Spring 2021

Cybersecurity Legislation and Ransomware Attacks in the United States, 2015-2019

Joseph Skertic
Old Dominion University, joseph.skertic@yahoo.com

CYBERSECURITY LEGISLATION AND RANSOMWARE ATTACKS IN THE UNITED STATES, 2015-2019

by

Joseph Skertic
B.A. December 2009, Christopher Newport University
M.A. May 2012, Regent University

A Dissertation Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

INTERNATIONAL STUDIES

OLD DOMINION UNIVERSITY
May 2021

Approved By:

Matthew DiLorenzo (Director)

Joshua Zingher (Member)

Hongyi Wu (Member)

ABSTRACT

CYBERSECURITY LEGISLATION AND RANSOMWARE ATTACKS IN THE UNITED STATES, 2015-2019

Joseph Skertic
Old Dominion University, 2021
Director: Dr. Matthew DiLorenzo

Ransomware has rapidly emerged as a cyber threat which costs the global economy billions of dollars a year. Since 2015, ransomware criminals have increasingly targeted state and local government institutions. These institutions provide critical infrastructure – e.g., emergency services, water, and tax collection – yet they often operate using outdated technology due to limited budgets. This vulnerability makes state and local institutions prime targets for ransomware attacks. Many states have begun to realize the growing threat from ransomware and other cyber threats and have responded through legislative action. When and how is this legislation effective in preventing ransomware attacks? This dissertation investigates the effects of state cybersecurity legislation on the number of ransomware attacks on state and local institutions from 2015-2019. I review various arguments linking cybersecurity legislation to cybersecurity vulnerability and develop a set of hypotheses about the features of legislation that should deter and prevent ransomware attacks. The cybersecurity literature suggests increased training is a key mechanism to prevent ransomware attacks. However, I find no relationship between direct state legislation on cybersecurity training and ransomware. Instead, the statistical evidence suggests that there are fewer ransomware attacks in states with legislation that indirectly encourages training by shifting the responsibility for a cyber failure back onto vulnerable institutions. This legislation typically focuses on data breaches and often requires the institution to disclose failures, which increases reputational costs. The threat of increased costs for a cybersecurity failure changes these institutions' cost benefit analysis and

encourages these institutions to proactively improve their cybersecurity, such as through increased training. I further examine data breach laws in California and find evidence that these types of laws can promote increased cybersecurity measures. Thus, future legislation should focus on holding institutions responsible for cybersecurity failures, which should in turn lead to increased cybersecurity.

This dissertation is dedicated to my family:

To my Grandparents – Grandma Jean and Grandpa Al and Grandma and Grandpa Skertic – their love and support encouraged me to pursue my passion for learning.

To my Mom who taught me to patience and compassion, as well as, made me apply to college.

To my Dad who helped me write my first paper and taught me how to succeed through hard work and service to others.

To my Wife, Elizabeth, who helped improve my writing by editing my papers and who put up with many last minute, late night papers over the years.

And finally, to my two Sons, Liam and Luke, who bring me more joy than they will know and who I hope will one day be inspired by this accomplishment to pursue their passions.

ACKNOWLEDGEMENTS

Many people have helped and contributed to my successful completion of this dissertation. I would like to extend the greatest thanks to Dr. Matthew DiLorenzo, who served as my dissertation chair for this project. His sharp advice, fast turn around, and guidance helped me take my scattered ideas and form them into an achievable and meaningful project. I would also like to extend sincere thanks to Dr. Joshua Zingher and Dr. Hongyi Wu for serving on my committee and providing valuable feedback on this project.

TABLE OF CONTENTS

Chapter Page

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

In January of 2020, the Town of Colonie, New York faced a hostage situation. In this case, the hostage was not a person, but the entire town. This may sound like the half-cocked plans of a super villain from a fictional spy movie, but it is actually a reality faced by more and more cities across the world. The Town of Colonie was just the newest victim to the rapidly growing issue of ransomware.

Ransomware is a type of malicious software that encrypts a victim's data and demands a ransom payment within a limited time window in exchange for a decryption key. If the victim refuses to pay, they risk losing their data forever (Kaspersky 2020). The hackers were able to infect the town's computer system with ransomware after town employees received emails that appeared to be from fellow employees, but were in fact phishing attempts with ransomware embedded inside (Carbonite 2020). Hours later Colonie's computer systems had been encrypted and the local government, including critical infrastructure, such as public safety, came to a screeching halt. Anonymous hackers then demanded $400,000.00 to release the decryption key for the town's data (Franco January, 2020). Local leaders faced a critical decision: pay the ransom to (hopefully) restore their systems or refuse and risk losing any data that was not backed up.

In the back of their minds was certainly the outcome of similar attacks, such as the ransomware attack on the city of Baltimore, Maryland only 8 months earlier. Niraj Chokshi with the *New York Times* reports the attack shutdown "voice mail, email, a parking fines database, and a system used to pay water bills, property taxes and vehicle citations" (Chokshi 2019). The criminals demanded payment of around $76,000.00 in bitcoins, a difficult-to-track digital

currency. They gave the city four days to comply or the demand amount would increase and advised if payment was not received within ten days the data would be lost forever. Despite the demands and with over 10,000 computers infected throughout the metropolitan, Baltimore's leaders refused to pay the ransom. However, Ian Duncan with the *Baltimore Sun* reports the city has since paid an estimated $18.2 million to recover its data and restore its systems (Duncan 2019).

The City of Baltimore is not alone as ransomware attacks have been increasing at a dramatic rate. Emsisoft, a cybersecurity company, estimates that the United States suffered more than $7.5 billion in damages caused by ransomware in 2019 (Emsisoft 2019). Damages from these cyber-attacks have been dramatically increasing over the past 5 years as global costs were at only $325 million in 2015 (Morgan 2017). With costs on the rise, the FBI recommends not paying a ransom, as there are many cases where the data is still not released and paying a ransom encourages further attacks (FBI 2016). In that spirit, some cities have refused to pay the ransoms, but have still suffered great costs as a result. The city of Atlanta, Georgia refused to pay a $51,000.00 ransom and has since paid around $17 million to recover their systems from an attack in March 2018 (Deere 2018). Other cities have chosen to pay the ransoms to avoid the potential extraordinary costs of recovering from an attack. For example, the city of Riviera Beach, Florida paid a ransom of $600,000.00 in Bitcoins in June 2019 (Karimi 2019). Whether these cities paid a ransom or not, they certainly suffered from not effectively investing in cyber security.

Smaller cities and local governments (like Colonie) have become prime targets of ransomware attacks. Local governments often cite a lack of budget to properly secure systems that provide critical community services (Gates 2019; Bond 2019). These smaller governmental bodies often have outdated systems and software, making them more vulnerable to attacks (Franco

February, 2020). One estimate places the odds of a local government falling victim to a ransomware attack at about one in four (Bond 2019).

In addition to the previously mentioned high profile attacks, the leaders of the Town of Colonie would also have been aware of two recent attacks closer to home. On March 30th, 2019, the City of Albany, New York was hit by a ransomware attack which forced them to shut down their systems. They decided against paying the ransom because they had much of their data backed up. They did not release the amount of the ransom, but noted the demand changed a few times. Amanda Fries of the *Times Union* reports they ended up paying an estimated $300,000.00 to recover from the attack (Fries 2019). Nine months later, on Christmas day 2019, the Albany International Airport was hit with a ransomware attack. The airport had a backup system in place, but the backup shared a drive with the main system and was also compromised in the attack. Based on the advice from their insurance company, Michael Novinson reports the Albany County Airport Authority decided to pay the ransom which was above their insurance policy's $25,000.00 deductible but below $100,000.00. Fortunately, the hackers provided a decryption code which allowed them to recover their data (Novinson 2020).

The Town of Colonie was fortunately in a better position than many of these other local governments. New York state has had cybersecurity as a major topic with the most proposed cybersecurity laws of any state between 2015-2019 (NCSL 2020). While the state has not been as successful at passing these laws, clearly some of the local governments have taken this issue to heart. The Town of Colonie realized the importance of cybersecurity as it had invested around $50,000.00 in a secure backup system three years prior to the ransomware attack on the town (Carbonite 2020; Franco February 2020). Despite fears of potentially becoming another Baltimore, the leaders ultimately decided to trust their backup system and IT department by refusing to pay

the $400,000.00 ransom demand. Using the backup system, they were able to continue to maintain day-to-day operations while the IT department worked extensive hours of overtime to restore their systems. Jim Franco of *Spotlight News* reports that over two weeks they brought in all 500 of the town's computers to be reset with the backup (Franco February 2020). While Colonie still suffered some consequences, it fared far better than many other cities mentioned and likely better than it would have by paying the ransom.

There is clearly great disparity in the outcomes of these examples. While many state and local governments have been caught under prepared, some, like the Town of Colonie, were aware of cyber security issues and have been working to better prepare their state and local institutions to the variety of cyber threats that exist. As stated before, the threat from ransomware was not significant until recently. While state governments have had little time to adapt to the rapidly emerging ransomware threat, they have been working to better prepare for cyber security issues in general. These efforts have clearly varied in their effectiveness. What policies have been successful? Has legislation on cybersecurity helped to avoid or mitigate the damage caused by ransomware attacks?

Argument and Approach

In spite of the enormous potential costs and consequences from ransomware attacks are enormous, governments have generally been slow to address cybersecurity concerns. Seventy-eight countries have national cybersecurity strategies, but almost all of these countries created their strategy only after 2010, almost 20 years after the Internet was opened to the public (CSIS 2020).[1]

[1] Of course, the United States was working on these issues at least since President Clinton's administration. On February 16, 2000, the President said,

It is difficult for governments to know how to react when there is limited knowledge both on the rapidly emerging threat of ransomware and on how policies can be effective to combat this threat. Both commercial victims and insurance companies have incentives to not report ransomware payouts, as they want to avoid scrutiny and protect their reputations (Dudley 2019). Further, while insurance is government regulated in the United States, it is regulated at the state level. Thus, any data collected is diffused throughout 50 different governing bodies.

This dissertation attempts to further our understanding of the effectiveness of legislative approaches to combatting ransomware attacks by exploring how legislation on cyber security passed at the state level from 2015 through 2019 correlates with the occurrence of ransomware attacks on state or local institutions. I argue that legislation providing or mandating cyber security *training* should have the largest negative effect on ransomware attacks. Legislation providing or mandating cyber security training is likely to be one of the most important mitigating factors from a policy perspective. This is because ransomware attacks typically occur through phishing. The word is a play on fishing because the strategy used in the two acts is the same – bait and hook. In phishing, the bait or lure is the text and appearance of the email, which is typically modeled after a common company's legitimate email and is used to trick its victim into getting hooked by following a link or attachment that can steal personal information or download malware, such as ransomware. Another common part of the lure is to create a sense of urgency by creating a false deadline to respond, such as stating the target's account will be deactivated within 24 hours if no action is taken. Novice attempts at phishing are typically easy to spot, as the lure is riddled with

---

> We know that we have to keep cyberspace open and free. We have to make, at the same time, computer networks more secure and resilient, and we have to do more to protect privacy and civil liberties. And we're here to work together (White House at Work 2000).

Yet, it still took until 2003 before a national cybersecurity strategy was adopted in the United States (CSIS 2020).

typos and grammatical errors. But cyber criminals have begun to excel at the art of subterfuge in phishing emails. Emails can be sent which appear in every way to come from legitimate organizations, such as banks, except that instead of coming from an @bank.org email address they come from @bank.com or other similar ruses. Thus, training government employees to recognize these threats is an increasingly important component of thwarting cybersecurity threats.

I evaluate the evidence for a relationship between types of cyber-legislation passed and the amount of ransomware attacks at the state level in the United States over the period of 2015-2019. To measure the presence of different types of cybersecurity legislation, I use data from the National Conference of State Legislatures (NCSL). This allows me to characterize variation in the adoption of cyber policies over time for all US states during the temporal domain of the study. The NCSL is an interstate organization whose mission "is to advance the effectiveness, independence and integrity of legislatures and to foster interstate cooperation and facilitate the exchange of information among legislatures" (NCSL 2020). One way they accomplish this is by tracking the legislation which has been proposed and if it has passed or failed to become law. They have tracked cybersecurity legislation in all 50 states, the territories, and commonwealths in the United States. They provide brief synopses of each law that was proposed and note if it has passed, failed, or is still pending. This information has to then be turned into usable data through the use of keyword algorithms to create variables for each type of legislation on cybersecurity. A limitation of this method is that it relies on the brief synopsis provided by NCSL, which may not use the same terms used in the actual laws and may not use the keywords in the algorithms. However, this allows a great deal of legislation data to be changed into a usable form.

To measure my outcome variable, I use data on successful ransomware attacks on state and local institutions from StateScoop.com, whose focus is on "news and events impacting technology

decisions in state and local government" (Freed 2019). StateScoop have built on previous research to develop a database of every known public-sector ransomware attack since 2013 by compiling attacks which have been made public in the news.[2] At the time of this writing, the total number of recorded attacks is 368. They track the target of the attack, strain of ransomware used, ransom amount demanded, and whether the victim paid or not. Unfortunately, due to the potential reputation costs, victims have incentives not to report attacks or to not fully report. Allan Liska explains, "Ransomware attacks are not always publicly reported by state and local governments and there is no centralized reporting authority, similar to HIPAA requirements, for these agencies" (Liska 2019). In some incidents were reported but the details on if the ransom was paid or how much was paid was not provided by the victim, likely to try to protect their reputation. Further, StateScoop acknowledges that smaller events, which likely occur daily throughout the country, go unreported (Freed 2019). This underreporting means the data only reflects a subset of attacks. In this case, it reflects attacks on the public sector which were large enough to be reported in the news. Despite this limitation, this is one of the most comprehensive data sets available on ransomware attacks.

In order to test the relationship between these two variables, this study uses regression models. The models help show the correlation between the types of legislation, which are the primary independent variables, and the number of ransomware attacks by state, which is the dependent variable. Legislation typically takes time to develop and implement; and can sometimes

[2] Initially on May 13, 2019, StateScoop reported on a dataset of 169 ransomware attacks, which was compiled by Allan Liska from Recorded Future, a cyber security company. Liska compiled most of the dataset by reviewing local papers and local television news reports, as "most of these incidents are not "big enough" to be considered national news […] (Liska 2019). StateScoop has taken up the mantel to continue tracking ransomware attacks since Lisa's initial report. I spoke with Colin Wood, the managing editor from StateScoop, on August 19, 2020. He explained that their first step was to contact some cybersecurity companies to try to obtain additional information on ransomware attacks. Since that time, they have continued to update the dataset based on local news and television reports. They use Google alerts, which update them as new stories are posted online. Then they sift through articles to compile as much information about the attack as possible to update their dataset.

be reactionary. For example, a state may suffer a few cyberattacks in a year leading them to enact legislation in reaction to these threats. To account for this, I use a lagged dependent variable in the regression model.

In addition to the primary independent variables, I include five other independent variables as a control for the models. The first two variables are included to account for the differences in state population size and technology. I use the estimated average population for each state for the 2010-2019 decade and the number of households per state with access to the Internet. I took the natural log of these variables to help adjust for the skew caused by states with substantially larger population and internet sizes. I also accounted for differences in cybersecurity budgets with a variable for the estimated cybersecurity expenditure per state per year. Finally, the literature suggests political party may have an effect on state cybersecurity. To control for this effect, I included a variable for the political party of the governor per state and a variable for the political party of the legislature. The legislature can include a varying number of seats per state and also includes both a house and senate per state, which can all have more subtleties than a variable which reflects the simple majority. To account for these subtleties, I used the percent of the total legislature that was either Republican or Democrat.

The initial models provide mixed results on the effects of state cybersecurity legislation on the number of ransomware attacks. When I analyze data from the whole 2015-2019 period, a number of cybersecurity legislation variables which are statistically significant, but in the opposite direction expected. Instead of a negative relationship with the number of ransomware attacks, these variables show a positive effect. However, when I isolate 2019 and test for the effects of all cybersecurity legislation from the preceding years on the number of ransomware attacks in 2019, the results provide evidence that state cybersecurity legislation can have a negative effect on the

number of ransomware attacks. In particular, state cybersecurity laws on data breaches have a negative relationship ransomware attacks. The reasons for the mixed results could be due to the great changes occurring during this timeframe. The initial period was a reactionary period as ransomware switched from indiscriminate attacks to targeted attacks against state and local institutions, while state governments on average increasingly became more active in enacting cybersecurity legislation. Then by 2019, the results of these laws began to take shape and states which had enacted more cybersecurity legislation, especially if focused on data breaches, tended to have less ransomware attacks.

Study Context

Research on the efficacy of legislation mandating or providing cyber security training to prevent or mitigate ransomware attacks is critically needed as the issue is quickly becoming a crisis. As mentioned, the United States alone likely suffered more than $7.5 billion in damages caused by ransomware in 2019 (Emsisoft 2020), up from an estimated $325 million in 2015 (Morgan 2018). The speed of this increase in cyber extortion has been matched only by an explosion of growth in cyber insurance. Renee Dudley reports, “between 2015 and 2017, total U.S. cyber premiums written by insurers that reported to the NAIC doubled to an estimated $3.1 billion” (Dudley 2019). Instead of solving this issue, cyber insurance appears to be part of the problem. According to Dudley, since insurance companies are willing to pay ransoms, more ransomware attacks are committed and, inevitably, more companies are purchasing cyber insurance to manage their risk (Dudley 2019). Thus, the cost of ransomware attacks appears likely to continue to increase becoming more of a threat to the global economy.

The costs of ransomware are not only monetary. Commercial or governmental victims can suffer extensive down time, delays, and reputational costs. The average number of days of downtime due to a ransomware attack rose to 16.2 days in the last quarter of 2019 (Siegel 2020). That is over half a month of potential lost revenue for businesses or lost services for government institutions. Siegel (2020) explains the increase is due to a high rate of attacks on larger enterprises and a new tactic used by some ransomware perpetrators. "In Q4 Ryuk[, a strain of ransomware,] actors began using a "Wake-on-Lan" feature to turn on devices within a compromised network that were initially powered off" (Siegel 2020). In other words, once infected with ransomware the program forces systems that are off to be powered back on and become infected, increasing the scope of the attack.

Downtime and delays can occur whether the ransom is paid or not, even if the victim has proper backups in place. As previously discussed, the attack on the Town of Colonie was relatively inexpensive. The town refused to pay the ransom because it had backup systems in place, which their IT staff was able to use to recover their systems. However, even a city as well prepared as the Town of Colonie had service issues and down time until the IT department was able to finish implementing the recovery of their 500 affected computers around two weeks later (Franco February 2020). Likewise, the ill-prepared city of Baltimore, had down time equivalent to the severity of the attack, which infected over 10,000 computers, and their lack of preparedness by not having backups in place. It took over a month to restore all city employee's email systems and around three months before they were finally able to distribute water bills (Chokshi 2019).

While down time and delays can be costly and frustrating, reputational costs of falling victim to a ransomware attack can lead to additional financial consequences due to loss of business and customers. One survey found that 59% of people would likely avoid using an organization that

experienced a cyberattack and 58% would leave a business affected by 2 or fewer attacks (Whitney 2020). Though these figures are based on hypothetical responses, consumers' actual reactions to real attacks generally align with survey results. In 2013, Target suffered a data breach of customers' personal information. Target's reputation plummeted soon after from a brand index rating on consumer perception of 20.7 in 2013 down to 9.4 in 2014 (Hospelhorn 2020).

Reputation is not only important for commercial victims, but also governmental victims. Government officials who are in charge when a ransomware attack occurs can suffer reputation costs and even potentially lose their position. For example, the IT manager in Lake City, FL was fired after the city suffered a ransomware attack. The attack ended with the city's insurer paying a ransom of around $460,000 and the city had to spend additional time and money to recover data which was lost in the attack (Robles 2019). Further, elected officials will undoubtedly see political opponents highlight preventive failures in future elections.

Ransomware is also evolving into a national security threat. Some forms of ransomware have changed from indiscriminate, blanket attacks to well planned, targeted attacks increasing in potential societal costs. Healthcare, law enforcement, and local government are being increasingly targeted. These institutions provide critical services. The criminals are focusing on these types of actors because these actors feel increased pressure to pay the ransom as often they need their computer systems as a matter of life or death. Further these entities are also typically at higher risk as their systems are more susceptible to attack. Healthcare facilities were allocated government funds to encourage the use of electronic health records increasing use of these records from 9.4 percent in 2008 to 96.9 percent in 2014. This rapid digitization of health records was not followed by a similar increase in IT infrastructure and resources, as no government funds were allocated for such measures. Thus, the rapid increase in IT utilization has left many healthcare facilities exposed

and vulnerable to cyber security threats (Spence, et al. 2018). In fact, in 2020 two ransomware attacks on healthcare facilities made global news due to the severity of the outcomes. An attack on Universal Health Services Inc., a company with over 250 hospitals throughout the US, forced facilities nationwide to use paper backups causing delays and potentially diverting patients elsewhere (Bajak 2020). Worse yet, a ransomware attack on Dusseldorf University Hospital may be responsible for the death of a patient. The attack disabled computer systems forcing a patient in need of critical care to undergo a lengthy transport to another hospital 19 miles away where she later died (Tidy 2020). With lives on the line, the decision for these institutions to pay or not pay a ransom are truly dire and a serious attack could create a national security crisis.

