nationally respected groups like National Institute of Standards and Technology (NIST); and a strong linkage to the economic health of the state (quoted from Spidalieri, 2015, p.7).

Well prepared state cybersecurity plans are route maps for state and local governments because they outline every necessary step to be taken. It should be reviewed or updated every year because technological changes are very dynamic. In addition, creating a position for the Chief Security Officer will be helpful for coordination among departments of state and local governments. It is a position that brings together both physical security and cybersecurity functions under a single division. The Chief Security Officer should create a state cybersecurity strategic plan that explains many important steps such as competent authority, regular threat assessment, NIST framework, and cyber hygiene. A state-wide cybersecurity plan creates coordinated cybersecurity strategies to help minimize cyber attacks and create effective administrative positions like the chief security officer.

The state of Maryland lacks a position for Chief Security Officer in the government. However, it has a chief information officer, who has a more general agenda that includes other technological development issues. The state of Maryland lacks a publicly accessible cybersecurity strategic plan. Instead, it has several reports on cybersecurity that aim more at commercial attention than the government's strategies on protecting its cyberspace. As Maryland CIO David Garcia explained, "the state is working to solidify an enterprise model statewide. DoIT is working to modernize and provide a baseline model across Maryland executive branch agencies and become the one-stop for all the commodity IT services" (quoted from Spidalieri, 2015, p.14).

The reports provided by the Department of Information Technology (DoIT) are still important as they inform the citizens of Maryland about the state's cybersecurity policies. Moreover, the reports aim to make Maryland an attraction center for the private companies and federal government agencies by ensuring them the cyberspace in Maryland is reliable. For instance, Mark Orndorff, the DISA program Executive Officer for Mission Assurance and Network Operations, stated that "We moved up to Fort Meade for a reason, to take advantage of the neighborhood" (quoted from The Maryland Department of Commerce, 2017, p.5).

Nevertheless, it is necessary for the state of Maryland to develop a cybersecurity strategic plan. The Maryland Commission on Cybersecurity Innovation and Excellence, agrees that there needs to be more guidance for the state agencies in addressing cybersecurity challenges: "DoIT did not have a formal process in place to enforce the provisions of its information security policy" and that it should "improve guidance to help agencies address certain security issues" (quoted from Spidalieri, 2015, p.15).

All in all, a cybersecurity strategic plan is crucial for state governments to clarify their cybersecurity vision, principles, goals, objectives, capabilities, and capacity about cybersecurity precaution steps. Knowing their capacity is crucial because all state and local governments have different needs in terms of cybersecurity since their capacities are very different from each other. For example, a state government with a complex organizational structure and many employees has different needs from a small local government. For this reason, their capacities and capabilities should be clarified in the cybersecurity strategic plan. Therefore, creating a Chief Security Officer position that brings together both physical security and cybersecurity functions under a single division and outlining procedures for rapid response can address state cyber threats.

5.3 Law Enforcement

Any state or local government policy should be binding and enforced to fully address cybersecurity challenges as well as combat cyber attacks. According to Spidalieri (2015), law enforcement is:

> Commitment to protect residents against cybercrime through laws, such as data breach notification law, and other regulatory governance mechanisms; established relationship with law enforcement officials to interdict and investigate events of fraud, crime, IP theft, privacy breach, and other cyber activities; state's ability to fight cybercrime, including training of law enforcement specialists, forensics specialists, judges, and legislators, and state law enforcement's ability to use tools at their disposal to combat cybercrime (pp.7-8).

State and local governments should demonstrate a strong commitment to protect its residents against cybercrimes, such as network intrusions, computer hacking, counterfeiting and piracy, theft of personal information, and telecommunications fraud. Not all the regulations and precautions are effective without a legal infrastructure. In other words, state and local government agencies should be backed with federal government laws and regulations. For instance, government agencies organize some trainings to increase its employees' knowledge about cybersecurity issues and new hacking techniques. However, these trainings are not always mandatory for government agencies. Mandatory training is critical to ensure effective cybersecurity policy implementation. Furthermore, collaboration among government agencies is not always obligatory even though collaboration among IT departments and law enforcement agencies is very crucial for implementing cybersecurity policies.