Another target with national security implications and potentially devastating societal costs is the election infrastructure. These venues are prime targets for ransomware attacks because they are manned by local authorities, who have varying levels of cybersecurity competency, and an approaching election creates an urgency to recover a system quickly in the event of an attack. "[A]dversaries also recognize that government cannot afford to shut down, especially during a contentious election season, and that a fallback to manual processes would be unacceptable. With so much at stake, it would be a difficult choice whether or not to pay the ransom" (Moore 2019). Even if a manual process could be implemented to count the votes, the reputational costs would be potentially enormous as doubt would be cast a cloud over the election results (Tucker, et al. 2020). These fears are not unwarranted: Florida had been a victim of a ransomware attack in 2016 only weeks before the election (Flores 2020). Further, ransomware criminals were active during the 2020 US election cycle by 'spamming' fake political campaign emails, tricking unsuspecting victims into downloading ransomware when they tried to unsubscribe (Solomon 2020).

There are further potential national security consequences of failing to act preventively on ransomware from both state and non-state actors. There is evidence some state actors have begun developing and spreading ransomware as an offensive cyber-weapon. For example, in 2017 two strains of ransomware were released with devastating effects around the world. First, the WannaCry ransomware strain quickly "infected over 300,000 computers in over 150 countries" (KnowBe4 2020). The attack is believed to have come from North Korea using an exploit stolen from the NSA (Trautman and Ormerod 2018). Later that year, it is believed Russia developed the NotPetya ransomware strain to attack Ukraine. However, similar to the WannaCry strain, the ransomware quickly spread beyond Ukraine around the globe (Trautman and Ormerod 2018; Palmer 2019). Disturbingly, it appears that unlike most previous ransomware this strain was developed not as a financial motivation, but solely as a weapon of cyber-destruction. The NotPetya strain was designed to encrypt the victim's files and then essentially throw away the key, potentially destroying the data forever (KnowBe4 2020). The WannaCry[3] and NotPetya[4] strain caused billions of dollars of damages worldwide, demonstrating the threat of state developed ransomware.

There are also national security concerns regarding non-state actors' use of ransomware. There are fears that paid ransoms could potentially fund terrorism. While there have been no confirmed reports of ransomware payments going to terrorists, many fear that terrorist groups could be utilizing this method as a source of financing as there is often no way of identifying the source of the attack (Blannin 2018). Others fear that terrorists could attempt a largescale ransomware attack (Acharya 2017), with some estimates advising "[it] could cost the global

[3] The WannaCry ransomware attack caused an estimated $4 billion in damages worldwide (Reinsurance News 2017).

[4] The NotPetya ransomware caused an estimated $10 billion or more in damages around the world. In fact, as few as nine companies lost and estimated $1.8 billion due to this ransomware strain (Tehrani 2017).

economy $193 billion and impact more than 600,000 businesses worldwide" (Chung 2019). Despite these fears, the US Cybersecurity Infrastructure Security Agency believes that terrorists do not currently have the "computer network capabilities and propensity to pursue cyber means." Yet, they do acknowledge the threat of cyberterrorism may increase in the future as the younger, more technologically savvy generation could join terrorist organizations (CISA 2020).

While grand cyber-attacks may be beyond terrorist organizations' reach, the threat of a terrorist led ransomware attack is not as farfetched given the ease of entry into this form of cybercrime. Ransomware has developed into a service economy for aspiring criminals who may not have sophisticated programming skills. Indeed, "a basic appeal of ransomware is simple: it's turnkey. Unlike many other forms of cyberattacks, ransomware can be quickly and brainlessly deployed with a high probability of profit" (Singh et al. 2017). Ransomware as a service (RaaS) is a term used to describe the illicit economic activity between ransomware creators and purchasers. The creators sell their ransomware to buyers for a fee and then often take a portion of the ransoms acquired, as well. Meland, et al. (2020) explain that "RaaS can have different formats, such as source code that the buyer compiles himself, pre-compiled binaries or an interface where the buyer inputs information about the victims. This collaborative strategy is a way of achieving a faster rate of infections with a lower risk of getting caught" (Meland, et al. 2020). In other words, would be criminals, including terrorists, can easily enter the market to obtain and then spread ransomware. With this risk in mind, governments need to take actions now to make sure they are properly prepared to avoid inadvertently funding terrorism while victim to a ransomware attack.

In sum, ransomware is clearly enormously costly. The financial costs of either paying the ransom or recovering from an attack have been high, especially in the case of the City of Baltimore. Yet, even cities which are better prepared, such as the Town of Colonie, can suffer delays and

downtime of critical infrastructure. The reputational costs can lead to lost business and erode trust in the organization. A lack of credibility can be potentially disastrous for an election. Finally, these costs are part of a criminal economy which is encouraging further ransomware attacks and potentially funding terrorist activities. Therefore, the issue of ransomware is critical and understanding how to effectively prevent it is only becoming more important. However, the efficacy of different policy tools remains poorly understood. Understanding whether and how legislation and policies are helping to deter or thwart ransomware attacks against state and local government institutions will inform policy makers' efforts to fight this emerging threat.

Outline

This dissertation consists of seven chapters, including this introductory chapter. In Chapter II, I summarize and synthesize the existing literature on legislation and cyber threats. This review is critical as a foundation for this study. It not only helps in understanding how legislation has and will affect ransomware, but also demonstrates how this study builds upon the current body of knowledge.

Chapter III presents my theoretical argument about how and when cybersecurity legislation should be effective at combatting ransomware. Chapter III builds on the previous chapter by directly tying existing theories to the research question I investigate here – what policies are most effective against ransomware? I examine ransomware strategies in more detail to understand what strategies cybersecurity experts recommend to combat ransomware and assess their potential effectiveness. Based on these recommendations, I argue that legislation providing or mandating cyber security *training* should have the largest negative effect on ransomware attacks. This is

because ransomware attacks typically occur due to human error from falling victim to phishing, which could be prevented with proper training.

In Chapter IV I examine how states have varied in their policy approaches to cybersecurity and present descriptive trends in cybersecurity legislation. This chapter explores what types of specific issues cybersecurity legislation has addressed and the frequency with which proposed legislation becomes law using a database of cybersecurity legislation at the state level from 2015-2019 from the National Conference of State Legislatures.

In Chapter V I outline a research design to analyze when and how cybersecurity legislation has deterred ransomware attacks and report the results of my analysis. I combine the data explored in Chapter IV with data on successful ransomware attacks on state and local institutions from StateScoop.com (Freed 2019).

Chapter VI builds on the previous chapter by exploring case studies of the legislation which the model indicates may have a negative impact on ransomware attacks. These laws are explained in more detail to better understand the mechanisms which may be helping them to prevent ransomware attacks.

Chapter VII concludes with outlining policy prescriptions for how states should approach future legislation. This section hopefully can serve as a guide for legislators to help state and local institutions better prepare for the rapidly emerging threat of ransomware. I also propose potential avenues for future research.

CHAPTER II

LITERATURE REVIEW

This chapter explores the broader literature on cybersecurity legislation to illustrate how this dissertation adds to the prior body of knowledge and to answer the following questions: Why has there been a relative lack of policy and research on cybersecurity? What factors have pushed cybersecurity concerns to the sidelines? The short answer is that politicians, and society in general, are often slow to adapt to technological changes (Moor 1985). To explore these issues further, I first examine the definitions of cybercrime. Then in the second section, I briefly examine the history of cybercrime in general to show the trends and how ransomware has recently emerged as a significant cybersecurity threat. The third section provides a brief history of cybersecurity legislation in the United States to provide insight into how the United States has attempted to address cybercrimes. Finally, in section four I review the literature on the effectiveness of cybersecurity legislation at combatting cybercrime. This review provides the foundation to then review cybersecurity legislation's effect on ransomware in the following chapter and developing the argument that legislation mandating or providing training should have the largest negative effect on ransomware attacks.

Defining Cybercrime

The information age took off with the spread of the Internet in the 1990s which brought significant benefits to global communications and commerce. Some people, such as Barlow (1996), even believed the Internet would be a virtual utopia free from the vices of the real world.[5]

[5] "A Declaration of the Independence of Cyberspace" was written in 1996 by John Perry Barlow, who imagined the Internet would be a utopia. He is a founding member of Electronic Frontier Foundation a nonprofit organization

However, the opportunity and freedom offered by the Internet were also available to would be criminals, who quickly capitalized on the lack of governance and the anonymity the Internet can provide. What was old became new again, as cybercriminals brought ancient vices, such as theft, fraud, and vandalism, onto the Internet firmly cementing a new era of cybercrime.

Defining cybercrime is complex as the term encompasses a wide variety of criminal acts and behaviors (Jane and Martellozzo 2017; Sarre, et al. 2018). Cybercrime can include crimes, such as theft, that have always occurred in the real world, but are now also taking place online. Yet, the term can also include other crimes, such as sextortion[6], which occur only in the digital world and have no clear real-world parallels (Jane and Martellozzo 2017). Many criminals now utilize the internet to facilitate more traditional criminal acts, such as drug trafficking (Jane and Martellozzo 2017; Sarre, et al. 2018). Still other crimes, such as stalking, bullying, and domestic violence, can often simultaneously occur offline but the Internet and other emerging technologies amplify the "abuse, harassment, and coercion" (Jane and Martellozo 2017).

To include this wide range of acts and behaviors, scholars have tried to breakdown cybercrime in various ways to make it more manageable. Gordon and Ford (2006) define cybercrime as a continuous scale between Type I, which is crime that relies on technical skills like hacking, and Type II, which relies more on social interaction such as cyberbullying. Most acts fall somewhere in between utilizing both technical and social aspects, such as phishing. This ambiguity

---

whose goal is to defend civil liberties in the digital world. In the essay, he argues that governments should stay out of cyberspace as the digital community is creating a "civilization of the Mind in Cyberspace," which "all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth" (Barlow 1996). Further, he believed the Internet would be a place where anyone could express their beliefs and "legal concepts of property, expression, identity, movement, and context do not apply" (Barlow 1996).

[6] Jane and Martellozzo (2017) define sextortion as "an emerging criminal practice in which perpetrators gain remote access to computers to obtain intimate or compromising footage of targets who are then blackmailed into performing sex acts (thereby becoming entrapped even further)." While the crime includes aspects of some traditional crimes, it does not fit easily into any one category. They explain "Sextortion, for instance, can involve elements of stalking, home invasion, theft, blackmail, pedophilia, domestic violence, sexual exploitation, harassment, and abuse, and organised crime" (Jane and Martellozzo 2017).

still makes it difficult to classify acts as it is difficult to measure how technical versus social some crimes may be.

Another approach tries to give cybercrime a more clear definition by breaking cybercrime into three main categories: targeting a computer, using the computer as the instrument to commit a crime, and using the computer to help facilitate the crime (Clifford 2001; Grabosky and Walkley 2007; Khadam 2012). Clifford (2001, page 15) explains,

> Cybercrimes are often characterized as falling into three categories: crimes in which the computer is the target of the criminal activity; crimes in which the computer is a tool used to commit a crime; and crimes in which the use of the computer is an incidental aspect of the commission of the crime. (Clifford 2001, page 15)

In other words the first category, where the computer is the target, can include crimes such as hacking or malware. The second category focuses on the computer as a tool which is necessary to commit the crime, such as digital fraud or cyber espionage. Finally the third category is the use of a computer as part of a crime as one of a few options, such as illicit drug sales which could have also been done over the phone or in person (Clifford 2001). This system certainly helps to clarify the criminal acts but is hindered by its rigid classification which cannot account for many of the subtleties of cybercrime that can cross all of the categories, such as sextortion.

A third approach is to focus on how technology is involved in the crime, but in a less rigid way from the second definition. McGuire and Dowling (2013) break cybercrime into two categories: cyber-enabled and cyber-dependent. Cyber-enabled crimes are enhanced or assisted by the Internet (McGuire and Dowling 2013). This category would include both cyberbullying, which is amplified by computers and the Internet (Jane and Martellozzo 2017), and drug-trafficking, which can be done more easily with the aid of the Internet (Sarre, et al. 2018). On the other hand, cyber-dependent crimes require computers and the Internet (McGuire and Dowling 2013). Crimes in this category include hacktivism and malware (Sarre, et al. 2018).

Each definition certainly has limitations, yet these definitions offer lenses to view ransomware, which is the focus of this dissertation. Ransomware will be reviewed in more detail later, but this form of cybercrime can have both a highly technical and a human interaction side so it would oscillate depending on the ransomware strain somewhere around the middle of Gordon and Ford's (2006) scale. Clifford (2001), Grabosky and Walkley (2007) and Khadam (2012) would have a difficult time placing ransomware as it has aspects which involve the computer as the target of the criminal activity, such as the malware encryption, but also involves the computer as the instrument used in the crime, such as through phishing and extortion. Finally, most ransomware would certainly fall under McGuire and Dowling's (2013) cyber-dependent category, as a computer is necessary for the malware and encryption aspects of ransomware. However, some of the less sophisticated forms of ransomware, such as fake anti-virus scams, could be seen as cyber-enabled (McGuire and Dowling 2013) as they could potentially be carried out offline as well. While none of these definitions can pinpoint ransomware exactly, they provide a backdrop that will be used to help determine the best methods to counteract this rapidly emerging form of cybercrime.

Brief History of Cybercrime

Since this dissertation focuses on ransomware, this review will focus only cybercrime that is similarly cyber-dependent. The struggle defining cybercrime shows that the term certainly encompasses a wide variety of criminal activity. In fact, one of the earliest acts considered a cybercrime dates back to 1834 when the French Telegraph System was "hack[ed … to] steal financial market information" (Herjavec 2019). Criminals have continued to evolve with the times

as attacks switched from telegraphs to telephones.[7] Then, as computers were developed, criminals soon followed. In 1969 the first virus disabled a computer at the University of Washington Computer Center. Then in 1970 one of the first cybercriminal sprees was begun by Kevin Mitnick, who tricked employees at Nokia and Motorola into providing him codes and passwords so he could access internal computer systems. Despite the lengthy history of cyber related crimes, the first person to be convicted specifically of a cybercrimes was Ian Murphy in 1981 when he hacked into AT&T's network (Herjavec 2019). Criminals clearly have evolved with technology.

To help understand this evolution, it is useful to view cybercrime through the lens of globalization. There is no consensus on the definition of globalization in the literature (Scholte 2005), but the focus of this dissertation is on changes in governance due to the emerging cybersecurity threat of ransomware. Due to this focus, globalization in this dissertation is defined in terms of respatialization or the process of deterritorializing social relations due to the increase in transplanetary connections (Scholte 2005). In other words, state boundaries and even geographic location matter less due to the increase in the speed of travel and communications which allow people located anywhere on the planet to interact instantaneously.

According to many scholars, respatialization has consequences for governance (Rosenau 2003; Scholte 2005). The increase in transplanetary connections have made states ill-equipped to deal with the issues highlighted by the dark side of globalization. Rosenau (2003) argues that the increase in these transplanetary connections, or as he calls them "distant proximities,"[8] has led to fragmegration or simultaneous processes of fragmenting and integrating across all levels of

[7] For example in 1878, only two years after its invention, teenagers were disrupting phone calls by "repeatedly and intentionally misdirecting and disconnecting customer calls" (Herjavec 2019). Later in 1955, David Condon was able to trick the phone system by whistling songs that caused the system to allow him to make calls to any phone number in the world for free (Herjavec 2019).

[8] Rosenau (2003) describes respatialization as an increase in "distant proximities," which oxymoronically implies that what happens far away has effects close by and vice versa (Rosenau 2003).

governance (Rosenau 2003). Fragmegration has also led to crises of authority at all levels of governance creating gaps which are not necessarily filled automatically by a different level of authority (Rosenau 2003). Rosenau elaborates, "[I]t is otherwise likely that the diminution of state authority throughout the world has led not only to a shift of authority to other collectivities but also to vacuums of authority, to situations in such disarray as to be lacking any centers of authority" (Rosenau 2003). These vacuums or gaps in authority and governance have led rise to the "dark side of globalization," which includes global terrorism, drug trade, and cybercrime (Heine 2011).

The early incidents of cybercrime certainly have evidence of this deterritorializing, fragmegration process. Schneier (2018) explains the criminals who hacked the French Telegraph System were the Blanc brothers, who were stock traders. At the time, information on the stock market was transported by mail coach from Paris to Bordeaux. The mail coach was slow and took several days. Many traders tried to obtain information ahead of time by using messengers or carrier pigeons to get an advantage in the stock trade. The Blanc brothers realized that to obtain the information they wanted they no longer had to physically move the messages from Paris to Bordeaux. Instead, they bribed a telegraph operator "to introduce deliberate errors into routine government messages being sent over the network" (Schneier 2018). These errors were codes that the Blanc brothers interpreted to gain an edge in the market. When their scheme was uncovered in 1836, the brothers were not convicted as there was no laws against misusing the telegraph network (Schneier 2018). In other words, the technology of the telegraph allowed for the deterritorialization by decreasing the need for physical messengers and increasing the speed and distance of communication. This advancement also created a crisis of governance over the use (or misuse) of this new technology which was not yet regulated.

To solve these problems of authority and governance, Scholte explains, "Authority has become increasingly 'multi-level' or 'multi-scalar'" (Scholte 2005). Some problems are now better addressed at the local level, while others can be better handled at the transnational level. Similarly, Rosenau argues that governance must become "as complex as its environment" (Rosenau 2003). He suggests a new form of governance, which he calls "mobius-web governance," that, like Scholte suggests, includes sub-state and supra-state entities (Rosenau 2003). Unlike Scholte's suggestion, Rosenau's system is far more complex and takes the shape of a web as opposed to the more traditional hierarchical forms of governance (Rosenau 2003). Yet, they both point out the need for a restructuring of governance due to respatialization.

Respatialization has only increased with the exponential spread of the Internet starting in 1989, which has allowed the communication to truly become transplanetary through the creation of the digital world – cyberspace. As mentioned previously, cyber-dependent crime quickly followed behind. Many of the early Internet crimes were essentially Internet vandalism where budding hackers or "cyber-vandals" could show off their skills to the nascent underground hacker community (CR 2017).[9] These pranks quickly gave way to more serious crimes as ecommerce and ebanking emerged creating avenues for illicit financial gains through digital theft. For example in 1994, a Russian software engineer, Vladimir Levin, hacked Citibank and stole $10 million. Another example comes from Max Butler, who used malware to steal "millions of credit card numbers and [make] around $86 million of fraudulent purchases" (Herjavec 2019).

[9] CR (2017) explains that many of these early hackers just wanted to create notoriety and maybe get a few laughs. They often took over or defaced websites with comical images to impress other hackers. "One infamous example from this period is the MS Blaster virus, also known colloquially as the 'LoveSan' virus. The virus forced the system to restart after 60 seconds and included two hidden messages in the code: 'I just want to say LOVE YOU SAN!!' and 'Billy Gates why do you make this possible? Stop making money and fix your software!!'" (CR 2017). Another infamous example was the 1999 attack on the White House's website. The hacker defaced the site with "red graffiti stating "Hacker wuz Here" (Alexander 2007).

Other cybercriminals sought to breach government and businesses' networks to steal data containing personal information, such as social security and credit card numbers, and proprietary information, such as research and technology, to use or sell on the black market. Breaches can occur through hacking, phishing, theft, inside jobs, or negligence. While data breaches have occurred for some time, the most significant ones began occurring since 2005 as most companies had converted to electronic records by that time. The number of breaches per year has been increasing overtime. Some of the notable breaches were AOL had 92 million records compromised in 2005, Heartland had 130 million compromised in 2009, Sony had 77 million records compromised in 2010, Target had 70 million records compromised in 2013, and Yahoo had one billion records compromised in 2016 (De Groot 2019).

When these breaches target proprietary information they can be considered cyber espionage. For example in 1998, the Moonlight Maze operation targeted American military technologies. Thousands of documents were stolen when hackers infiltrated the Wright Patterson Air Force Base. While Russia was blamed, there was not enough proof available to pursue them (Paganini 2017). Another notable example is the Night Dragon operation conducted by Chinese hackers, who targeted European and American energy companies. The hackers were able to steal maps with locations for potential oil reserves (Paganini 2017).

At the same time, criminals began creating computer viruses and malicious software or malware, sometimes for the sole purpose of destruction. The first major virus outbreak was in 1988. Robert Morris of MIT intended to measure the size of the internet but instead created the first worm and first denial-of-service (DoS) attack (SentinelOne 2019; Townsend 2019).[10] "[The

[10] A denial-of-service (DoS) attack prevents users from accessing "systems, devices, or other network resources" (CISA 2019). A DoS attack is caused by "flooding the targeted host or network with traffic until the target cannot respond or simply crashes" (CISA 2019).

program] replicated so aggressively that the early internet slowed to a crawl, causing untold damage" (SentinelOne 2019). The 1990's saw the growth of anti-virus software. Initially there were less than a hundred thousand malware samples, but these numbers quickly rose to around five million in 2007. "By 2014, it was estimated that around 500,000 unique malware samples were being produced every day" (SentinelOne 2019).