In addition, mandatory policies can also relate to the care and protection of the personal information of citizens. For example, employees and citizens (users) use a username and password to connect and take actions on the IT systems that keep their sensitive information. Because some people don’t use secure passwords, government agencies may choose to utilize two-factor or multi-factor authentication techniques. These are methods of using a combination of different components to verify a user's claimed identity. However, when these authentication methods are not mandatory, most users don’t take the initiative to utilize them. To work effectively these methods should be made mandatory. If state and local government agencies do not have enough professionals to adopt those kind of techniques, they should put funds towards opening more positions for these experts.

Apart from these strategies to reduce cyber attacks at the local level, state and local governments should simply spend more on cybersecurity issues. However, they should be careful how to use this extended budget because it is more important how to allocate the budget than how much money is spent.

Beyond all these suggestions, the research based on the literature and interviews with the IT and cybersecurity professionals reveal that it is impossible to completely eliminate the cyber attacks because of the dynamic nature and increasing sophistication of cyber threats. Those strategies can protect the cyberspace from some cyber attacks and reduce the damage of others. Nevertheless, state and local governments will face cyber threats no matter how much they utilize these strategies and reserve budget for IT systems. Thus, they must also develop mechanisms to respond to cyber attacks. As I have quoted in Chapter 4, Norris et al. (2015) cites from the interviews that "…even with greater funding and more staff, their systems will continue to be attacked and will probably, eventually, be a victim of a successful attack." (p.199). The state and local governments in Maryland do not have very sophisticated response mechanisms to cyber attacks, whereas State of Michigan has developed a sophisticated system for early detection and rapid response. According to Spidalieri (2015), the Michigan Cyber Command Center, part of the Michigan State Police, is the state's lead response to incidents with a criminal nexus and is charged with directing law enforcement operations, including investigation, mitigation, and prosecution of cybercrimes. The State Police serves as a liaison with federal law enforcement agencies, too. According to the Michigan Cyber Initiative (2015), Michigan is successful at blocking cyber attacks because of its rapidly-responding law enforcement.

All in all, building partnerships with the larger security community and outsourcing security needs, creating a cybersecurity strategic plan, and enabling more law enforcement are crucial in addressing cybersecurity challenges. Adequate budget and strategic allocation of it are also vital for protecting the cyberspace efficiently. Despite all these precautions, the local and state governments are inevitably going to face cyber attacks. The most important action to take is to develop sophisticated systems for early detection and rapid response to cyber attacks.

Chapter 6

CONCLUSION

The first chapter was an introductory chapter that draws a road map for my research. Chapter 2 addressed the transition to the information revolution from the agricultural and industrial revolution after clarifying vulnerabilities of state and local governments. Subsequently, I detailed a variety of the most dangerous hacking techniques state and local governments face after discussing the motivations behind cyber attacks.

In brief, cybersecurity is not only a problem at the federal level, but also a problem at the local level. State and local governments cannot wait for the federal government to provide all responses and solutions before taking actions. They have a responsibility to create a safe cyberspace and must work to secure their critical infrastructure and cyber assets. Cybersecurity is one of the most significant issues currently facing the nation because we are living in the age of technology and this is an increasingly-networked world, from personal banking to government infrastructure. Some state and local governments take some specific precautions towards cybersecurity; however, most of them have not taken sufficient measures. Even if they try to take precautions about the cybersecurity problem, they still face significant barriers in addressing cybersecurity challenges.

Chapter 3 explained findings on the barriers to addressing cybersecurity challenges in United States state and local governments based on the literature review. Lack of sufficient funding, inadequate availability of cybersecurity professionals, lack of documented processes, increasing sophistication of threats, and lack of visibility and influence within the enterprise are the main barriers identified. These significant barriers stem from not effectively applying policies and strategies. The reason is the nature of cyber attacks and hacking techniques. It is not possible to completely protect the cyberspace by creating a specific framework and applying stable strategies because those attacks and techniques are extremely dynamic. There are known strategies to reduce the effects of cyber attacks, but complete protection is not feasible.

According to Norris et al. (2015), “There is a need not only to continually harden the IT infrastructure, but also to have in place a recovery plan in the event of a successful attack. This is so because, in case the systems go down, there is the need for continuity in government.” (p.200). As Dawson and Desouza (2015) recommend, “states closely examine and adopt standards, policies and procedures enacted by nationally respected groups like NIST in order to jump start their cybersecurity planning”. In addition, state and local governments need to build partnerships with the larger security community, outsource their security needs as appropriate, create a state cybersecurity strategic plan, and create law enforcement to establish a secure cyberspace and maintain or gain public trust.

Chapter 4 examined the state of Maryland as a case study to demonstrate the barriers explained in Chapter 3. I used interviews conducted through focus groups that included IT and cybersecurity professionals from state and local governments in Maryland. I argued that the lack of sufficient funding, inadequate availability of cybersecurity professionals, insufficient or under-enforced policies, and governance issue are the most relevant barriers that state and local governments in Maryland face in their attempts to create cybersecurity. The fact that cybersecurity policies are underdeveloped, even in Maryland, reveals the difficulty of tackling the issue completely. Because cyber attacks are so dynamic and difficult to predict, the barriers to cybersecurity remain unaddressed.

Lastly, Chapter 5 proposes different strategies state and local governments can employ to be most effective at enhancing their cybersecurity. The discussion and suggestions are based on my inferences from the shared literature, recommendations by Federal government and NASCIO, and thoughts gathered from the interviews. All of the strategies that I discussed in Chapter 5 would help to reduce cyber threats for state and local government agencies.

Despite the precautions, state and local government agencies are still going to face cyber attacks. Thus, it is necessary that state and local governments invest in creating an early detection and rapid response system for cyber attacks as well as investing in updated IT infrastructure and qualified IT and cybersecurity professionals. However, the most important action a governmental organization can take is developing a sophisticated system for early detection and rapid response to cyber attacks.

REFERENCES

Abelson, R., & Goldstein, M. (2015). Millions of Anthem Customers Targeted in Cyberattack. *The New York Times*. Retrieved from https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html

Asllani A., White C.S, & Ettkin L. (2013). Viewing cybersecurity as a public good: The role of governments, businesses, and individuals. *J. Leg. Ethical Regul. Iss. Journal of Legal, Ethical and Regulatory Issues*, *16*(1), 7–14.

Barber, R. (2001). Hacking Techniques: The tools that hackers use, and how they are evolving to become more sophisticated. *Computer Fraud & Security*, *2001*(3), 9–12. Retrieved from https://doi.org/10.1016/S1361-3723(01)03014-7

Beaver, K. (2013). The 5 Common Network Security Vulnerabilities That Are Often Overlooked. Retrieved from https://www.acunetix.com/blog/articles/the-top-5-network-security-vulnerabilities/

Benedikt, M. (1991). Cyberspace: first steps.

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

Brasso, B. (2016). How State and Local Governments Can Solve Their Cyber Security Staffing Shortage. Retrieved from https://www.fireeye.com/blog/executive-perspective/2016/02/how_state_and_local.html

Brown, R. (2012). More Details of South Carolina Hacking Episode. *The New York Times*. Retrieved from https://www.nytimes.com/2012/11/21/us/more-details-of-south-carolina-hacking-episode.html

Bucci, S. P., Rosenzweig, P., & Inserra, D. (2013). A congressional guide: Seven steps to US Security, Prosperity, and Freedom in Cyberspace. *Backgrounder*, (2785). Retrieved from http://s3.amazonaws.com/thf_media/2013/pdf/bg2785.pdf

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

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

Chun, S. A., Shulman, S., Sandoval, R., & Hovy, E. (2010). Government 2.0: Making connections between citizens, data and government. *Information Polity*, *15*(1), 1. Retrieved from http://cimic.rutgers.edu/~soon/papers/2010/ip2010.pdf

Daniel, M. (2014). State and Local Government Cybersecurity. Retrieved from https://obamawhitehouse.archives.gov/blog/2014/04/02/state-and-local-government-cybersecurity