This rise in malicious software led to some significant attacks. One of the most notorious was the ILOVEYOU worm, which infected millions systems around the world only hours after its initial release (Townsend 2019). Ogu, et al. (2020) explain the 2000 ILOVEYOU malware outbreak "infected about 10% of the global internet-connected computers, caused the global economy damages of up to $8 billion, with an added $15 billion estimated as the cost for removing the malware" (Ogu, et al. 2020). Yet, the legal charges against the two young Filipino programmers responsible for these attacks were dropped because of the "the absence of effective trans-national legislation" (Ogu, et al. 2020). In other words, just like the example of Blanc brothers in 1834 France, there was a gap in authority and governance due to this new technology, which was exploited on a transplanetary level by the ILOVEYOU virus.

With so many devastating cybercrimes, it may seem that governments are powerless to fight the dark side of globalization. However, some scholars, such as Krasner (2001) and Hastings (2010), argue that the state is still capable and may actually be better equipped to deal with issues due to globalization. Krasner (2001) explains, "Technological changes over the last 200 years have increased the flow of people, goods, capital, and ideas – but the problems posed by such movements are not new. In many ways, states are better able to respond now than they were in the past" (Krasner 2001). Krasner supports his argument by citing the difference in state capacity to control the negative effects of the Asian financial crisis in the late 1990s to the Great Depression

(Krasner 2001). Similarly, Hastings (2010) argues that while it is easier for people, including illicit groups, to move and communicate across borders in a globalized world, the technologies and infrastructure are still, to a large part, controlled by states (Hastings 2010). This control is especially evident at "chokepoints, such as international airports." In other words, states still control the infrastructure of globalization which gives them enough power to overcome the new threats, such as global terrorism, highlighted by the dark side of globalization.

A rapidly emerging threat from the dark side of globalization certainly is putting states' capacity to the test. Ransomware is in many ways a combination of three previously mentioned major issues: data breaches, malware, and theft (through extortion). Ransomware is a type of malicious software or malware which after infecting a computer tries to extort the victim (Hernandez-Castro, et al. 2020). While the idea has been around for some time, it took the diffusion of sophisticated encryption technology and the development of cryptocurrency, such as Bitcion, for this cybercrime to truly take off (Hampton and Baig 2015). When these developments came together in 2013 they took ransomware from a minor nuisance to a global threat costing the global economy billions each year (Emsisoft 2020). For example, in 2017 the WannaCry ransomware strain infected around 300,000 computers throughout the world and caused losses around $4 billion (Reinsurance News 2017).

Certainly, Krasner (2001) and Hastings (2010) line of thinking could be used to help explain ransomware attacks prior to 2013. Ransomware attacks prior to that time were more of a nuisance that cost victims usually around a few hundred dollars an attack (Keizer 2011; Savage, et al. 2015; Scott-Cowley 2017). In part, these low ransom demands were due to a lack of a secure, scalable payment method (Hampton and Baig 2015). While larger ransoms could have been demanded through wire payments, the criminals understood if they drew too much attention the

police could become involved and use traditional means of tracing wire payments and freezing bank accounts. Thus, the state, like Hastings (2010) argues, had control of the 'chokepoints' through the financial institutions.

However, with the rise of cryptocurrencies, such as Bitcoin in 2009, ransomware criminals found they could retain their anonymity and request higher ransoms by demanding the ransom be paid in cryptocurrency, which is very difficult if not impossible to trace. This change allowed ransomware criminals to change their targets to businesses and other enterprises. They have also been steadily increasing their demands with some, as noted above, now in the hundreds of thousands of dollars. Ransomware is quickly becoming one of the most significant cyber threats. It is therefore critical that this threat be studied so that proper countermeasures can be taken to stop ransomware from continuing to grow.

Brief History of Cybersecurity Legislation in the US

The rapidly emerging threat of ransomware is an aspect of the dark side of globalization which requires a restructuring of authority at the national, subnational, and supranational levels. However, this threat has only become relevant recently with little time for governments to react. Yet, ransomware shares many characteristics with other, more longstanding cybercrimes, such as data breaches, malware, and digital theft. The government has had more time to react to these other cybercrimes, which has led to the passage of several cybersecurity laws. Still these laws took years to be passed and were still considered by many to be insufficient in addressing cybersecurity concerns. "Cybersecurity law in the United States," explains Kosseff (2017), "currently is a patchwork of outdated privacy and computer crime laws" (Kosseff 2017). At the same time, cybercrime, as made clear in the above section, became a significant threat to the global economy.

The first section explores the reason for the delays and lack of comprehensive legislation on cybersecurity in the United States. The second section then discusses the history of cybersecurity legislation at the federal level. Then I examine how the federal legislation has been supplemented at the supranational and subnational (state) levels in the third and fourth sections.

Policy Vacuum

To better understand the history of cybersecurity legislation in the United States, this section will first attempt to answer the following questions: Why has the passage of cybersecurity legislation taken so long when cybercrime has developed so quickly? Why has there been a relative lack of policy and research on cybersecurity? What factors have pushed cybersecurity concerns to the sidelines? The short answer is that politicians, and society in general, are often slow to adapt to technological changes. Moor (1985) explains that new technology (e.g., computers) creates a policy vacuum by raising practical and ethical question about its use that cannot be answered until it is clear *how* it is being used, as the potential applications of a technology are often unknown at its inception (Moor 1985).

The automobile, invented in 1885 by Karl Benz, provides a convenient example of how technological innovation can create policy vacuums and how societies may be slow to adapt to new technologies. At first, only the wealthy were able to acquire cars, yet property damage, injuries, and even deaths from automobile accidents were quickly a problem. In Great Britain, police were already attempting to deal with overcrowded and dangerous streets due to increased traffic of carts, carriages, horses, and the recent invention of the bicycle, which youth were "furiously – 'scorching' – through towns and cities" (Emsley 1993). The addition of the automobile made these issues worse and were far more dangerous. In 1913, less than 30 years after

automobiles were invented, there were already 4,200 motor-vehicle deaths per year in the United States (*Injury Facts* 2020), while in England and Wales there 38,050 non-fatal accidents and 1,743 fatal-accidents (Emsley 1993). These numbers only continued to rise until 1972 when deaths from motor-vehicle accidents in the United States peaked at over 56,000 (*Injury Facts* 2020).

Despite the clear dangers of automobiles, legislation on the subject was slow to arrive. There was little legislation for the British police officer to use to regulate the "furious driving" that was causing mayhem on the roads.[11] The chief constable of Huntingtonshire reported that drivers often refused to stop when signaled by police, provided false identification, had faster vehicles than the police, and would often attempt to bribe the constables (Emsley 1993). It was not until 1903 when Britain introduce the Motor Car Act, which brought about some regulation, most notably the introduction of driver's licenses (Driver & Vehicle Standards Agency 2020).

Similarly, Dedrick (2020) explains that "the early traffic years of the twentieth-century were lawless. […] there were absolutely no street signs, street lights, road laws, traffic signals, brake lights, drunk driving laws, the list goes on. The streets were complete chaos" (Dedrick 2020). In the United States the first statewide speed limit was established in Connecticut in May, 1901 (History.com Editors 2009).[12] Legislation continued slowly over the next two decades as traffic signs and signals were slowly implemented.[13] The first stop light was introduced in 1914, but took

[11] Clive Emsley explains the British police officers had only the "1896 Locomotives on Highways Act, which had made it lawful to drive self-propelled vehicles of less than three tons on the roads without a man in front carrying a red flag." This law was intended for traction engines and was not useful for regulating motor-vehicle drivers (Emsley 1993).

[12] The law passed in Connecticut in 1901 limited speed for motor vehicles to 12 mph in cities and 15 mph on country roads. Prior to this some local laws were in effect, but primarily codes relating to non-motor vehicles were utilized. "In 1652, the colony of New Amsterdam (now New York) issued a decree stating that "[N]o wagons, carts or sleighs shall be run, rode or driven at a gallop" at the risk of incurring a fine starting at "two pounds Flemish," or about $150 in today's currency" (History.com Editors 2009).

[13] History.com Editors explain that "the first traffic island was put into use in San Francisco, California in 1907; left-hand drive became standard in American cars in 1908; the first center painted dividing line appeared in 1911, in Michigan; and the first "No Left Turn" sign would debut in Buffalo, New York, in 1916 (History.com Editors 2009).

another decade to become commonplace in many larger cities (Stromberg 2015). It was not until the 1950s that factory installed seatbelts started appearing in cars. In 1968, the Motor Vehicle Safety Standard took effect, which required manufacturers to install seat belts in all vehicles (Donaldson 2019). So, it took just over 80 years from the creation of the automobile to the legislation requiring seat belts in cars even though fatal accidents were steadily rising throughout this period.

Federal Level Legislation

Clearly, society and politicians can take an exceedingly long time to adjust to new technological innovations and fill in the policy vacuum (Moor 1985), even when lives are on the line. Similarly, the policy vacuum issue has affected cybersecurity legislation. Computer technology had been improving and diffusing throughout the United States since the 1950s. Yet, the first law to address concerns of crime affecting or using computers was not passed until the mid-1980s before the spread of the Internet. The Computer Fraud and Abuse Act (CFAA) was passed in 1984 and had further revisions in 1986, 1996, 2001 (Alexander 2007), and 2008 (Flowers, et al. 2013). The focus of the law was to criminalize certain acts that targeted government and (later) financial institutions' computers. It specifically prohibits "transmission of a program, information, code, or command" that causes damage to a computer or computer program, which makes the distribution of malware and other cybercrimes illegal (Alexander 2007). Flowers, et al. (2013) explains, "[The CFAA] is the most significant law to date in the US to address cybersecurity. [… However,] such laws have little effect on individuals, groups, or governments over whom the US lacks – or is unable to secure – regulatory or criminal jurisdiction" (Flowers, et al. 2013). In other words, while this law is necessary and important its reach is limited due to

the transplanetary reach of cybercrime, which in accordance with Rosenau (2003) and Scholte (2005) would require cybercrime to also be addressed at a supranational level.

Likewise, legislation on cybersecurity since the advent of the Internet in 1991 has been sluggish. Three vague federal laws were passed in the decade following the rise of the Internet which addressed cybersecurity in some way. First, the 1996 Health Insurance Portability and Accountability Act (HIPAA) was passed. The law required health organizations to secure their systems both physically and technically to protect Protected Health Information (PHI), which is essentially a patient's information, such as social security numbers and health records (Arrigo 2019). The 1999 Gramm-Leach-Bliley Act similarly requires financial institutions to protect customers' personally identifiable data. These regulations were updated in 2003 to include requirements for financial institutions to have comprehensive security plans (Wills 2020). Finally, the Federal Information Security Management Act of 2002 (FISMA) extends the requirements to protect and secure data to federal entities (Trautman 2015).

While these laws required healthcare, financial, and government organizations to secure their data, they did not provide guidelines or standards on cybersecurity, only that it be 'reasonable' (Singh 2016). Alexander (2007) explains "The many acts of legislation that have been formed still allow for loopholes and do not properly address the many threats that are occurring or are soon to occur" (Alexander 2007). Thus, even though some laws were created around cybersecurity, they were not comprehensive enough to truly address the simultaneously growing cybercrime challenges. Singer and Friedman (2014) attribute the slow development of cybersecurity policy to the fact that those making the policies are often not familiar with computers in general or cybersecurity in particular due to either age or lack of technical expertise.

The older generation of leaders are not likely to have much familiarity with computers because computers are relatively new. The personal computer was invented in 1974, but did not become widespread until the 1980s. Even then, machines were limited in their capabilities. Singer and Friedman (2014) explain, "[a]s late as 2001, the Director of the FBI did not have a computer in his office, while the US Secretary of Defense would have his assistant print out e-mails to him, write his response in pen, and then have the assistant type them back in" (Singer and Friedman 2014). These officials are not alone. In a 2015 interview with NBC correspondent Chuck Todd, Senator Lindsey Graham and Senator John McCain advised they have never used email. Chuck Todd explained,

> And he wasn't alone. In fact, a bunch of senators looked up from their typewriters to say they don't use email either. So our luddite caucus includes Tom Carper from Delaware, Orrin Hatch, Pat Roberts, Chuck Schumer said if he started emailing, he'd never stop, and Richard Shelby of Alabama. Even Bill Clinton's spokesperson insists the former president has only sent two emails in his life. (Meet The Press 2015)

The lack of familiarity with computers and cyberspace even affects the third branch of government, as eight out of nine Supreme Court justices confirmed in 2013 they also do not use email. These various leaders are in charge of establishing cyber security legislation or, in the case of the Supreme Court, determining what is legal in cyberspace, yet they have such limited experience with this area (Singer and Friedman 2014).

While the older generation lacks experience with computers in general, younger generations are not necessarily more adept at cybersecurity. A 2017 Pew Research Center survey, tested the American public's knowledge of cybersecurity and found a majority of Internet users were unfamiliar with key cybersecurity terms and concepts. In fact, only 20% of individuals surveyed were able to answer eight or more of the thirteen questions correctly. Younger and more

educated individuals tended to score better, but overall the survey found the American public's level of cybersecurity knowledge is limited (Smith 2017).

Singer and Friedman (2014) attribute this unfamiliarity with cybersecurity to a lack of interest in the technical side of computers and information technology (IT). This lack of interest is likely due to the fact that most companies have an IT department or third party IT support. Most people's focus is on their job role and anything technical is relegated to the IT support. If a printer breaks, call IT. If an application will not load, call IT. If your computer gets a virus, call IT. Singer and Friedman explain, "Anything related to the digital world of zeros and ones was an issue just for computer scientists and the IT help desk. Whenever they spoke, most of us would just keep quiet, not our heads, and put on what author Mark Bowden calls "the glaze"" (Singer and Friedman 2014).

Whether due to lack of experience or lack of interest, society's lack of familiarity on cybersecurity has created a policy vacuum (Moor 1985). This gap is present in both the policy realm and academic realm. For the policy realm, Singer and Friedman (2014) explain "the issue is perceived as too complex to matter in the end to voters, and as a result, the elected representatives who will decide the issues on their behalf. This is one of the reasons that despite all these bills no substantive cybersecurity legislation was passed between 2002 and [2014]" (Singer and Friedman 2014). During this twelve year gap there were numerous high profile data breaches (De Groot 2019), damaging viruses (SentinelOne 2019), and the initial rise of ransomware (Savage, et al. 2015). Yet, like the history of automobiles, the government has been slow to react and to fix the crisis of authority created by this dark side of globalization.

With these impediments to effective cybersecurity legislation in mind we can examine the third wave of legislation at the federal level. When President Obama took office in 2009, he quickly

announced cybersecurity as a top priority.[14] However due to other issues taking precedence and partisan gridlock in Congress, his administration was unable to help cybersecurity legislation pass until the end 2014. At that time, a flurry of four laws were passed addressing various aspects of cybersecurity reform: Cybersecurity Enhancement Act of 2014, Federal Exchange Data Breach Notification Act of 2015, National Cybersecurity Protection Advancement Act of 2015, and Cybersecurity Information Sharing Act (CISA) of 2015. Of note, the Cybersecurity Enhancement Act of 2014 attempts to enhance cybersecurity through a voluntary public-private partnership which provides for "research and development, workforce development and education and public awareness and preparedness" (Singh 2016). CISA attempts to further strengthen the public-private partnership through voluntary sharing of information, which can help with strengthening defensive measures (Tran 2016).

These measures are certainly a step in the right direction and may have already helped to improve businesses' cybersecurity. Yang, et al. (2020) analyzed the investment in cybersecurity of select publicly traded US firms and used a control group of firms from around the world based on the location of their headquarters. They found that CISA positively affected investment in cybersecurity (Yang, et al. 2020). However, many scholars and technologists find the laws have not gone far enough. Importantly, the sharing of information and other measures are strictly voluntary (Singh 2016; Tran 2016). Further, Hallenback (2020) argues that legislation does not address IT hygiene, which are the fundamentals of security that are often missed (Hallenback 2020). Finally, Tran (2016) argues the information sharing will do little to prevent cyberattacks as it was, in some ways, already in place (Tran 2016).

[14] In February 2009, shortly after being inaugurated, President Obama requested a review of cybersecurity. The review was completed a few months later and concluded that there were serious deficiencies in the United States' cybersecurity. In May, President Obama gave a speech declaring his administration would make cybersecurity a top priority (Bain 2009; Armerding 2017).

Overall, the history of cybersecurity legislation at the federal level reflects Moor's (1985) concept of the policy vacuum. The laws have come slowly and are still inadequate to address cybersecurity concerns. Walker and Masood (2020) even explore the question if law is an appropriate instrument to fight cybercrime? They find that, while law is "an imperfect instrument in cyberspace" it is part of "a whole-of-society approach" that is necessary to combat cybercrime (Walker and Masood 2020). In other words, federal law is necessary as part of the multi-scalar approach described by Scholte (2005). Supranational and subnational (state) level actions are also required to fill in the gaps of authority created by this dark side of globalization.

Supranational Level Legislation

Legislation at the federal level in the United States has taken some steps on cybersecurity, but is unable to address aspects of cybercrime that are transnational. Globalization, through the spread of the Internet, has erased national borders by allowing communication on a truly transplanetary level (Scholte 2005). This respatialization causes issues for national governments, especially in criminal matters that transcend traditional borders. National governments are powerless to prosecute criminals residing in other countries without the assistance of that country's government. This gap in authority has to be addressed through multi-scalar governance at the supranational level (Scholte 2005).

The previously mentioned ILOVEYOU virus attack provides a telling example. 2000 ILOVEYOU malware outbreak, which "infected about 10% of the global internet-connected computers, caused the global economy damages of up to $8 billion, with an added $15 billion estimated as the cost for removing the malware" (Ogu, et al. 2020). Yet, the legal charges against

the two young Filipino programmers responsible for these attacks were dropped because of the "the absence of effective trans-national legislation" (Ogu, et al. 2020).

To prevent this type of issue from reoccurring, Schjolberg (2008) argues for the creation of new laws on cybercrime which are clear and as specific as possible. He reviews the history of legislation in international law and argues that states cannot rely on interpretations of old laws which they try to stretch and bend to include cyber issues. These laws were not written with cyber issues in mind, so attempting to utilize them to prosecute criminals will only create further confusion. These laws also need to be as similar as possible in each state. Schjolberg explains, "Cyberspace has made a new environment for criminal offenses. Through international organizations, efforts must be taken to ensure the similarity of provisions in the individual countries" (Schjolberg 2008).

In 2001 the Budapest Convention on Cybercrime was led by the Council of Europe and the United States was welcomed as an observer. In 2006, the United States ratified the convention, which focused on establishing uniformed criminal law, similar to the suggestion from Schjolberg (2008). This allows for increased ability for member states to cooperate on cybersecurity and cybercrime investigations, enhancing policing of cybercrime (Seger 2011; Clough 2014). The "harmonization" of cybercrime law also helps to "eliminate or at least reduce the incidence of 'safe havens'" (Clough 2014). These 'safe havens' are areas or countries that a cybercrime is not criminalized, so there is no ability to prosecute perpetrators (Clough 2014). An example is the Philippines at the time of the ILOVEYOU virus attack (Ogu, et al. 2020).

Additional states can also join the convention and the treaty becomes more effective and beneficial with each additional state (Seger 2011). There are now sixty-four countries from all

around the world. Further, many states that have not joined have still used the convention as a template for their own national cybercrime legislation (Hakmeh and Peters 2020).

However, there are some critics of the Budapest Convention. Seger (2011) argues that the criticism is less the substance of the treaty but the fact that their respective country did not participate in the negotiation of the Convention" (Seger 2011). Countries also criticize that the treaty was developed by a regional body, the Council of Europe, and not part of a more global discussion (Seger 2011; Hakmeh and Peters 2020). Russia in particular is very critical of the convention, which they see as a challenge to state sovereignty (Clough 2013; Hakmeh and Peters 2020). In fact, at the United Nations in December 2019 Russia proposed the establishment of a committee to examine the creation of a new treaty on cybercrime to replace the Budapest Convention (Hakmeh and Peters 2020).

In addition to critics, the Budapest Convention also has some limitations. Importantly, the Budapest Convention establishes criminal law on cybercrime, but it does not address cybersecurity, which is more focused on "critical information infrastructure and national security" making it difficult for states to come to an agreement (Seger 2011). Ogu, et al. (2020) argue that the digital divide[15] and sovereign political interests are preventing the world from moving towards such a legislative framework. In the short term, states with similar attributes, such as falling on the same side of the digital divide and from similar regions, can begin to establish supra-state legislative frameworks as a first move towards a global consensus (Ogu, et al. 2020). Ilves, et al. (2016) similarly find that the cybersecurity uniformity has suffered due to differing opinions on cybersecurity amongst the member states of the European Union. For example,

[15] Ogu, et al (2020) explains that the term "digital divide" refers to dichotomy the areas of the world that have access to advanced digital technologies, such as computers and the Internet, and those areas that do not have these technologies. This concept is now being extended to include the "cross-border limitations on data flows by dominating countries of the world due to sovereign economic and trade interest […]" (Ogu, et al. 2020).