Deloitte. (2014). *2014 Deloitte-NASCIO Cybersecurity Study - State governments at risk: Time to move forward*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-state-nascio-cybersecuritysurvey_102714.pdf

Deloitte. (2016). *2016 Deloitte-NASCIO Cybersecurity Study*. Retrieved from https://dupress.deloitte.com/content/dam/dup-us-en/articles/3470_2016-Deloitte-NASCIO-cybersecurity-study/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf

Department of Homeland Security. (2016a). Critical Infrastructure Sectors. Retrieved from https://www.dhs.gov/critical-infrastructure-sectors

Department of Homeland Security. (2016b). National Network of Fusion Centers Fact Sheet. Retrieved from https://www.dhs.gov/national-network-fusion-centers-fact-sheet

Eidam, E. (n.d.). Governors Discuss Better Coordination, Establishing Protocols to Improve Cybersecurity. Retrieved from http://www.govtech.com/security/Governors-Discuss-Better-Coordination-Establishing-Protocols-to-Improve-Cybersecurity.html

Fox-Brewster, T. (2016). Ransomware Crooks Demand $70,000 After Hacking San Francisco Transport System. Retrieved from https://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/#49eee6774706

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine*, *30*(1), 28–38. Retrieved from https://doi.org/10.1109/MTS.2011.940293

Garcia, D. (2016). 5 benefits for government agencies to use social media in 2016. Retrieved from https://www.linkedin.com/pulse/5-benefits-government-agencies-use-social-media-2016-dan-garcia

Garcia, G. (2017). POLICYBER: Time for State Cyber Grants. Retrieved from https://www.linkedin.com/pulse/policyber-time-state-cyber-grants-greg-garcia

Gibson, W. (1995). Neuromancer. 1984. *New York: Ace*.

Gregory Dawson, & Kevin C. Desouza. (2001). How state governments are addressing cybersecurity. Retrieved from https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/

Han, C., & Dongre, R. (2014). Q&A. What Motivates Cyber-Attackers? *Technology Innovation Management Review*, *4*(10), 40–42.

Kharpal, A. (2015). Hackers are selling your data on the "dark web"... for only $1. Retrieved from http://www.cnbc.com/2015/09/23/hackers-are-selling-your-data-on-the-dark-web-for-1.html

Levinson, M. (2012). Are You at Risk? What Cybercriminals Do with Your Personal Data. Retrieved from http://www.cio.com/article/2400064/security0/are-you-at-risk--what-cybercriminals-do-with-your-personal-data.html

Lipman, P. (2015). 4 Critical Challenges to State and Local Government Cybersecurity Efforts (Industry Perspective). Retrieved from http://www.govtech.com/opinion/4-Critical-Challenges-to-State-and-Local-Government-Cybersecurity-Efforts.html

Loewegart, V. (2012). *An Introduction to Hacking and Crimeware: A Pocket Guide*. IT Governance Publishing.

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

Lohrmann, D. (2017b). Government Ransomware: Stories and Tips. Retrieved from https://www.linkedin.com/pulse/government-ransomware-stories-tips-dan-lohrmann

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

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

McQuade, S. C. (2009). *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press.

Mehmood, S. (2016). *Enterprise Survival Guide for Ransomware Attacks*. SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-ransomware-attacks-36962

Mitnick, K. D., & Simon, W. L. (2011). *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.

Morgan, S. (2015). Cybersecurity job market to suffer severe workforce shortage. Retrieved from http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

Morgan, S. (2016). *Hackerpocalypse: A Cybercrime Revelation*. Cybersecurity Ventures. Retrieved from http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

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

National Consortium for Advanced Policing. (2016). *Cybersecurity Guide for State and Local Law Enforcement*. Retrieved from https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/NCAPCybersecurityGuide-2016.pdf

National Governors Association. (2015). *Enhancing the Role of Fusion Centers in Cybersecurity*. Retrieved from https://www.nga.org/files/live/sites/NGA/files/pdf/2015/1507EnhancingTheRoleOfFusionCenters.pdf

National Institute of Standards and Technology (NIST). (2014). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