> Some governments, including Germany and the Netherlands, treat cybersecurity as a question of homeland security, while others, such as Latvia and Denmark, consider it a question of defense. Still other countries, including Finland and Italy, see cybersecurity as a matter of commerce and communications. (Ilves, et al. 2016)

In other words, they find that an issue to a European consensus on cybersecurity is member state concerns over sovereignty.

The United States is party to the only convention on cybercrime at the supranational level. This treaty certainly benefits the United States and its ability to prosecute cybercriminals. However, the convention could be improved and adopted more widely to reduce 'safe havens' (Clough 2014). Further, the convention does not address cybersecurity, as that is a more sensitive subject that may be better dealt with at the national or subnational levels (Seger 2011). The next section reviews how this gap in governance has been addressed at the subnational level.

State Level Legislation

Cybersecurity legislation at the subnational or state level is as complex as or more than at the federal or supranational levels. It would be easy to assume that cybersecurity at the state and local level is simpler because these entities are smaller than national governments or supranational organizations, but this assumption would be a mistake. State and local governments have a wide range of entities that fall within their mandate to secure both physically and in cyberspace. Flynn (2016) explains, "State and local governments have the responsibility to protect dams, freeway systems, power and water plants, emergency communications, personal identifiable information, health care records, educational institutions, and banking systems" (Flynn 2016). These systems and entities are difficult to address at the national or supranational level, so it is left to state and local governments to help fill in the gaps in governance on cybersecurity.

Even with these complexities, states have been capable of enacting legislation more quickly than at the federal level. For example, California was ahead of the curve on requiring companies to disclose security breaches that affected personal information of Californians. In 2003, which is before the large wave of major security breaches starting in 2004, California passed the Notice of Security Breach Act to address these concerns and "punish firms for cyber security failures" (Singh 2016).

Further, Alexander, et al. (2020) found that cybersecurity legislation at the state level has been increasing overtime. They examined cybersecurity legislation over an eight year period from 2011-2018 and found 454 policies were proposed from all fifty states and Washington D.C (Alexander, et al. 2020). Of these 138 policies were enacted, while the remaining policies were either still being deliberated on or were not enacted due to failure to pass the legislature or being vetoed by the governor. The most active period was 2016-2018 in which some states, such as Maryland, proposed as many as 15 bills in one year. However, other states, such as Nebraska and North Carolina, had only one bill proposed in the entire 8 year period (Alexander, et al. 2020). More recently, states have overall remained relatively active. From 2015-2019 an average of 21 states a year enacted cybersecurity related legislation while considering over 900 potential cybersecurity related bills (NCSL 2020).

Given the wide range of state and local government's responsibilities, the bills proposed from 2015-2019 covered a variety of cybersecurity related topics. Some legislation focused on training and preparedness through "improving government security practices," "creation of commissions, task forces, and studies," requirements for security audits, and "promoting of cybersecurity training and education" (NCSL 2020). Similarly, Alexander, et al. (2020) reviewed twenty categories of cybersecurity legislation and found states most often proposed legislation

related to “Legal/Insurance,” “Personal Identifiable Information,” and “Education” (Alexander, et al. 2020). They found states appear to fill in the gaps left by federal legislation, which focuses more on “Defense, Cyber Pre-through-Post Incident, and in Cyber Sharing between organizations” (Alexander, et al. 2020).

Despite the attention many states have devoted to cybersecurity legislation recently, the consensus of the literature is that states are underprepared for cybersecurity issues (Norris, et al. 2015; Spidalieri 2015; Flynn 2016; Robinson and Subramanian 2016; Karakoç 2017; Rosner 2017). Spidalieri (2015) put it bluntly, “No state is cyber ready” (Spidalieri 2015). State and local governments face numerous challenges towards addressing cybersecurity, including “Lack of sufficient funding,” “Inadequate availability of cybersecurity professionals,” “Lack of documented processes,” “Increasing sophistication of threats,” “Lack of visibility and influence with the enterprise” (Robinson and Subramanian 2016). While all these issues present challenges, a 2016 survey of state officials found that 80% cite a lack of funding as a major barrier to addressing cybersecurity. In fact, the survey found that in most cases cybersecurity allocation made up 2% or less of a state’s overall IT budget (Robinson and Subramanian 2016). With budgets this low, it becomes difficult to obtain, deploy, and maintain appropriate cybersecurity systems, as well as, employ adequate cybersecurity professionals (Karakoç 2017). Lack of funding also undermines cybersecurity programs, such as training, as these programs are not effective if no one is there to enforce them, which takes funding (Norris, et al. 2015). In other words, the lack of funding undermines the policies and work that states have done. This lack of serious attention and devotion of resources could be attributed in part to Moor’s (1985) policy vacuum, but no matter the reason there is clearly a need for additional work on cybersecurity legislation at the state and local level.

Effectiveness of Cybersecurity Legislation

The review of the history of cybercrime and cybersecurity legislation in the United States provides the background needed to review the literature on the effectiveness of cybersecurity legislation. With the scene set, I first review Moor's (1985) policy vacuum to explain how this knowledge gap has similarly affected academic work on cybersecurity legislation. The next section reviews the relevant literature, including the debate between a centralized versus decentralized authority, which is one of the major debates in the literature. Then, I review the current methods used to evaluate the effectiveness of cybersecurity legislation. Finally, the last section explains how this dissertation fits in and adds to this body of knowledge.

Knowledge Gap

As previously discussed, Moor (1985) explains that new technology (e.g., computers) creates a policy vacuum by raising practical and ethical question about its use that cannot be answered until it is clear *how* it is being used, as the potential applications of a technology are often unknown at its inception (Moor 1985). This policy vacuum certainly is clear from the review of the history of cybersecurity legislation, but this effect can also be found in academic studies. Pylant (2020) explains the literature is still "immature" compared to other fields and much of the current knowledge has been collected by journalists reporting mostly on cybersecurity failures (Pylant 2020).

As discussed above, this gap can be caused by lack of experience or lack of interest prevalent throughout society. An additional factor, especially for scholarly work, is the lack of information on a subject. Initially, knowledge of cybersecurity is limited to those on the ground level actually involved in creating and maintaining cyberspace. Like an explorer on some distant

frontier, the cybersecurity pioneers are on the front lines making new discoveries, but their focus is primarily on their mission, which in this case are the technical aspects of cybersecurity. We can see these types of reports coming from cybersecurity companies, such as Symantec,[16] who are on the frontlines. These reports help to supplement journalist's stories, but they are still limited in the information provided due to their focus. Further, the reports are not typically peer reviewed and the data behind the reports is not typically shared because it is proprietary and, in some cases, may contain personally identifiable data. Thus, these cybersecurity explorers help to close the knowledge gap but are unable to bridge it.

This lack of information is exacerbated due to incentives for victims to keep cybersecurity failures quiet. Both commercial victims and insurance companies have incentives to not report cybersecurity attacks, such as ransomware payouts, as they want to avoid scrutiny and protect their reputations (Dudley 2019). These motivations are certainly rational, but without adequate data scholars are limited in the approaches, such as quantitative analysis, they can use to study this subject, which holds back the field widening the knowledge gap.

Literature Review

The knowledge gap, especially due to the lack of available data, has resulted in most of the literature being comprised of qualitative analyses. These studies often approach cybersecurity legislation with a historical review of legislation in the country, supranational organization, or state they were assessing.[17] Within this approach, some authors chose to perform a comparative

[16] See: Savage, Kevin, et al. "The Evolution of Ransomware." *Symantec*, 6 Aug. 2015, pp. 1–56.
[17] See examples of this approach: United States, Congress (2013), Ilves (2016), Kelly (2012), Newmeyer (2012), Nwankwo and Ukaoha (2019), Schjolberg (2008), and Sutherland (2017).

historical review in which they assessed two or more entities' cybersecurity legislation.[18] This approach has an advantage of demonstrating the differences of cybersecurity legislation throughout the world and the authors also often analyze the pros and cons of each entity's legislation. For example, Nir Kshetri (2019) analyzes the cybersecurity legislation in Africa.

Other scholars have taken more unique approaches to examine cybersecurity legislation. Trautman (2015) approaches cybersecurity policy in the United States through the lens of epidemiology. In addition to providing a thorough review of US cybersecurity legislation, he compares the cybersecurity dilemma to the Ebola crisis. He argues, "***Cybersecurity*** vulnerability has the potential to be the "ultimate weapon" used against the ***United States***" (Trautman 2015). Conversely, Brito and Watkins (2011) argue against framing the cybersecurity issue in dire terms. They caution against over-inflating the issue as it presents dangers akin to the pre-war inflation of weapons of mass destruction in Iraq. They believe it could lead to the creation of a "cyber-industrial complex" similar to the military-industrial complex, which has great sway over policy that often benefits security companies. Their main concern is to make sure cybersecurity policy is based on facts, not over-inflation or economic self-interest (Brito and Watkins 2011).

Moore (2010) examines cybersecurity legislation from an economics perspective, which focuses more on the cost benefit analysis of actors. Importantly, the costs of failed cybersecurity often do not fully fall on the organization that failed. Instead, these costs are spread out amongst other actors, but primarily society as a whole. He argues to solve this issue of misaligned incentives, legislation, such as *ex post* liability, should be passed which "allocate responsibilities

[18] See examples of this approach: Blomquist (2020) explores legislation across the 50 states in the United States; Kshetri (2019) analyzes countries in Africa; Flowers, et al. (2013) focuses on the United States but briefly touches on a variety of countries throughout the world; Shackelford and Kastelic (2014) examine the United States and G20 countries; and Schackelford and Bohm (2016) compares and contrasts United States and Canada.

and liabilities so that the parties in a position to fix problems have an incentive to do so" (Moore 2010). This analysis provides an alternative look at potential cybersecurity legislation.

Also utilizing an economic perspective, Yang, et al. (2020) focus on the exploring the effects of the Cybersecurity Information Sharing Act of 2015 (CISA) on "firms' attitudinal changes toward investing in cybersecurity" (Yang, et al. 2020). They perform a quantitative assessment of this recent cybersecurity legislation. They analyzed the investment in cybersecurity of select publicly traded US firms and used a control group of firms from around the world based on the location of their headquarters. They found that CISA positively affected investment in cybersecurity (Yang, et al. 2020).

Amongst these various approaches, some of the literature has debated over the centralized or decentralized cybersecurity authority. At a national level, Kelly (2012), who believes the Department of Homeland Security should have authority, and Newmeyer (2012), who believes that a new cabinet position should be established to have authority, agree that authority on cybersecurity needs to be centralized. Kelly (2012) explains the decentralized framework, which was being proposed by the opposition, relies more on private entities to enhance cybersecurity, which is less effective at organizing and leading the country's cybersecurity. On the other hand, Rosner (2017) suggests a bottom up approach could focus on strengthening state and local governments so that they can handle cybersecurity issues.

Blomquist (2020) examines the pros and cons of centralized and decentralized frameworks at the state and local level. Blomquist (2020) finds that centralization allows for consistent application of security controls (Center for Digital Government 2018), reduced cost and complexity (Check Point 2020), and greater flexibility to expand networks and adopt new technologies (Palo Alto Network 2017). One way to accomplish this is through virtualization

(Rasmussen 2002), which allows enhanced controls of cybersecurity (Sullivan 2018), reduces the number of physical servers increasing efficiency (Rouse 2019), and allows for issues on the network to be more easily identified and remediated (Pal 2015). On the other hand, decentralization of cybersecurity allows entities to reduce vulnerability from a single point of failure (SPOF) by creating redundancy (Rouse 2009), which can prevent an issue from affecting the entire system (Blomquist 2020). The decentralization and elimination of SPOF can be achieved by blockchain technology, which replicates data creating redundancy (Farmer 2017). Blomquist (2020) argues that states and local authority should adopt a hybrid approach, which both incorporates virtualization to centralize the security controls and blockchain technology to decentralize the points of failure and create redundancy (Blomquist 2020). In fact, many states have begun to explore both options in recent years (NCSL 2020).

Pylant (2020) takes a more systematic approach to evaluating the centralized versus decentralized versus hybrid debate. She uses data from the Nationwide Cybersecurity Review and the National Institute of Standards and Technology's five key functions, "identify, protect, detect, respond, and recover," to evaluate the effectiveness of each form of governance at the state level (Pylant 2020). Through quantitative analysis she finds that states with centralized authority are more effective at the five cybersecurity functions, while states with decentralized authority performed the worst. The hybrid approach appeared to be close to a centralized approach and she suggests it as an alternative to full centralization (Pylant 2020).

In addition to Pylant's (2020) approach, other studies have sought to not only recommend potential policy prescriptions, but also evaluate the effectiveness of cybersecurity legislation. One of the most used standards is the Cyber Readiness Index (CRI) (Hathaway 2013). The index measures countries' cybersecurity readiness on five criteria:

- Articulation and publication of a National Cyber Security Strategy
- Does the country have an operational Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT)?
- Has the country demonstrated commitment to protect against cyber crime?
- Does the country have an information sharing mechanism?
- Is the country investing in cyber security basic and applied research and funding cyber security initiatives broadly? (Hathaway 2013)

These criteria were updated in the CRI 2.0 in 2015 to seven detailed categories: "1. National strategy; 2. Incident response; 3. E-crime and law enforcement; 4. Information sharing; 5. Investment in research and development (R&D); 6. Diplomacy and trade; and 7. Defense and crisis response" (Hathaway, et al. 2015). In either case, the criteria helps to identify the areas where a country could improve their cybersecurity policy.

At least two other studies have utilized the CRI framework developed Hathaway (2013) or Hathaway, et al. (2015) to evaluate cybersecurity legislation. Spidalieri (2015) adapted the CRI to assess the cybersecurity legislation of California, Maryland, Michigan, New Jersey, New York, Texas, Virginia, and Washington state. Utilizing this framework, she provides a comprehensive review of these states' cybersecurity legislation and finds that Washington and Michigan have addressed the most cybersecurity criteria, making them the most cyber ready (Spidalieri 2015). Similarly, Rosner (2017) uses an adapted version of the CRI to assess state and local governments to see how they should be included in the cybersecurity defense of the country (Rosner 2017).

These different versions of the CRI are certainly helpful qualitative tools for the evaluation of cybersecurity legislation. However, these tools cannot fully assess the effectiveness of cybersecurity legislation against actual cyberattacks without data on attacks. Thus, while the tool is certainly useful, the applications found in this review of the literature have been limited to qualitative approaches, which cannot statistically assess the effectiveness of the cybersecurity legislation. Additionally, while Pylant (2020) utilizes quantitative analysis, she still fails to assess

the effectiveness against actual cybersecurity attacks. This lack of testing is almost certainly due to the aforementioned difficulty of obtaining data regarding cybersecurity attacks.

Conclusion

Based on the studies reviewed there is a major gap in the literature as there are only a few quantitative analyses on cybersecurity legislation. Almost all the work on the subject has been qualitative, which can suffer from selection bias due to a focus typically on successful attacks. The lack of quantitative analysis most likely stems from the lack of data, which, as noted previously, is due to the incentive for victims not to report attacks to avoid potential reputation costs (Liska 2019). Fortunately, this dissertation is able to help fill this gap with a novel dataset that includes data on cyberattacks. This data will be used in a quantitative analysis to assess the effectiveness of cybersecurity legislation against preventing cyberattacks. Different types of legislation may be more or less effective and the analysis in this dissertation helps to discern amongst the many policy prescriptions that states have enacted. Further, the use of quantitative analysis helps correct the selection bias of qualitative studies by taking into account both the successful, reported attacks and the unsuccessful, unreported incidents.

To study the quantitative analysis of legislation on ransomware attacks, this dissertation will focus on state level legislation. The state level is the focus because it is the most appropriate level for actually preventing ransomware attacks for two reasons. First, action is needed now and the higher up the hierarchy of governance the more difficult it is to move quickly. As noted above, there has not been any truly global convention on cybersecurity at the supranational level. The most successful has been the Budapest Convention lead by the European Union in 2001, but there have been many other regional efforts. Similarly, at the national level the United States has been

slow to adopt new policies with decades in between the major legislation. On the other hand, from 2015-2019 states enacted 233 cybersecurity laws (NCSL 2020). Second, as Scholte (2005) and Rosenau (2003) suggest, the governance issues caused by respatialization require a multi-scalar approach of governance. In the case of cybersecurity, the focus of governance at the supranational and national levels are on broader issues. Supranational legislation is focused on sharing information amongst nations and ensuring cybercrimes are criminalized similarly in all countries so that perpetrators can be prosecuted if caught. Similarly, at the national level the focus has been on criminalization, information sharing between public and private sectors, and data protection more broadly. However, the state level can fill in the governance gaps caused by respatialization. State governments can enact laws specific to the issues their constituents face, which can help combat cybersecurity threats, such as ransomware.

The next chapter will explore ransomware in more detail to reveal the strategies used in this cybercrime. By understanding ransomware's strategies, it will become clearer how different policies may affect ransomware attacks. Training will be shown to be an effective counterstrategy to ransomware.

CHAPTER III

UNDERSTANDING RANSOMWARE AND AN EFFECTIVE COUNTERSTRATEGY

Cybersecurity legislation is critical to defend against cybercrime in general, but the focus of this dissertation is on ransomware. To determine the best counterstrategy against ransomware, we first need to better understand what ransomware is and how it works. This chapter starts by defining ransomware. Then the history of ransomware is discussed to give a background for understanding the strategies used by cybercriminals in ransomware. These underlying strategies of ransomware are then discussed in more detail. The final section builds on these lessons to make clear that a combination of training, up to date anti-virus programs, and good cyber hygiene are the most effective counterstrategies for preventing ransomware.

Definition of Ransomware

Ransomware is a type of malicious software or malware which, after infecting a computer, tries to extort the victim (Hernandez-Castro, et al. 2020). Some forms of ransomware add files to a computer, which could be incriminating. Then the attacker threatens to reveal the illicit materials to the authorities unless a ransom is paid (Hernandez-Castro, et al. 2020). However, the focus of this dissertation is on ransomware that encrypts a victim's data and demands a ransom payment within a limited time window in exchange for a decryption key. If the victim refuses to pay, they risk losing their data forever (Kaspersky 2020). This type of attack was "originally called cryptovirus but later also referred to as crypto-ransomware or simply ransomware" (Hernandez-Castro, et al. 2020).

History of Ransomware 1989-2010

Surprisingly, the first attempted ransomware attack occurred before the spread of the Internet. In 1989, the AIDs Trojan, also known as PC Cyborg Trojan, was spread to victims from infected floppy discs (Trautman and Ormerod 2018). The floppy discs were handed out at a World Health Organization's International Aids conference and were thought to contain information about the AIDs health crisis (Richardson and North 2017). The scam was enacted by Joseph Popp, an evolutionary biologist, who distributed "20,000 copies of [the floppy disc] to researchers in 90 countries" (Waddell 2016). Once installed on a computer, the malware then laid dormant for 90 computer reboots and then encrypted file names (Waddell 2016). An error message was then displayed disguising the ransom demand as a software renewal which demanded $189 for renewal or $378 for lifetime renewal. However, the encryption was rudimentary and only encrypted the file names, not the actual files. So many security experts were able to fix the issue without paying the ransom. Further, the ransom was rather arduous to pay, as the demand required victims to send a cashier's check or international money order to an address in Panama. In the end, Popp did not make much money off the attack and was eventually arrested (Waddell 2016).

During the next decade and a half, as the Internet was established, ransomware attacks were insignificant (Nadir and Bakhshi 2018).[19] However, during this time the theoretical underpinnings of cryptoviral ransomware attacks was established. Traditionally, cryptography has been seen as a defensive tactic, but Adam Young and Moti Yung (1996) theorized that cryptography could be used offensively with malware to infect a computer, encrypt it, and force

[19] Nadir and Bakhshi (2018) explain that during this time period ransomware in the form of "fake tools," such as spyware or performance enhancement, were used. These attacks, similar to Popp's attack, made the victim believe they were in need of additional software to prevent or fix problems with the computer, but in actuality there was no issue. These attacks generally requested the victim pay between $30 and $90. Once paid, nothing happened as there was no issue to begin with (Nadir and Bakhshi 2018).

the victim to pay a ransom (Young and Yung 1996). They advised they came up with the idea based off Plopp's failed floppy disc attempt and thinking about the 'facehugger' creature from the movie *Alien*. Like the creature, ransomware forms "a forced symbiotic relationship between a computer virus and its host where removing the virus is more damaging than leaving it in place (Young and Yung 2017). Young and Yung (1996) were able to accomplish creating a "forced symbiotic relationship" by making the victim dependent on the attack in order to be able to regain access to their encrypted data.[20]

The first modern ransomware, which used encryption similar to the theoretical models developed by Young and Yung (1996), began to emerge in 2005 (Hampton and Baig 2015). For the next six years, ransomware criminals began developing different strains of ransomware to try to stay one step ahead of security experts. In 2005 and 2006, some early forms of cryptoviral ransomware, such as Trojan.Gpcoder, Trojan.Cryzip, and Trojan.Archiveus, were created and were often spread using spam emails (Richardson and North 2017). In 2008, locker ransomware, which locked victims out of their computer, began to appear alongside more sophisticated fake antivirus programs, which made victims believe they were obtaining a legitimate security software (Savage, et al. 2015).

These early attacks suffered from suboptimal payment methods. The Trojan.Archiveus ransomware strain "asked the victim to buy medication over the internet using certain online

[20] The dependence is created because of the way the cryptovirus is created. Young and Yung (2017) explain:

> In cryptoviral extortion, the attacker generates a key pair for a public key cryptosystem and places the "public encryption key" in the cryptovirus. The corresponding "private decryption key" is kept private. The crypto-virus spreads and infects many host systems. It attacks the host system by hybrid encrypting the victim's files: encrypting the files with a locally generated random symmetric key and encrypting that key with the public key. It zeroizes the symmetric key and plain-text and then puts up a ransom note containing the asymmetric ciphertext and a means to contact the attacker. The victim sends the payment and the asymmetric ciphertext to the attacker. The attacker receives the payment, decrypts the asymmetric ciphertext with his private key, and sends the recovered symmetric key to the victim. The victim deciphers his files with the symmetric key. (Young and Yung 2017)

pharmacy URLs. The victim then needed to submit the order ID to get the password to decrypt the archive files" (Savage, et al. 2015). While the locker ransomware strain, Trojan.Randsom.C, locked the victim's computer and required the victim to call a premium-rate phone number. Other forms of payment included premium rate SMS message (Scott-Cowley 2017) and Ukash or a Paysafecard, which is a pre-paid voucher (Keizer 2011). While better than Popp's mail in payment method, these early ransomware strains' payment methods still limited the expected payment per attack to a few hundred dollars or less (Keizer 2011; Savage, et al. 2015; Scott-Cowley 2017).

Further, these early attacks generally contained numerous flaws and poor encryption techniques. Hampton and Baig (2015) explain, "Many variants of GPCode contained flaws including poorly implemented encryption routines, insecure encryption keys, or poor file deletion strategies, which allowed recovery of deleted content […] (Hampton and Baig 2015). Decryption keys or passwords were often left in the code of the malware, which could be accessed by a tech savvy victim to unlock their system (Nadir and Bakhshi 2018). For example, the Trojan.Cryzip ransomware strain copied files into password protected folders and deleted the original files, but left the password in the coding, which could be found and used to recover the files without paying the ransom (Savage, et al. 2015).

The limited payment methods and generally deficient encryption kept these early attacks from becoming much of a widespread threat. The initial wave in 2005 concentrated in Russia and its neighbors (Hughes 2016). Soon after attacks began to spread to Europe and the United States (Zetter 2015). Certainly many victims were affected over this time period, but it pales in comparison to recent year which have seen hundreds of millions of attacks annually (Clement 2020). Further, these more recent attacks have increased from the few hundred dollar ransoms of the early attempts, to demanding ransoms in the hundreds of thousands of dollars (Karimi 2019).

How did ransomware go from largely amateurish attempts to a global threat costing billions per year?

Hampton and Baig (2015) argue that there are three core technologies which were needed to allow ransomware to become a global menace:

- Requirement for strong, reversible encryption to lock up a user's files,
- Dependence on a system for anonymously communicate keys and decryption tools, and
- Concealment i.e., setup of an untraceable way to pay the ransom (Hampton and Baig 2015)

In other words, the ransomware developers needed the ability to encrypt at a level consistent with the cryptovirus described by Young and Yung (1996). They also needed to have a communication system that allowed them to remain anonymous but communicate directly with the victims. Finally, they needed a payment method that was not only untraceable but also scalable so that larger amounts could be demanded.

In addition to Hampton and Baig's (2015) assessment on necessary technology, there are two other shifts which occurred that allowed ransomware attacks to escalate so quickly. First, the development of the illicit ransomware as a service (RaaS) economy has allowed high-tech ransomware strains to be easily deployed by novice cybercriminals for a small cost. RaaS is a term used to describe the illicit economic activity between ransomware creators and purchasers. The creators sell their ransomware to buyers for a fee and then often take a portion of the ransoms acquired, as well. Meland, et al. (2020) explain that "RaaS can have different formats, such as source code that the buyer compiles himself, pre-compiled binaries or an interface where the buyer inputs information about the victims. This collaborative strategy is a way of achieving a faster rate of infections with a lower risk of getting caught" (Meland, et al. 2020). This has vastly increased the number of attacks as entry barriers to get into ransomware have become so low.

Second, the adaptation of ransomware attacks to target specific victims or types of victims, such as hospitals, has vastly increased the cost per attack. The criminals are focusing on these types of actors because these actors feel increased pressure to pay the ransom as often they need their computer systems as a matter of life or death (Spence, et al. 2018). The cost and the likelihood of receiving a ransom payment can be higher when victims have a greater immediate need for their data.

History of Ransomware 2011-2020

The first two steps necessary for this revolution in ransomware began to take shape in 2011 and 2012. The first major ransomware outbreak occurred in 2011 with about 120,000 new ransomware detections in the first three quarters of the year (KnowBe4 2020). KnowBe4, a cybersecurity company, attribute this increase in ransomware to the availability of "anonymous payment services, which made it much easier for authors to collect money from their victims" (KnowBe4 2020). In other words, a new technology had emerged that allowed payments that were untraceable, which made ransomware criminals more willing to engage in widespread ransomware attacks without fear of being discovered by the authorities. This new technology was cryptocurrency, especially Bitcoin which was launched in 2009.

With a new method of anonymous payment, ransomware developers then took another step towards making ransomware into a global threat. In 2012 an early version of ransomware as a service took off with the development of two toolkits that were sold on the black market to allow even amateurs to create and distribute ransomware (Richardson and North 2017). For example, one kit was Citadel, which allowed purchasers to both "distribute malware and manage infected computers (bots)" for a cost of around $3,000.00-$4,000.00 (Segura 2016). The Citadel platform

even allowed novice users to perform advanced cybercriminal techniques, such as WebInject,[21] with relative ease (Segura 2016).

While these two advances helped to increase the overall number of ransomware attacks, the scope was still limited as the encryption capabilities were still not available. So, attacks in 2012 focused on locker ransomware (Savage, et al. 2015; KnowBe4 2020). In particular, a strain of ransomware called Reveton became popular. This strain of ransomware infects a computer, locks it, and then "[a] bogus message from the FBI pops up on the screen saying the user violated federal law. To unlock their computer, the user must pay a fine" (Halpern 2012). These messages typically claimed that the victim was in trouble for pirating music or movies, or for downloading illicit material such as child pornography. This form of 'scareware' was intended to scare the victim into paying the ransom (Savage, et al. 2015). The authors of Reveton even had the forethought to have the ransom message appear to come from different law enforcement agencies based on the region in which the victim was located (Hughes 2016; KnowBe4 2020).[22] The message was convincing enough that some victims even turned themselves into the police (Fitz-Gerald 2013).[23]

In 2013 a ransomware developer finally achieved the level and method of encryption described by Young and Yung (1996). The result was the infamous CryptoLocker ransomware, which "used military grade encryption of RSA-2048 bits to encrypt files" (Nadir and Bakhshi 2018). The author of the malware was also the first to store the decryption key on a remote server,

---

[21] The WebInject or man-in-the-middle attack is a method of obtaining identity or financial information (Segura 2016). It works by creating a popup on a legitimate website that asks for relevant personal information which appear to come from the legitimate website. WebInject "is a very powerful technique that can be used to deceive the user, as he will believe that the content he is seeing has been received directly through his bank's website" (Boutin 2014).

[22] Hughes (2016) explains, "The makers of Reveton covered all their bases. It was localized for virtually every European country, as well as Australia, Canada, New Zealand, and the United States."

[23] In July 2013, a man in Virginia turned himself into the police after his computer was locked by Reveton ransomware. He believed the message came from the FBI as it stated he had been caught with child pornography on his computer. He did not realize the message was fake and turned himself in to face charges as he did have child pornography. He brought his computer in to the local police, who arrested him after finding the pornography on his device (Fitz-Gerald 2013).

matching the Young and Yung (1996) theory on how a cryptovirus would function and making it close to impossible to reverse the encryption without paying the ransom (Nadir and Bakhshi 2018).

CryptoLocker was released around September 2013. It primarily spread through phishing spam emails containing an attachment that held the malicious programing (Alintanahin 2013). Three months later, in December 2013 this ransomware had already infected a reported 250,000 machines and made an estimated $27 million in Bitcoins (KnowBe4 2020). However, the lifespan of the ransomware was short lived. In June 2014 a "coalition of academics, security vendors, and law enforcement agencies" took down the botnet servers that distributed CryptoLocker and two vendors released a database "which allowed victims [of the ransomware] to decrypt their files free (Hughes 2016).

While CryptoLocker had a quick demise it was a clear proof of concept of Young and Yung's (1996) theory. It made clear that cryptoviral attacks could be highly lucrative, which spurred copycats and an explosion of new strains of ransomware to be developed in the following years. In fact there have been at least 72 ransomware strains developed since CryptoLocker was released. This explosion was aided by the development of true ransomware-as-a-service in 2015, where complete novices can go to a "TOR website "for criminals by criminals," roll your own ransomware for free, and the site takes a 20% kickback of every Bitcoin ransom payment" (KnowBe4 2020). This service increased the amount of ransomware strains as individuals could access the site and modify existing strains to make new virulent forms with essentially zero entry cost. While it is not the focus of this project to examine each one individually, it is worth noting many of the strains here in Table 3.1 to show the extent of the increase in ransomware post-CryptoLocker. These various strains are often related, building off one another to help stay one step ahead of the security experts.

Table 3.1 Ransomware Strains Released by Year

Year	Ransomware Strains
2014	CryptoDefense, CryptoWall, Koler.a, Cryptoblocker, SynoLocker, and TorrentLocker
2015	TeslaCrypt V2.0, LockerPin, LowLevel04, and CryptoWall V2.0, V3.0, and V4.0
2016	7ev3n, Locky, Petya, Mishca, The Ransomware That Knows Where You Live, CrptoHost, CryptXXX, DMA Locker V4.0, BART (duh!), Satana, Ranscam, Cry, Mamba, Fantom, CryPy, Ransoc, Karma, Osiris, and Goldeneye
2017	Spora, DynA-Crypt, PetWrap, Samas, WannaCry, NotPetya, Erebus, Diablo6, SyncCrypt, Defray, nRansomware, Bad Rabbit, Ordinypt, and Scarab
2018	Kirk, Annabelle, GandCrab, Zenis, SamSam, AVCrypt, Blackheart, BitKangoroo, Satan, CommonRansom, Dharma, and Ryuk
2019	CyptoMix, Anatova, LockerGoga, Matrix V2.0, vxCrypter, MegaCortex, eCh0raix, Android/Filecoder.C, GermanWiper, Lilocked, Nemty, PureLocker, Maze, Snatch, and REvil

Data Source: KnowBe4. "Ransomware." *KnowBe4*, 2020, www.knowbe4.com/ransomware#ransomwaretimeline.

To understand more about the changes made to ransomware over this time period, it is instructive to review a few of the more notorious ransomware strains. In 2014 CTB-Locker or Curve- TOR-Bitcoin was released (Salvi and Kerkar 2016). Hampton and Baig (2015) argue that CTB-Locker is the first ransomware to successfully combine the previously discussed attributes needed to become a successful ransomware strain. They explain that CTB-Locker had "fast secure encryption," anonymous communication through TOR (The Onion Routing protocol), and "secure, untraceable" payment through Bitcoin (Hampton and Baig 2015). Many other strains have since incorporated these attributes, as well as, developed additional tactics to increase the breadth or the depth of their attacks.

While there have been many devastating ransomware strains, 2017 saw two of the worst. First the WannaCry ransomware strain struck in May and quickly spread worldwide. India was one of the worst affected countries, but the ransomware also affected "FedEx, Nissan, railway companies in Germany, Russian Railways, Interior ministry, telecommunication company like [MegaFon in Russia and] Telefonica in Spain" (Mohurle and Patil 2017). The attack quickly "infected over 300,000 computers in over 150 countries" (KnowBe4 2020). The reason the attack was able to spread so quickly was due to an innovation making the ransomware strain behave more like a worm[24] allowing it to "propagate and attack various target networks in a short space of time without any human intervention" (Zimba and Chishimba 2019). The attack is believed to have come from North Korea using an exploit stolen from the NSA (Trautman and Ormerod 2018).

The second attack struck less than a month later from the NotPetya ransomware strain. This attack utilized the same exploit as the WannaCry ransomware (Palmer 2019). It is believed to have been developed by Russia to attack Ukraine, but the ransomware quickly spread beyond Ukraine around the globe (Trautman and Ormerod 2018; Palmer 2019). One unintended victim was the global shipping company Maersk, which had "almost 50,000 infected endpoints and thousands of applications and servers across 600 sites in 130 countries" (Palmer 2019). There were two innovations that made the NotPetya attack such a devastating and widespread attack. First, this ransomware strain had no intentions of returning the victim's data as the program was designed to encrypt the victim's files and then essentially throw away the key (KnowBe4 2020). This meant that even if the ransom was paid, there was no chance at recovering the files, which would need to be either recovered from a backup or rebuilt. Second, NotPetya included a secondary mechanism

[24] A computer worm is another form of malware, which can modify and delete files, make copies of itself to be spread over a network, "steal data, install a backdoor, and allow a hacker to gain control over a computer and its systems settings" (NortonLifeLock 2020). In this case, the WannaCry ransomware utilized the techniques worms use to copy themselves and spread in order to infect additional computers quickly (Zimba and Chishimba 2019).

called Mimikatz, which was able to obtain "a Windows user's password out of a computer's RAM" Trautman and Ormerod 2018). This allowed the malware to infect vulnerable machines that had not been correctly patched to fix the previously mentioned exploit and then using Mimikatz the ransomware was able to obtain the administrator credentials to infect the entire network, including computers that had been patched (Trautman and Ormerod 2018). This secondary mechanism greatly increased the breadth of the attack, allowing the ransomware to spread like wildfire around the globe.

More recent ransomware strains have developed further innovations. MegaCortex was developed specifically for targeting corporate networks (KnowBe4 2020. It is designed to automatically infect the network and spread throughout, increasing the depth of the attack and potentially the likelihood the ransom will be paid (Osborne 2019). Ryuk ransomware developers added an innovation to increase the depth of their attacks. "In Q4 Ryuk[, a strain of ransomware,] actors began using a "Wake-on-Lan" feature to turn on devices within a compromised network that were initially powered off" (Siegel 2020). In other words, once infected with ransomware the program forces systems that are off to be powered back on and become infected, increasing the depth of the attack. Finally, Maze ransomware has developed into "leakware" which not only encrypts the victim's data but steals it as well (KnowBe4 2020). Marsh (2020) explains "With this data in hand, hackers then dictate a specific date to pay by before they publish stolen records on the open internet, strong-arming companies to pay the ransom" (Marsh 2020). This innovation makes it much more likely a victim will pay the ransom as even if they have a backup that they could recover the encrypted data with, the victim likely does not want the data released. Even if the ransom is paid, there is some worry that the criminals could potentially still sell the stolen data to the highest bidder (KnowBe4 2020).

The development of new technologies, as well as the innovations of ransomware developers clearly allowed for an explosion in ransomware strains, attacks, and damages. For technology, stronger encryption capabilities allowed ransomware brought Young and Yung's (1996) theory into reality and forced more victims into paying the ransom. The development of TOR provided anonymous communication between the attacker and the victim, allowing attackers to negotiate leading to ransoms being paid more often (Nadir and Bakhshi 2018). Finally, the creation of cryptocurrencies, such as Bitcoin, provided untraceable and scalable payment options, which allowed ransomware to attack more broadly and demand more in ransoms with less fear of reprisal from law enforcement agencies.

In addition to technological advances, the ransomware developers themselves made advances which added to the rapid growth of ransomware attacks. Importantly, the creation of ransomware as a service has made entry costs for would be criminals essentially zero by providing them with the sophisticated ransomware programs for use (Meland, et al. 2020). This service has vastly increased the number of criminals using ransomware and the number of attacks. Other innovations have increased the both the breadth (Trautman and Ormerod 2018) and the depth (Marsh 2020) of ransomware attacks, making them affect more victims and encrypt data in a way that prevents recovery, such as deleting backups (Zimba and Chishimba 2019) or stealing the data (Marsh 2020). With more victims there is an increased likelihood some will pay and with more serious attacks there is an increased likelihood a victim will be forced to pay the ransom.

These new technologies and innovations have allowed ransomware to expand and shift the focus of their targets. Previously, ransomware targets were mostly indiscriminate consumers using Windows operating systems. Now, ransomware can infect Windows, Mac, and mobile devices, such as Android (KnowBe4 2020). The focus for many ransomware developers has shifted to

businesses and other enterprises, which can be forced to pay higher ransoms per attack (Zimba and Chishimba 2019; KnowBe4 2020). Since enterprises can be more lucrative targets, many ransomware developers now craft custom ransomware specifically for a single entity or type of entity, such as health care facilities (Spence, et al. 2018), to increase the likelihood of a successful attack. In other words, these new technologies and innovations have changed ransomware into a sophisticated, highly targeted, cyber threat, which costs the global economy billions each year (Emsisoft 2020).

Ransomware Strategy

The history of ransomware clearly shows that the malware has evolved from "hobby hackers into a billion-dollar industry" (CR 2017). Early ransomware developers often made numerous mistakes, such as including the key in the code of the malware. However, today's developers of ransomware are now often very innovative and talented programmers, who are part of sophisticated organized crime syndicates. They have consistently shown they can stay one step ahead of cyber security experts by developing new tactics and innovations. Yet, throughout the 30 years of ransomware history there is one underlying strategy, which can be seen in both the early less sophisticated attacks and the newer, highly targeted, and technically proficient attacks.

The goal of ransomware is for as many victims as possible to pay the ransom (Hernandez-Castro, et al. 2020). To accomplish this goal, most ransomware[25] uses social engineering to both trick the victim into downloading the malware and to make victims believe they have no other option but to pay the ransom. Social engineering a manipulation technique which plays on human

[25] Some ransomware uses other methods, such as "brute force" attacks, to break into a victim's system. They may also have other goals besides collecting a ransom, such as NotPetya which Russia primarily released to cripple Ukrainian businesses. However, the overwhelming majority of ransomware does rely on social engineering as its primary strategy (KnowBe4 2020).

error and emotions to trick victims into providing "private information, access, or valuables" (Kaspersky 2020). This strategy has been key throughout the history of ransomware.

To trick victims into downloading the ransomware, the developers have often relied on phishing. The word is a play on fishing because the strategy used in the two acts is the same – bait and hook. In phishing, the bait or lure is the text and appearance of the email, which is typically modeled after a common company's legitimate email and is used to trick its victim into getting hooked by following a link or attachment that can steal personal information or download malware, such as ransomware. Another common part of the lure is to create a sense of urgency by creating a false deadline to respond, such as stating the target's account will be deactivated within 24 hours if no action is taken. These emails are usually sent out as part of a spam phishing, or mass indiscriminate attack (Kaspersky 2020). Novice attempts at phishing are typically easy to spot, as the lure is riddled with typos and grammatical errors. But cyber criminals have begun to excel at the art of subterfuge in phishing emails. Emails can be sent which appear in every way to come from legitimate organizations, such as banks, except that instead of coming from an @bank.org email address they come from @bank.com or other similar ruses.

Rob Sobers from Varonis, a cybersecurity company, provides a detailed explanation of this tactic in his article, "The Anatomy of a Phishing Email" (Sobers 2020). In an example in the article, the scammer mimics an email from a major company, such as Apple, creates a sense of urgency, and requests the target click a link or download a file, which would of course contain the ransomware program.

The deception used in phishing attacks is currently the easiest method for cyber criminals to overcome cyber defenses. In their report, "Verizon's 2016 Data Breach Investigations Report finds cybercriminals are exploiting human nature," Verizon finds that cyber criminals continue to

exploit cyber defenses through weak passwords, known exploits which have not been updated by the user, and phishing.

Considering the cyber criminals use of phishing, the most effective legislation should be training on cyber security. Cyber defenses can certainly be bolstered, but in the end without effective training cyber criminals will continue to exploit the weak link in the system, which is human error. One erroneous click by an undertrained staff member can undo seemingly impenetrable cyber defenses. "You might say our findings boil down to one common theme -- the human element," said Bryan Sartin, executive director of global security services, Verizon Enterprise Solutions. "Despite advances in information security research and cyber detection solutions and tools, we continue to see many of the same errors we've known about for more than a decade now. How do you reconcile that" (Verizon 2017)?

More recent ransomware strains, which are more targeted, use an advanced form of this technique called spear phishing or even whaling. Spear phishing attacks use personalized information to target victims, such as impersonating another employee in the office or another person from your contact list. Whaling is a targeted attack which “specifically aim at high-value targets like celebrities, upper management, and high government officials” (Kaspersky 2020).

Through these techniques, ransomware criminals are able to trick unsuspecting victims into downloading the ransomware program. At this point, the focus of the attackers is to make the victim believe, regardless of the truth, that their only option is to pay the ransom. This task again is accomplished through social engineering. Certainly having sophisticated encryption, which actually does prevent alternative recovery, can be helpful, but since the goal is to have as many victims pay the ransom as possible, the critical problem for ransomware developers to solve is

convincing the victims to pay. This problem has been most successfully resolved with social engineering.

Early ransomware attempts relied entirely on social engineering to trick the victim into paying the ransom. Kharraz, et al. (2015) found that most of the early ransomware samples they reviewed lack the technical complexity to perform successful attacks [… because they] fail to seriously take the victim's resources as hostage" (Kharraz, et al. 2015). Yet, we know from the history of ransomware that victims still paid ransoms during this period, which means that they must have paid due to the social engineering manipulation that convinced them paying was the best or only option. This social engineering can be seen as far back as Popp's original ransomware note, which tried to make the victim believe that they owed money to renew their subscription to use their computer programs (Waddell 2016). Later fake antivirus ransomware often did not even encrypt or lock any data, it relied entirely on making the victim believe that they needed to buy upgraded antivirus software (Savage, et al. 2015). Later, law enforcement scareware, most infamously done by the locker ransomware Reveton, tried to scare the victim into believing they had been caught by law enforcement and needed to pay a fine or they would face harsher punishment. These tactics were in at least one case too convincing, as the victim turned themselves in to the police (Fitz-Gerald 2013).

The more recent cryptoviral ransomware has become so powerful that the encryption of the affected data is irreversible. However, cyber security experts have fought back by increasingly trying to back files up. The two sides are locked in an arms race. Ransomware developers have been devising ways to either encrypt or delete backup files, while cyber security experts have developed new ways to securely back up files. Yet, even in situations when the data truly is irreversibly encrypted, the ransomware developers must still convince the victim to pay. This task

is increasingly difficult as the FBI, mayors, and some cyber security experts have begun campaigning to pressure victims not to pay ransoms (Nadir and Bakhshi 2018). The ransomware criminals are still able to convince victims to pay by using social engineering to tout their notoriety and provide customer service in order to make paying a ransom seem normal and acceptable.

"Ransomware is rare (maybe unique) in being a cybercrime that positively benefits from publicity and greater knowledge" (Cartwright, et al. 2019). Ransomware criminals want the victims to know of their skills and success. If it becomes common knowledge or belief that a strain of ransomware is, in fact, irreversible without paying the ransom, then this increases the likelihood that a victim will pay the ransom. Further, these criminals want victims to believe that in the end they will return the victim's data unharmed, because the ransomware attack is business, not personal. They want to become known as criminals you can trust (Michael 2016). For example, the CryptoWall ransomware strain made a reputation of releasing data promptly upon payment (Rashid 2016).

While ransomware criminals have the goal of being viewed as trustworthy, their industry suffers from a free rider problem. All ransomware strains want as many victims to pay the ransom as possible. As previously stated, building trust with the victims that their data will be recovered upon payment of the ransom is a way to increase the number of ransoms paid. However, there is a cost to unencrypt the data, such as sending the encryption key (Cartwright, et al. 2019). This cost provides an incentive to free ride on the trust built by other ransomware criminals by not helping to unencrypt the victim's data upon payment. In some cases, the ransomware attacker does not actually know how to undo the damage they have caused. This issue is especially prevalent with the increase in novice ransomware criminals. These free riders degrade the trust and decrease the

overall willingness of victims to pay a ransom, which undermines the non-free riders' business model (Cartwright, et al. 2019).

To combat the free rider problem, some ransomware criminals try to create a brand through their notoriety by providing customer service. Some ransomware strains provide professional user interfaces to make payment easy and customer service is available to assist with any questions (Michael 2016). In fact, many ransomware strains now have customer support websites (Weisbaum 2013) or even customer service departments who can help assist victims in paying the ransom (Cartwright, et al. 2019). For example, Rashid (2016) explains that "The CryptoWall gang is well known for its excellent customer service, such as giving victims deadline extensions to gather the ransom, providing information on how to obtain bitcoins (the preferred method of payment), and promptly decrypting the files upon payment" (Rashid 2016). Some ransomware customer service rivals that of legitimate businesses with support in multiple languages, a FAQs section, customer support forms to ask questions, and customer service agents to provide fast answers and assistance. They even may decrypt a file to prove they can reverse the damage and build trust with the victim (Savage, et al. 2015; Michael 2016).

Often through these customer service methods the ransomware criminals will actually negotiate the amount of the ransomware payment. "Getting less ransom is better than no ransom at all, that is generally the basic psyche behind ransomware attacks" (Nadir and Bakhshi 2018). Cyber security company, F-Secure, found that 3 out of 4 ransomware criminals that they contacted were willing to negotiate and, on average, granted a 29% discount (Michael 2016).

Ransomware has and continues to rely heavily on social engineering as a strategy to obtain their goal of obtaining as many ransom payments from victims as possible. They use social engineering to trick victims into downloading their malicious programming. From there, they

focus on pushing their victim into payment by limiting their options with cyber techniques and using social engineering to convince the victim to pay the ransom. They even provide customer service to make paying the easiest option for the victim.

Counterstrategy

Now that the history of ransomware and its strategy has been reviewed, we can examine the best ways to counter ransomware through legislation at the state level, which as explained in the previous chapter is the most appropriate level for preventing ransomware attacks. To combat ransomware many previous studies recommend individuals and enterprises employ a multifaceted approach which includes steps to prevent, mitigate, and recover from a ransomware attack (Savage, et al. 2015; Pope 2016; Salvi and Kerkar 2016; Sittig and Singh 2016; Richardson and North 2017; Nadir and Bakhshi 2018; KnowBe4 2020). Preventing an infection altogether can be accomplished through up to date antivirus software (Savage, et al. 2015; Pope 2016; Salvi and Kerkar 2016; Sittig and Singh 2016; Nadir and Bakhshi 2018; KnowBe4 2020), practicing good cyber hygiene by keeping programs patched and up to date (Savage, et al. 2015; Pope 2016; Salvi and Kerkar 2016; Sittig and Singh 2016; Richardson and North 2017; Nadir and Bakhshi 2018; Hallenback 2020; KnowBe4 2020), implementing best practice procedures (Richardson and North 2017), and training on recognizing phishing and ransomware threats (Savage, et al. 2015; Pope 2016; Sittig and Singh 2016; Richardson and North 2017; KnowBe4 2020). To mitigate a successful attack shut down and disconnect a compromised system at the first sign of infection (Salvi and Kerkar 2016; Sittig and Singh 2016; Richardson and North 2017), backups should be kept offline or otherwise unavailable to not be compromised (Pope 2016; Salvi and Kerkar 2016; Sittig and Singh 2016; Nadir and Bakhshi 2018; KnowBe4 2020), authorization should be

restricted to reduce attacks from spreading (Salvi and Kerkar 2016; Nadir and Bakhshi 2018), and have a business continuity plan (Savage, et al. 2015). Finally, to recover from a ransomware attack know what resources are available for decryption tools (Savage, et al. 2015; Nadir and Bakhshi 2018) and data recovery tools (Savage, et al. 2015; Nadir and Bakhshi 2018), have a disaster recovery plan in place (Savage, et al. 2015; Sittig and Singh 2016), and, once again, have strong backups of data to aid in quick recovery (Savage, et al. 2015; Pope 2016; Salvi and Kerkar 2016; Richardson and North 2017; Hernandez-Castro, et al. 2020; KnowBe4 2020).

The previous literature certainly outlines a comprehensive approach to combat ransomware attacks. States could potentially enact laws requiring, providing access, or providing support for many of these various cybersecurity suggestions. However, this dissertation is focused on preventing ransomware attacks from occurring, because the data on ransomware attacks, which will be discussed in more detail in a later chapter, is limited in most cases. Unfortunately, the majority of the data only includes enough information to know when and where an attack occurred. Mitigation strategies and recovery plans are unlikely to have much effect on the number of attacks. Instead, they would by more likely to affect the severity of the attack. Since the data for the most part does not have additional details that describe the severity of the attacks, we are unable to truly assess the effectiveness of these strategies in this study.

Due to these data limitations, the focus of this dissertation is on ransomware prevention. As discussed above, phishing is the main tactic used by ransomware to bypass cybersecurity measures. Therefore, anti-phishing training is an important prevention tactic as humans are consistently one of the most vulnerable aspects of cyber security (Wash and Cooper 2018; Fernando and Arachchilage 2020). The literature on preventing phishing attacks focuses on two aspects: the user and the software (Apandi, et al. 2020).

Studies on the user side of phishing prevention often focus on the effectiveness of various methods of anti-phishing training. Fernando and Arachchilage (2020) find that traditional anti-phishing programs are often outdated and unable to assist users to deal with modern phishing techniques (Fernando and Arachchilage 2019). Jensen, et al. (2017) similarly find issue with traditional rule-based training techniques. They argue in addition to the traditional approach, mindfulness techniques should be taught, which they found can increase overall awareness while evaluating emails helping to prevent them from falling victim to a phishing attack (Jensen, et al. 2017). On the other hand, Wash and Cooper (2018) find that the perceived origin of the training can have an effect on the success of the anti-phishing training program outcome. Training performed by experts was more likely to reduce likelihood of falling for phishing than if the information was provided from a peer, while stories given by peers were more effective than stories from experts (Wash and Cooper 2018).

However, Dodge, et al. (2012) finds that anti-phishing training alone is not as effective as training received after falling victim to a simulated attack. Similarly, Kumaraguru, et al. (2008) found embedded training systems, such as PhishGuru, that provide training if the user falls victim to a simulated phishing attack work better than generic training a week after the training (Kumaraguru, et al. 2008). Building on this study, Kumaraguru, et al. (2009) confirmed these results even after 28 days and also found participants preferred receiving anti-phishing training in their regular use of email (Kumaraguru, et al. 2009).

To be most effective, Jampen, et al. (2020) argue anti-phishing training should be part of a layered approach, which includes software, such as machine learning, to automatically filter or block phishing attacks (Jampen, et al. 2020). However, Qabajeh, et al. (2018) argues that machine learning is critical to dealing with phishing in the future as phishing tactics are evolving faster than

they can be implemented into a training program (Qabajeh, et al. 2018). Yet, Jampen, et al. (2020) agree machine learning is important, but argue machine learning is not a "silver bullet" as phishers can use the technology as well to try to out maneuver the defense (Jampen, et al. 2020). Similarly, Althobaiti, et al. (2019) review the literature on different automated techniques and find that anti-phishing training is still a key component to augment the automated filters (Althobaiti, et al. 2019).

Altogether, the majority of the literature find that anti-phishing training is part of an effective prevention strategy. However, there is a lack of evidence that legislation providing training is actually effective. While the above studies focus on specific training programs, no previous studies examine if training programs initiated through legislation are effective. Instead, works, such as Spidalieri (2015), simply argue that training should be encouraged or utilized as part of a state's comprehensive cybersecurity strategy. Thus, there is a belief that cybersecurity legislation that provides training would be beneficial. Certainly, if training leads to the detection of a phishing email, it can directly prevent a ransomware attack. Therefore, I argue that legislation providing or mandating cyber security *training* should have the largest negative effect on ransomware attacks.

The review of the literature also found that automated filters can detect and prevent phishing attacks before they even reach a user and are therefore an important part of an effective anti-phishing strategy. However, the available data limits the study of the effectiveness of this tactic, as well as, the ransomware prevention tactics of up to date antivirus software, practicing good cyber hygiene, and implementing best practice procedures. While the research reviewed points to these three tactics being important as part of a comprehensive ransomware defense strategy[26], there is no available data on these topics. This lack of data is, in part, due to states, with

[26] Hallenback (2020) argues that minimum standards of cyber hygiene should be included in cybersecurity legislation as many government agencies continue to neglect this important security tactic (Hallenback 2020).

the exception of a bill providing funding for next generation antivirus software in Montana in 2019, not including these items in legislation during 2015-2019 time period (NCSL 2020). Without available data, there is no way to quantitatively evaluate the efficacy of these tactics on the number of ransomware attacks.

With the hypothesis in mind, the next chapter explores the data on legislation in more detail. I examine how states have varied in their policy approaches to cybersecurity and present descriptive trends in cybersecurity legislation. This chapter explores what types of specific issues cybersecurity legislation has addressed and the frequency with which proposed legislation becomes law using a database of cybersecurity legislation at the state level from 2015-2019 from the National Conference of State Legislatures.

CHAPTER IV

STATE CYBERSECURITY LEGISLATION TRENDS

In the last chapter, I examined ransomware, its strategies, and potential counter-strategies in detail. In this chapter I explore how states have responded to this rapidly emerging threat through legislation. The data on state cybersecurity legislation used in this dissertation come from the National Conference of State Legislatures (NCSL) (NCSL 2020). The NCSL provides a database of all the cybersecurity related state legislation that was proposed from 2015 through 2019. First, I provide a general overview and background of the NCSL and the data. Then I present descriptive trends in cybersecurity legislation to explore the frequency types of legislation are proposed versus passing. I also provide some examples of these bills. I start with election laws in the second section, followed by breach laws, insurance laws, crime laws, and training insurance laws in the following sections. Finally, I conclude this chapter in the sixth section.

Background of the NCSL

The NCSL was founded in 1975 as a resource to help legislatures in the states, territories, and commonwealths of the United States. Their mission is to help these various legislatures communicate and share resources to improve all of their effectiveness. The NCSL also represents legislatures in disputes over power and authority issues between states and the federal government.[27] One way they accomplish these goals is to provide resources for legislators and

[27] States and the federal government can have disputes over power and authority between these two levels of government. These disputes can include "state sovereignty and state flexibility and protection from unfunded federal mandates and unwarranted federal preemption" (NCSL 2020). The NCSL assists states in defending state interests against the federal government on these and other issues.

their staffs to use. An important resource are the databases they collect on the proposed bills on various topics, such as cybersecurity, throughout the United States (NCSL 2020).

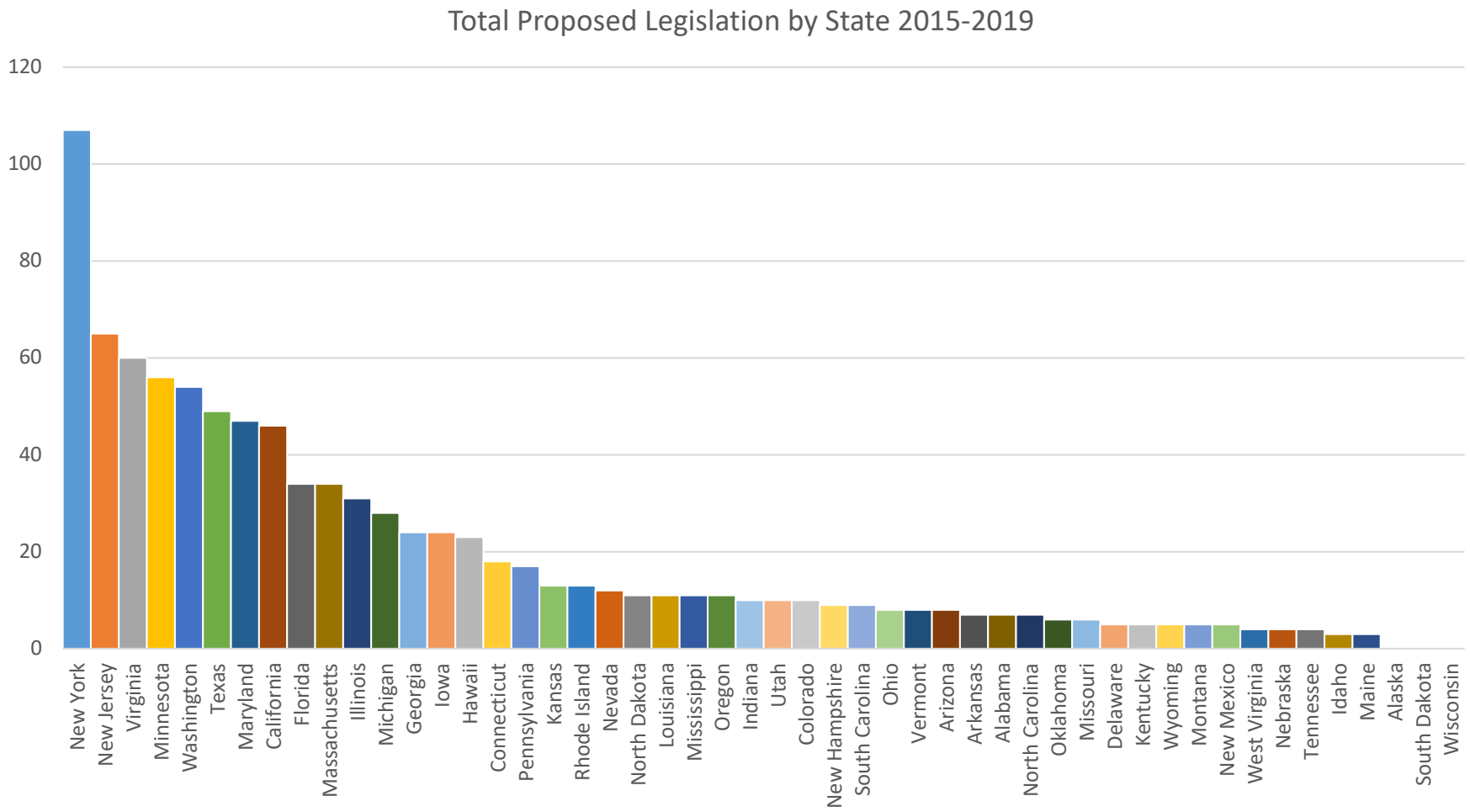
The NCSL's cybersecurity bill database was initiated in 2015, which is the first year they began searching for and compiling proposed bills on the subject. Due to the complex nature of cybersecurity issues, they set up a "task force" to further bring legislators together and help educate them on cyber issues. While the main cybersecurity database compiles the proposed bills by year, they also provide additional resources on sub-topics (e.g., phishing statutes) to allow legislators the ability to easily get information on previously passed bills on these more specific topics.

The database on cybersecurity bills provides the bill number and a brief synopsis of all cybersecurity related bills proposed at the state, territory, and commonwealth level from 2015 continuing into 2020. They report whether a given bill was enacted or whether it failed due to various reasons, such as being vetoed by the governor. While they do not provide a detailed explanation of the process they use to obtain the information in the database, they advise checking the relevant legislature's website for the most current bill status or bill details. Thus, it appears the NCSL obtains most of its information directly from state, territory, and commonwealth websites that include the full bill's language.

From 2015-2019 there were 947 proposed bills on cybersecurity throughout all 50 states.[28] Of the proposed bills, 233 were enacted into law, about 24 percent. The remaining 714 bills either failed to pass through the state legislature, were paused indefinitely, or were vetoed. States proposed an average of almost nineteen laws and enacted an average of four and half laws. As seen in Figure 4.1 and Figure 4.2, New York proposed the most laws, almost double any other state at 107, but only enacted four, or about 4%, of these laws. They were followed by New Jersey

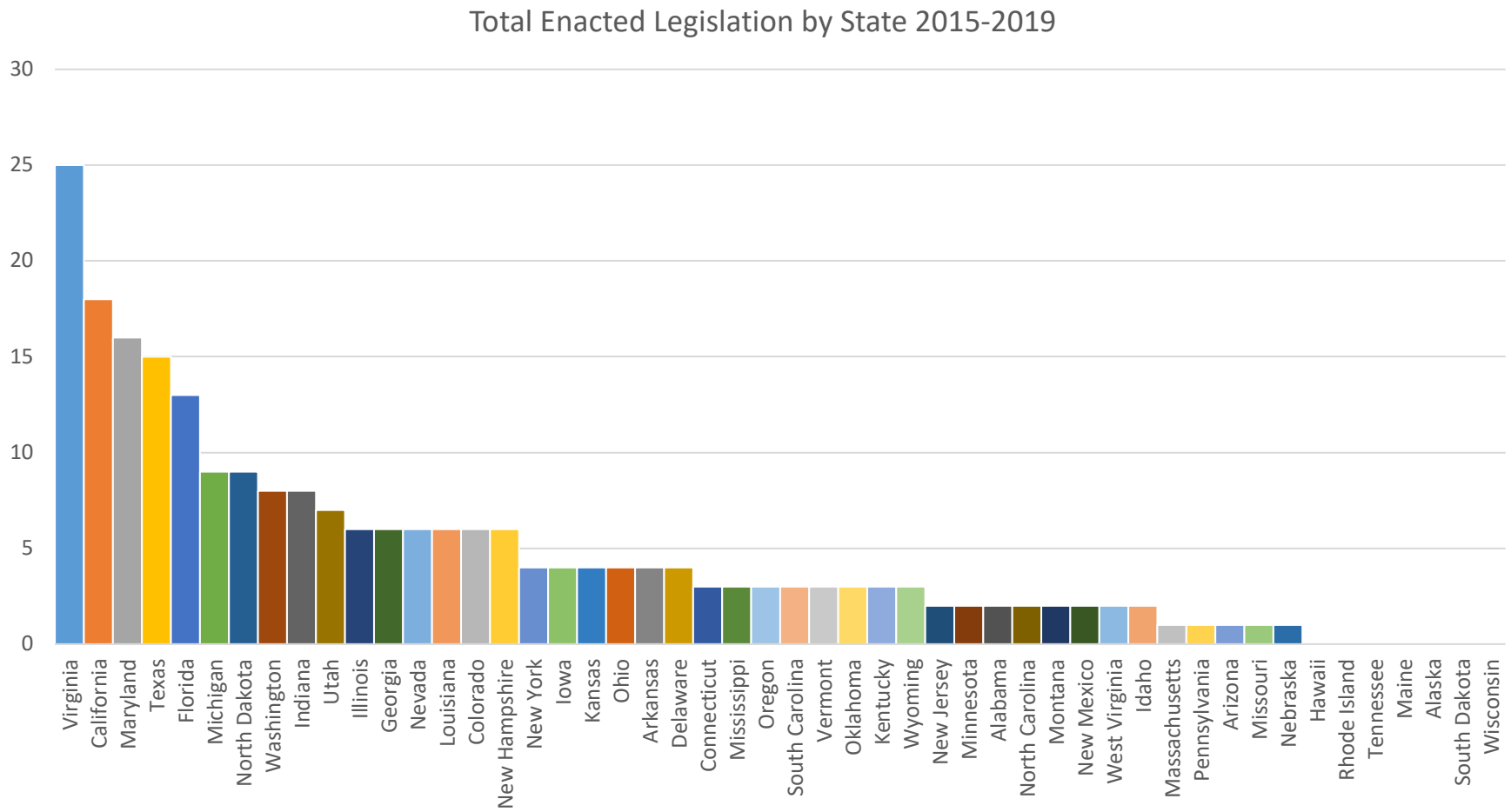
[28] The database also includes bills from the District of Columbia, and Puerto Rico, but the thirteen laws proposed by Puerto Rico and the District of Columbia are not included in this study because they were missing other data.

Figure 4.1: Total Proposed Legislation by State 2015-2019



Data Source: NCSL, "Cybersecurity Legislation 2019," *NCSL* [data file], 2020, accessed August 15, 2020, retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

Figure 4.2: Total Enacted Legislation by State 2015-2019



Data Source: NCSL, "Cybersecurity Legislation 2019," *NCSL* [data file], 2020, accessed August 15, 2020, retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

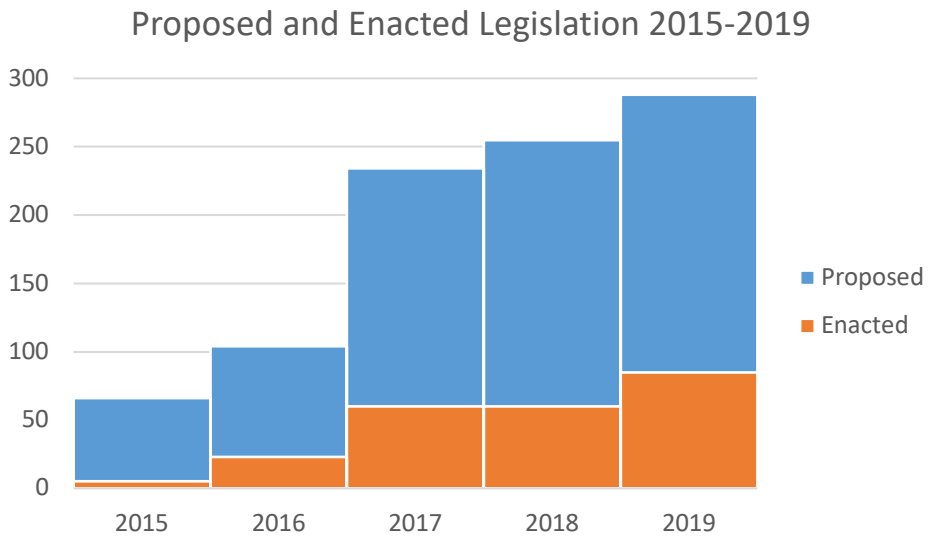
with 65 bills, Virginia with 60 bills Minnesota with 56 bills, and Washington with 54 bills proposed. Alaska, South Dakota, and Wisconsin did not propose any legislation. Virginia was the largest producer of new laws, passing 25 proposed bills into law. They were followed by California with 18, Maryland with 16, Texas with 15, and Florida with 13 bills passed into law. Interestingly, Virginia was able to accomplish both a high amount of proposed legislation and the most number of passed legislation while they had a legislature that was an average of 60% Republican and a Democrat governor. Thus, at least in the case of Virginia, it appears that cybersecurity had a high degree of bipartisan consensus.

North Dakota, Indiana, and Delaware were the most successful at passing proposed laws with an 82%, 80%, and 80% pass rate respectively. However, when compared with other states, these states passed relatively fewer laws at nine, 8, and 4 laws passed respectively. Interestingly, these three states had either Republican or Democrats in control of both the legislature and governor. The government in North Dakota and Indiana remained in Republican control, while Delaware remained in Democrat control. Four states, Hawaii, Rhode Island, Tennessee, and Maine, were the least successful states who had none of the proposed laws pass. Of note, Rhode Island proposed thirteen laws and Hawaii proposed twenty-three laws without successfully enacting them. It is not clear from the data why Rhode Island and Hawaii were so unsuccessful when Rhode Island had a legislature that was an average of 86% Democrat and Hawaii's was an average of 90% Democrat and both states had a governor who was Democrat for the whole time period. So the failure to enact cybersecurity legislation was not a result of partisan gridlock in these two states.

As seen in Figure 4.3, both the number of proposed and enacted cybersecurity legislation have risen steadily since 2015. There were only 66 bills proposed in 2015 and only 5 were enacted

into law. By 2019 these numbers had risen to 288 different bills proposed and 85 of those bills became law.

Figure 4.3: Proposed and Enacted Legislation 2015-2019



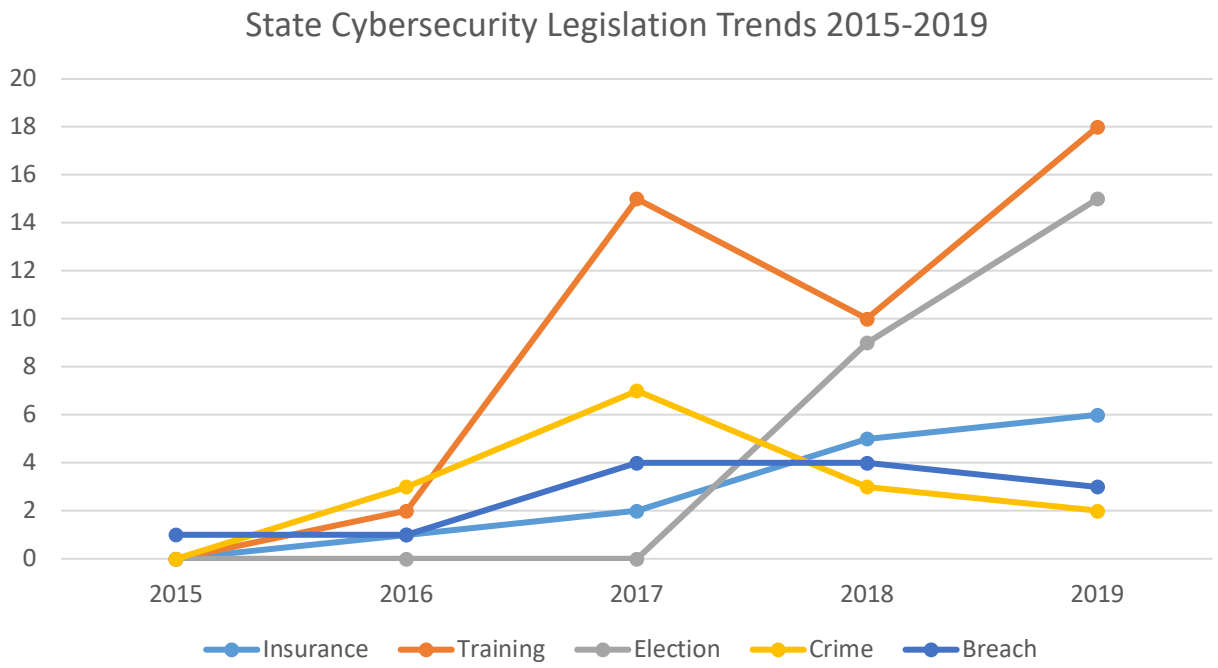
Data Source: NCSL, "Cybersecurity Legislation 2019," *NCSL* [data file], 2020, accessed August 15, 2020, retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

The previous chapters helps explain why the number of cybersecurity laws being proposed and enacted rapidly increased after 2015. Cybercrime, especially security breaches, expanded rapidly starting in 2005 (De Groot 2019). At the same time due to the policy vacuum (Moor 1985) there were few laws even at the federal level regarding cybersecurity. Then when President Obama came into office in 2008, he worked to update federal cybersecurity legislation and was finally successful in 2014 and 2015. Yet, these bills were still insufficient to address these growing cyber challenges (Singh 2016; Tran 2016). Further, 2013 saw the release of CryptoLocker, the first true

cryptoviral ransomware, which caused damage worldwide in only a few months (Nadir and Bakhshi 2018). Thus, due to the increase in cybercrime threats, such as ransomware and security breaches, and due to the passing of insufficient cybersecurity bills at the federal level, states likely realized the need to address these growing challenges themselves through legislation.

What is clear from the database is that states have worked on similar bills at similar times. The bills cover a multitude of topics, but there are a few trends in the bills, including bills on: elections, breaches, insurance, crimes, and training. The five trends were found by searching for keywords within the description of the enacted laws. If a keyword was found within the text, then the variable was coded as 1 for that category, otherwise it would be a 0. The data was then combined per category by state and year, meaning a single year could have multiple laws for one category. If a law covered multiple topics, a single enacted law could potentially be coded as a 1 for each category. For the election legislation the keywords used were “election”, “vote”, and “voti” to cover any permeations of the word vote. The breach and insurance legislation variables were straightforward searches for the words, “breach” and “insurance”, themselves. While, the crime legislation variable was compiled by searching for “crim”, “offense”, and “penalt” and the training legislation variable was created with the keywords “training”, “educ”, and “aware”. I checked for quality control by sorting by year and then alphabetically by state. Then I examined the first and last 10 cases in the data set to confirm they were accurately coded. As Figure 4.4 shows, most of these similar bills passed in clusters in 2017, 2018, and 2019. For example, Figure 4.4 shows that as the 2020 election year drew closer more states passed laws concerning cybersecurity and elections. These trends show that the legislators within states clearly communicate and reach out for ideas from other states, likely with the NCSL’s assistance. The next sections discuss these trends in more detail.

Figure 4.4: State Cybersecurity Legislation Trends 2015-2019



Data Source: NCSL, "Cybersecurity Legislation 2019," *NCSL* [data file], 2020, accessed August 15, 2020, retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

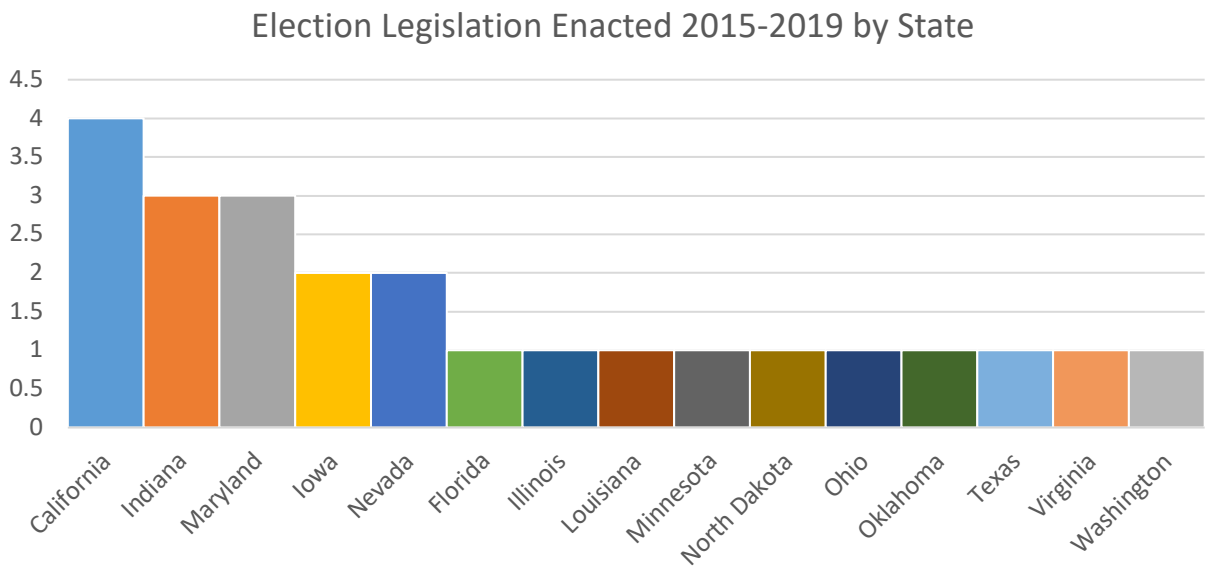
Election Legislation

The first trend observed in the cybersecurity legislation enacted during the study period are laws concerning cybersecurity for elections. As seen in Figure 4.5, there were a total of 24 laws passed in this category. No election laws were passed from 2015-2017, then as the 2020 election drew closer nine laws were passed in 2018 and fifteen laws were passed in 2019. California passed four election cybersecurity laws, while Indiana and Maryland passed three each. Iowa and Nevada both passed two laws. The remaining ten were passed by Florida, Illinois, Louisiana, Minnesota, North Dakota, Ohio, Oklahoma, Texas, Virginia, and Washington with one law each. These laws focused on appropriating funding for election cybersecurity infrastructure and auditing of local

election security processes, require information on election equipment used in each jurisdiction, and requires reporting of any security violations to appropriate body (NCSL 2020).

This trend of laws is almost certainly in response to the widespread cyberattacks which occurred in the last presidential election in 2016. At that time, there were attacks on voting systems in 39 states. In Illinois the hackers attempted to change voter data and while they were discovered they were able to steal personal information for around 90,000 people. Other states known to be affected were California and Florida (Riley and Robertson 2017). Interestingly, Florida in addition to being compromised in the Russian hack, they also had a ransomware attack on an election site only weeks before the 2016 election (Flores 2016). Yet, Florida only passed one legislation on cybersecurity for elections in 2019 which appropriated funds to "country supervisors of elections for cybersecurity initiatives" (NCSL 2020).

Figure 4.5: Election Legislation Enacted 2015-2019 by State

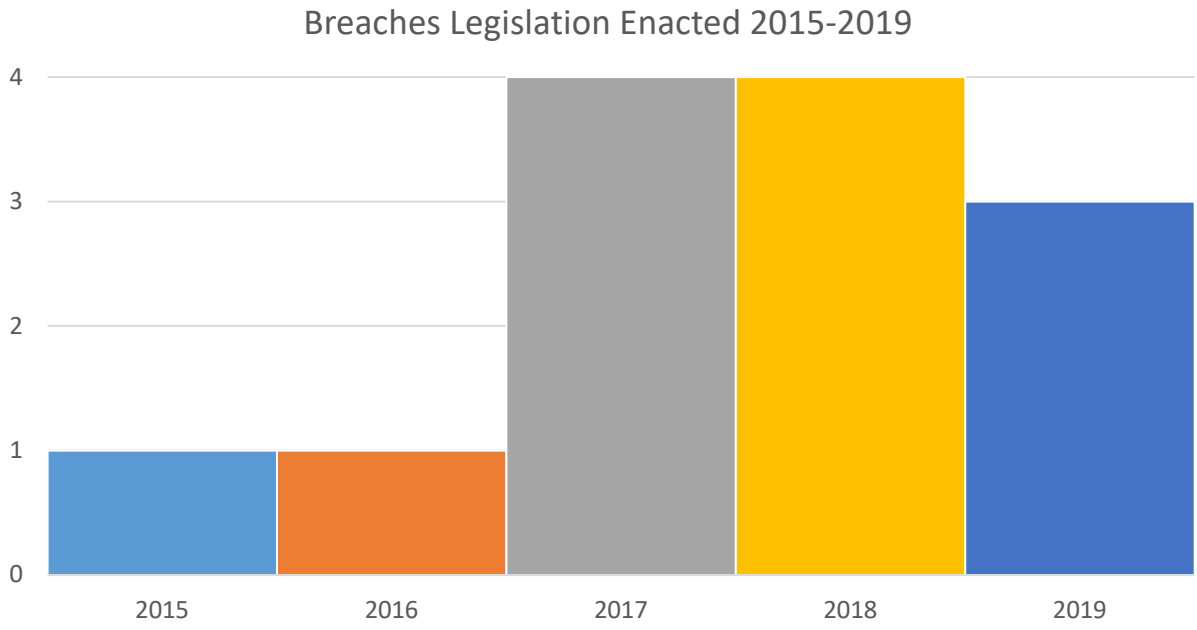


Data Source: NCSL, "Cybersecurity Legislation 2019," *NCSL* [data file], 2020, accessed August 15, 2020, retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

Breaches Legislation

A second trend observed in the cybersecurity legislation from 2015-2019 are laws related to security breaches. There were a total of thirteen of these laws enacted in the study period. As seen in Figure 4.6, one law was passed in 2015 and 2016, then four were passed in 2017 and 2018, and finally three more were passed in 2019. California and Florida passed the most breach related laws with two each. The remaining laws were spread out amongst Arizona, Arkansas, Delaware, Illinois, Michigan, Nebraska, New Hampshire, North Carolina, and Virginia each passing one law. These laws address concerns over the storage of voter or consumer credit information, disclosing breaches of voter or consumer credit information, and yearly reviews of breaches to address any weakness in cybersecurity measures to prevent future breaches (NCSL 2020).

Figure 4.6: Breaches Legislation Enacted 2015-2019



Data Source: NCSL, "Cybersecurity Legislation 2019," *NCSL* [data file], 2020, accessed August 15, 2020, retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

As discussed previously as part of the history on cybercrime, some cybercriminals attempt to breach government and businesses' networks to steal data containing personal information, such as social security and credit card numbers, and proprietary information, such as research and technology, to use or sell on the black market. Breaches can occur through hacking, phishing, theft, inside jobs, or negligence. This type of cybercrime has always been present but became more significant starting in 2005. Criminals have successfully stolen millions of records of personal and proprietary data since that time (De Groot 2019). Thus, the laws passed in this category are to address this serious issue by requiring companies to provide reasonable protection of personal data and requiring companies to disclose breaches to the affected parties.

As previously mentioned in the history on cybersecurity legislation, California was ahead of the curve on requiring companies to disclose security breaches that affected personal information of Californians. In 2003, which is before the large wave of major security breaches starting in 2004, California passed the Notice of Security Breach Act to address these concerns and "punish firms for cyber security failures" (Singh 2016). As seen in the data, California appears to be continuing to lead the pack on this issue. The two newest laws, Assembly Bill No. 1678, Chapter 96 and Assembly Bill No. 1859, Chapter 532, add to the code on security breaches by explicitly stating that entities holding voter registrations information and consumer credit report information must maintain adequate security and disclose any breaches (NCSL 2020).

Importantly, ransomware can be classified as a breach under HIPPA if personal health information was compromised (McGee 2016). All of the states, except for Delaware, which passed breach laws had a ransomware attack occur either the year of or the year before the law was passed (NCSL 2020). Some of these laws may have been enacted in reaction to the growing threat of ransomware.

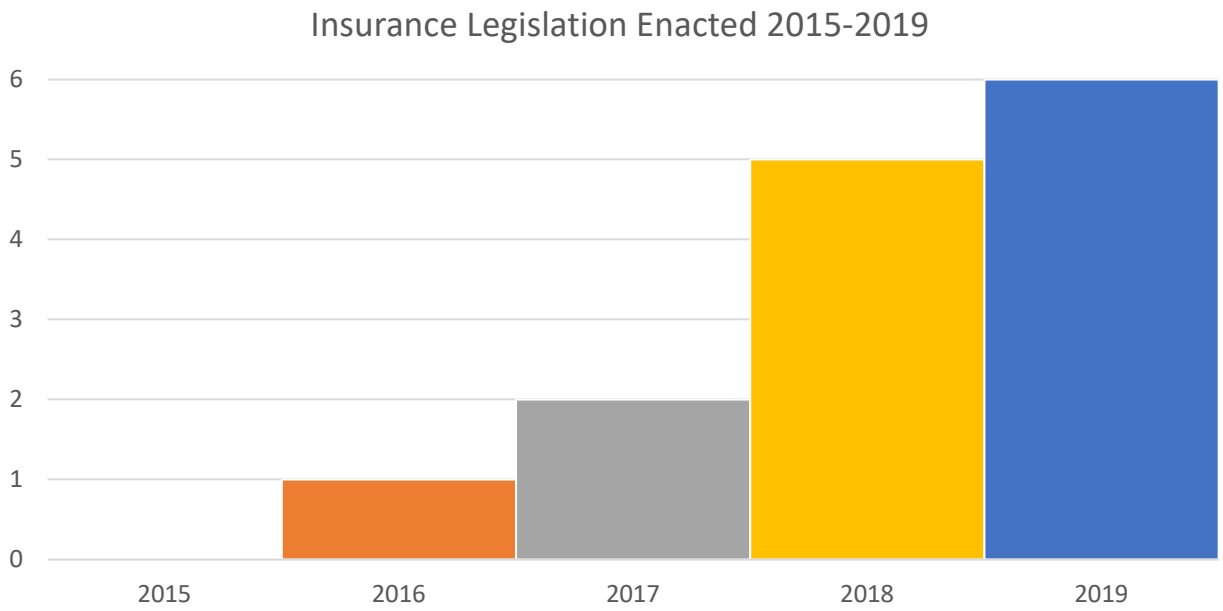
Insurance Legislation

The third trend observed in NCSL data is legislation concerning insurance. There were a total of fourteen laws passed regarding insurance. As seen in Figure 4.7, the number of these laws passed each year increased over time. One was passed in 2016, two in 2017, five in 2018, and six in 2019. Indiana passed two laws, while the remaining laws were passed amongst twelve states, Alabama, Connecticut, Delaware, Florida, Georgia, Kansas, Michigan, Mississippi, New Hampshire, Ohio, South Carolina, and West Virginia. Within this trend there are two sub-trends. First, some laws focus on appropriating funds or investigating risks in order to obtain cyber insurance state government. The second set of laws focus on requiring standards based on the licensee's risk for data security, after cyber incident investigation, and notification to the director (NCSL 2020).

The first sub-trend focuses on appropriating funds for cyber insurance for state government agencies. Insurance can potentially help boost cybersecurity because insurance companies may require a level of cybersecurity in order to write the policy or encourage better cybersecurity measures through premium reduction based on the insured's cybersecurity level (CISA 2020). The Cybersecurity & Infrastructure Security Agency (2020) explains cyber insurance could help promote cybersecurity "by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection" (CISA 2020). The insurance company wants to limit its risk and may refuse to write policies or charge higher premiums for businesses that do not meet the standard level of cybersecurity since they would be considered too risky. In fact, just the steps to apply for cyber insurance could benefit organizations' cybersecurity. "[Insurers] help businesses identify tools and best practices they may lack [… and] ask questions to better gauge how embedded

cybersecurity is in a company's risk management strategy and determine how vulnerable a firm is to compromise" (Nakashima 2015). Therefore, laws that provide funds for state governments to obtain cyber insurance could potentially increase a state's cybersecurity because the government agencies will need to meet the insurance company's cybersecurity standards.

Figure 4.7: Insurance Legislation Enacted 2015-2019



Data Source: NCSL, "Cybersecurity Legislation 2019," *NCSL* [data file], 2020, accessed August 15, 2020, retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

Two states passed these types of laws. Georgia passed House Bill 44, Act 37, which appropriated funds to the state government for, among other items, cyber insurance. On the other hand, Indiana appropriated funds for a study on the possibility of adding cybersecurity as a component of the commercial code for liability insurance. These laws could potentially help to strengthen the cybersecurity in these two states.

As explained above, cybersecurity insurance should help promote better cybersecurity. However, there is a possibility that cybersecurity insurance could cause the opposite effect through the creation of a moral hazard, or an incentive to take on higher risk than an entity would otherwise take on due to the entity's expectation to be indemnified through insurance (Bailey 2014). Porup (2018) explains, "Why bother doing the right thing if insurance is going to pay you to do the wrong thing?" Moral hazards affect all types of insurance, including cybersecurity insurance. For cybersecurity insurance the fact of having insurance could cause an organization to invest less in cybersecurity, essentially opening itself up to more risk of suffering a cyberattack (Bailey 2014; Porup 2018). Baily (2014) explains that this can cause insurers to increase premiums to all insureds, which also may increase risk as now organizations must pay higher premiums using funds which could potentially have been spent to increase cybersecurity.

While moral hazards certainly can create an incentive for organizations to decrease cybersecurity, the insurance companies have means to counteract this effect. Borup (2018) explains, "The time-tested strategy by insurance carriers to limit moral hazard is to use insurance deductibles and co-pays, and to cap maximum payouts. That way the insured shares in the financial risk and is motivated to […] deploy strong cybersecurity controls in their enterprise." Further, the reputational costs of suffering a cyberattack present a risk that cannot always be fully repaired through insurance indemnification. The loss of customers and future business due to the reputation damage from a cyberattack should also dissuade most organizations from falling into a moral hazard on cybersecurity.

The second sub-trend focuses on requiring standards based on the licensee's risk for data security, after cyber incident investigation, and notification to the director, which are all aspects of the National Association of Insurance Commissioners' (NAIC) Data Security Model Law. The

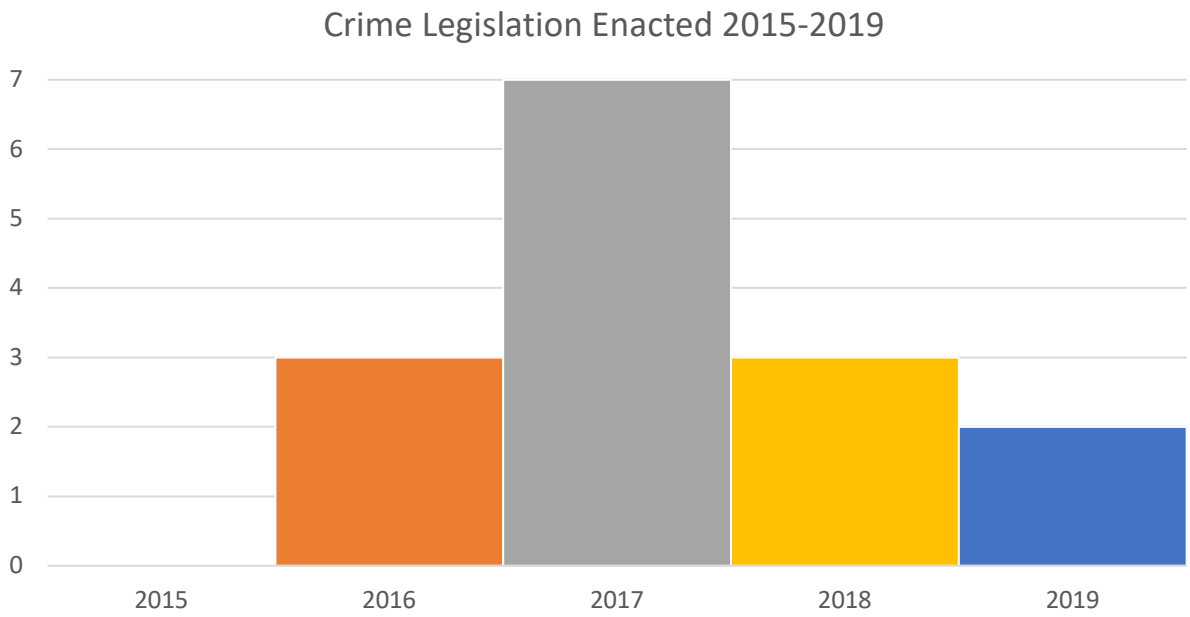
NAIC is an association of the insurance commissioners from all fifty states, because in the United States insurance is regulated at the state level. The Data Security Model Law was created as a guide for states to use for legislation to "establish standards for data security and for the investigation of and notification to the Commissioner of a cybersecurity event" (Kanwisher and Mobley 2018). In some ways, this is similar to the breach laws, because it requires the insurance companies to comply with minimum standards for protecting personal data and failures to insurance Commissioner.

Within the study period Alabama, Connecticut, Delaware, Mississippi, New Hampshire, South Carolina, and Michigan, adopted versions of the Data Security Model Law. However, at the time of this writing, this has expanded to three additional states, including Indiana, Louisiana, and Ohio. A further six states, Illinois, Maine, Minnesota, Oklahoma, Rhode Island, and Wisconsin, are currently considering adopting the law (Weatherford 2020).

Crime Legislation

The fourth trend observed in the cybersecurity legislation from this time period are bills pertaining to crime or criminalization. There were fifteen laws passed concerning crime in the study period. Figure 4.8 shows that three laws were enacted in 2016, seven in 2017, three in 2018, and two in 2019. Utah passed the most crime laws of any state with a total of three laws. Colorado and Virginia passed two, while California, Connecticut, Indiana, Louisiana, Michigan, Texas, Washington, and Wyoming passed one law each. These laws concerned the criminalization of interruption or interference with critical infrastructure, electronic communication harassment, utilizing a computer to engage in prostitution of a minor, skimming payment cards, and ransomware (NCSL 2020).

Figure 4.8: Crime Legislation Enacted 2015-2019



Data Source: NCSL, "Cybersecurity Legislation 2019," *NCSL* [data file], 2020, accessed August 15, 2020, retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

As discussed in the history on cybersecurity legislation, it is critical that cybercrimes be criminalized through laws specifically outlawing the particular behavior, as opposed to relying on interpretations of previous non-cyber laws (Schjolberg 2008). Failure to properly codify and criminalize cybercrimes can result in the perpetrator walking free, such as those responsible for the ILOVEYOU virus (Ogu, et al. 2020). Thus, this grouping of legislation is attempting to ensure that the cybercrimes being committed are in fact illegal in their state so that, if found, they can hold the perpetrator responsible. The threat of punishment could deter potential cybercriminals (Alexander 2007).

In fact, it appears Connecticut was following this logic with bill H.B. 7304 passed in 2017 as Public Act No. 17-223. This legislation criminalizes computer extortion through the use of

ransomware as a class E felony. A person is guilty of this crime if they introduce ransomware onto a computer and make a demand of payment to remove it in exchange for restoration of access. Importantly, they define ransomware clearly in the law, as Schjolberg (2008) advised should be done.

> "[R]ansomware" means any computer contaminant or lock placed or introduced without authorization into a computer, computer system or computer network that restricts access by an authorized person to the computer, computer system, computer network, or any data held by the computer, computer system or computer network. (Public Act No. 17-223 2017)

The timeframe of this bill shows that the Connecticut legislature was concerned about the rise of ransomware and wanted to ensure that criminals could be held accountable for these acts.

Similar laws specifically criminalizing computer extortion were passed by Texas and Wyoming in 2017 and Michigan in 2018 (NCSL 2020). Interestingly based on the ransomware data from StateScoop, Michigan, Wyoming and Texas were struck by ransomware attacks in 2016. Michigan had one reported attack in 2016 and then another in 2018. Wyoming's only reported attack occurred that year, while Texas had six in 2016 and four in 2017 (Freed 2019). It could be that these laws were in response to the attacks they suffered. In fact, Johnston (2018) attributes Michigan's 2018 laws to ransomware attacks, which were not reported in the data, totaling $2.6 million in damages in 2017 (Johnston 2018). On the other hand, Connecticut had no reported attacks before passing the above mentioned law. Their inspiration for passing the law may have come from attacks on one of their New England neighbors, such as Massachusetts who suffered four attacks in 2016.

These laws may have been in reaction to the emerging threat of ransomware, but the criminalization of computer extortion does not seem to have deterred would be ransomware criminals. While Wyoming had no further reported attacks, Michigan suffered two attacks in 2019

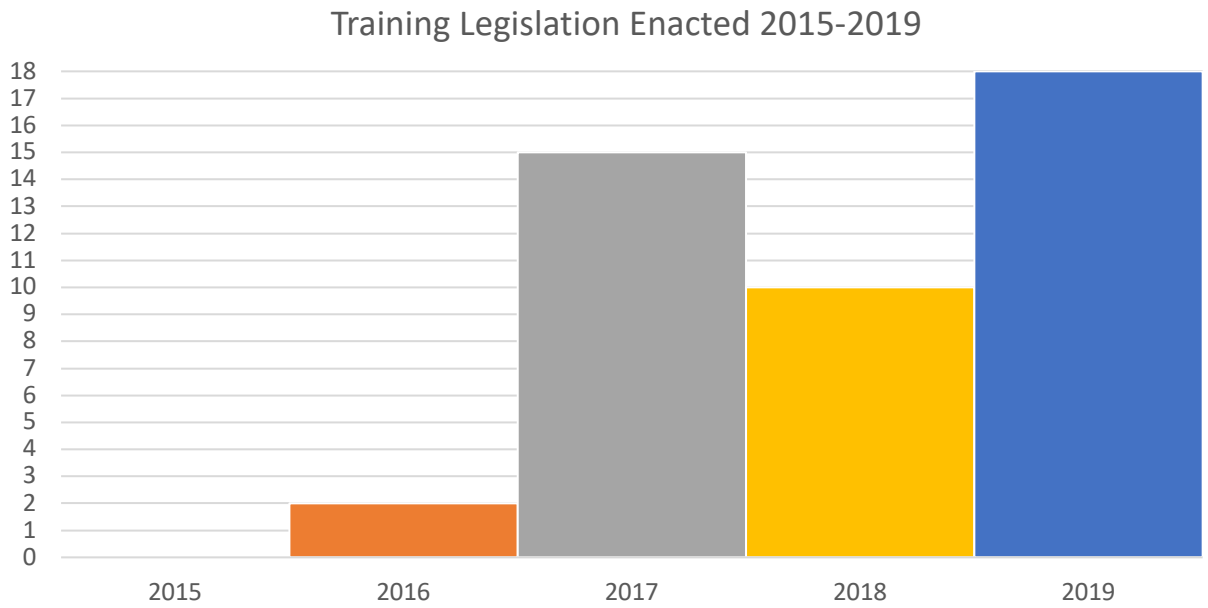
and Connecticut had seven reported attacks in 2018 and eight in 2019. However, the worst was Texas who had 17 reported attacks in 2019 (Freed 2019). Potential ransomware criminals were likely not deterred by criminalization because of the low technical cost of entry, the anonymity of the attack, and globalized nature of the crime. As discussed before, ransomware requires very low technical abilities due to the availability of ransomware as a service, which essentially provides 'do it yourself' kits for purchase. Further, the attacks are almost entirely untraceable since the advent of cryptocurrency as a payment method. Finally, respatialization means the attacker could, and likely is, on the other side of the world and thus difficult, if not impossible, to hold accountable unless the crime was egregious enough to be addressed at the international level. Yet, even though the criminalization of computer extortion does not appear to deter attacks, it was still important for these states to pass these laws to discourage their own residents from engaging in this activity and so that if caught the perpetrators can be prosecuted.

Training Legislation

The fifth and final trend observed in the cybersecurity legislation data set are bills pertaining to training. There were forty-five training related bills passed. As seen in Figure 4.9, two were passed in 2016, fifteen in 2017, ten in 2018, and eighteen in 2019. Maryland had the most laws relating to training, passing six. California and Texas passed four laws each, while Georgia, Indiana, Michigan, and Virginia each passed three laws. Delaware, Florida, and Nevada each passed two laws. The remaining thirteen were passed by Arkansas, Colorado, Connecticut, Illinois, Iowa, Missouri, New Jersey, New Mexico, North Dakota, Ohio, Oklahoma, Pennsylvania, and Vermont. These laws focus on establishing requirement for training on cybersecurity for certain state employees and members working on voting systems, appropriating funds for

workforce education and training, establishes scholarship programs for cybersecurity studies, and forming committees to investigate cybersecurity preparedness (NCSL 2020).

Figure 4.9: Training Legislation Enacted 2015-2019



Data Source: NCSL, "Cybersecurity Legislation 2019," *NCSL* [data file], 2020, accessed August 15, 2020, retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

Training is a key component in combating cybercriminals, especially against phishing (Althobaiti, et al. 2019). Phishing targets the weakest link, human error, to bypass cybersecurity defenses and infiltrate the network (Verizon 2017). Phishing is used in many different cybercrimes, including security breaches and ransomware. This trend of laws help to better prepare states and potentially businesses or the public to be more aware of cybercrime strategies, such as phishing. They also help to strengthen cybersecurity in the workforce through scholarships and education programs.

Illinois enacted a law specifically with these goals in mind. House Bill 2371, passed in 2017 as Public Act No. 100-0040, requires state employees to undergo cybersecurity training. “The training shall include, but need not be limited to, detecting phishing scams, preventing spyware infections and identity theft, and preventing and responding to data breaches” (Public Act No. 100-0040). The law requires every employee, but the definition of employee “does not include an employee of the legislative branch, the judicial branch, a public university of the State, or a constitutional officer other than the Governor” (Public Act No. 100-0040). If implemented well, this additional training should help to reduce the future number of cyberattacks, including ransomware.

In addition to this short term training, these bills also focus on developing the future cybersecurity workforce through education and scholarships. A 2016 survey found that state officials cite a lack of available cybersecurity talent as a major issue for creating an effective cybersecurity strategy (Robinson and Subramanian 2016). This lack of talent is due largely to small cybersecurity budgets, which mean small cybersecurity salaries. States simply cannot compete for talent with private sector, where “salaries for information security professionals have risen dramatically in recent years” (Robinson and Subramanian 2016). Thus, laws that create programs to educate and develop future cybersecurity professionals are needed to help states have the resources for effective cybersecurity programs.

To address this issue, Maryland passed Senate Bill 204 in 2018 as Chapter 415. The bill establishes the Cybersecurity Public Service Scholarship Program, which provides funds for cybersecurity degrees in return for working for the state government for a certain number of years. The successful applicant must also maintain a GPA of at least 3.0. This program should help to

strengthen Maryland's cybersecurity workforce. However, many bachelor's degrees take four years to complete. Thus, it will take some time before Maryland would notice any change.

Conclusion

The NCSL database of cybersecurity legislation provides important information to help state legislators combat the now pervasive threat of cybercrime. Examining the database for the time period of 2015-2019 there are five trends in the bills, including bills on: elections, breaches, insurance, crimes, and training. The laws on elections are likely in response to the cyberattacks committed by Russia and others during the 2016 presidential election. These laws will hopefully better prepare states for the 2020 presidential election. Similarly, the breach laws are likely a response to the now ever present threat of hackers stealing personal information. These laws should encourage entities to strengthen their cybersecurity to avoid any penalties due to breaches. Insurance legislation can strengthen the insured's cybersecurity levels through the underwriting process (Nakashima 2015). These laws can also help to strengthen insurance companies cybersecurity through laws based off the NAIC's Data Security Model Law. On the other hand, criminal laws seek to make sure these cybercrimes are illegal in their states so the perpetrator can be prosecuted if caught. Finally, training laws can directly prevent cybercrimes by teaching employees how to spot cybercrime threats, such as phishing. Further, these laws focus on developing the future workforce through scholarships to help compete with the private sector for cybersecurity talent.

All of these different legislation trends are expected to have negative relationships with the number of ransomware attacks. As the number of laws goes up, the number ransomware attacks should go down. States more concerned with cybersecurity should be passing more cybersecurity

legislation, which should improve their cybersecurity preventing ransomware attacks. Thus the hypotheses, including the main hypothesis described in the previous chapter, are as follows:

> **Hypothesis 1 (H1)**: State legislation providing or mandating cyber security training is negatively associated with the likelihood that the state experiences a ransomware attack.
>
> **Hypothesis 2 (H2)**: State legislation on cybersecurity for elections is negatively associated with the likelihood that the state experiences a ransomware attack.
>
> **Hypothesis 3 (H3)**: State legislation related to cybersecurity on insurance is negatively associated with the likelihood that the state experiences a ransomware attack.
>
> **Hypothesis 4 (H4)**: State legislation on cybersecurity breaches is negatively associated with the likelihood that the state experiences a ransomware attack.
>
> **Hypothesis 5 (H5)**: State legislation on cybercrime is negatively associated with the likelihood that the state experiences a ransomware attack.
>
> **Hypothesis 6 (H6)**: Any enacted state cybersecurity legislation is negatively associated with the likelihood that the state experiences a ransomware attack.

This review of cybersecurity legislation trends sets the foundation for the next chapter. This data is combined with the ransomware attack data, as well as some other control variables to assess the effectiveness of this legislation on reducing the number of ransomware attacks. The chapter starts with a further review of the data and methodology. Then the results are discussed and analyzed.

CHAPTER V

DATA, METHODOLOGY, RESULTS, AND ANALYSIS

In this chapter, I explain the data and methods used to test my main hypothesis that laws providing or mandating cybersecurity training have a negative impact on the amount of ransomware attacks. The first section focuses on the data used in this study. I describe the dependent and independent variables, explain how they were collected, and how they were included in my models. In the second section I describe each model used followed by the results of these tests. Finally, the fourth section provides an analysis of the results.

Data

In this section, I describe the data used, explain how they were collected, and how they were used in my models. First, I discuss the dependent variable, number of ransomware attacks. Then in the second section I discuss the primary independent variables, which are the trends in state cybersecurity legislation. Finally, in the third section I describe the control variables.

Dependent Variable