Norris, D., Joshi, A., & Finin, T. (2015, June). Cybersecurity challenges to american state and local governments. In *15th European Conference on eGovernment* (pp. 196-202). Academic Conferences and Publishing Int. Ltd.. Retrieved from http://eprints.covenantuniversity.edu.ng/6419/1/E-

Government%20(2015%20Proceeding%20%20%20Published)ECEG_Proceedings-dropbox(1).pdf#page=213

NTTSecurity. (n.d.). New Q4 Threat Intelligence Report from NTT Security Finds Attacks on Organizations Becoming More Targeted, Sophisticated. Retrieved from http://www.marketwired.com/press-release/new-q4-threat-intelligence-report-from-ntt-security-finds-attacks-on-organizations-becoming-2191251.htm

Obama, B. H. (2015). Remarks by the President at the Cybersecurity and Consumer Protection Summit. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

Papadopoulos, E. (2014). State and local governments have important roles to play in managing cyber risks. Retrieved from http://americancityandcounty.com/security/state-and-local-governments-have-important-roles-play-managing-cyber-risks

Peters, G. (n.d.). Sens. Peters & Perdue Introduce Bill to Enhance Cyber Security Coordination. Retrieved from https://www.peters.senate.gov/newsroom/press-releases/sens-peters-and-perdue-introduce-bill-to-enhance-cyber-security-coordination

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

Ponemon Institute. (2016). *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*. Retrieved from http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

PwC. (2016). *Tech breakthroughs megatrend:Hhow to prepare for its impact*. Retrieved from https://www.pwc.com/gx/en/issues/technology/tech-breakthroughs-megatrend.pdf

Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk Management. In *Cyber-Risk Management* (pp. 33–47). Springer International Publishing. Retrieved from https://doi.org/10.1007/978-3-319-23570-7_5

Rhode Island Cybersecurity Commission. (2015). *A Framework for the Development of Cyber Protection and Resiliency in State Government Operations*. Retrieved from http://www.governor.ri.gov/documents/press/RICybersecurityCommissionOctober2015Report.pdf

Rosenzweig, P., Bucci, S., & Inserra, D. (2013). A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace. Retrieved from http://www.heritage.org/defense/report/congressional-guide-seven-steps-us-security-prosperity-and-freedom-cyberspace

Shinder, D. L., & Cross, M. (2008). *Scene of the Cybercrime*. Syngress.

Spidalieri, F. (2015). State of the states on cybersecurity. *Pell Center for International Relations*. Retrieved from http://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf

Steinberg, J. (2017). New Cybersecurity Business Report Highlights Geographic Trends. Retrieved from http://www.inc.com/joseph-steinberg/new-cybersecurity-report-highlights-surprising-geographic-trends.html

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

Symantec. (2016). *Internet Security Threat Report* (No. 21). Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

The Maryland Department of Commerce. (2016). *Cybersecurity Maryland*. Retrieved from https://open.commerce.maryland.gov/wp-content/uploads/2016/10/Cybersecurity-Maryland.pdf

The Maryland Department of Technology. (2017). *Maryland Cybersecurity Program Policy*. Retrieved from http://doit.maryland.gov/Lists/DoIT%20Policies/Attachments/32/cybersecurity-program-policy-v1.0%20(Updated%20with%20Sigs).pdf

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

The Utah Department of Health. (2012). More About the Data Breach. Retrieved from http://www.health.utah.gov/databreach/about.html

U.S. Office of Personal Management (OPM). (n.d.). Cybersecurity Incidents. Retrieved June 11, 2017, from http://www.opm.gov/cybersecurity/cybersecurity-incidents/

US-CERT. (2009). Security Tip (ST04-015): Understanding Denial-of-Service Attacks. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-015

Webster, F. (2014). *Theories of the information society*.

The White House. (2009). White House Announces Open Government Website, Initiative. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/white-house-announces-open-government-website-initiative

The White House. (2013). Presidential Policy Directive -- Critical Infrastructure Security and Resilience. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

The White House. (2016). FACT SHEET: Cybersecurity National Action Plan. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan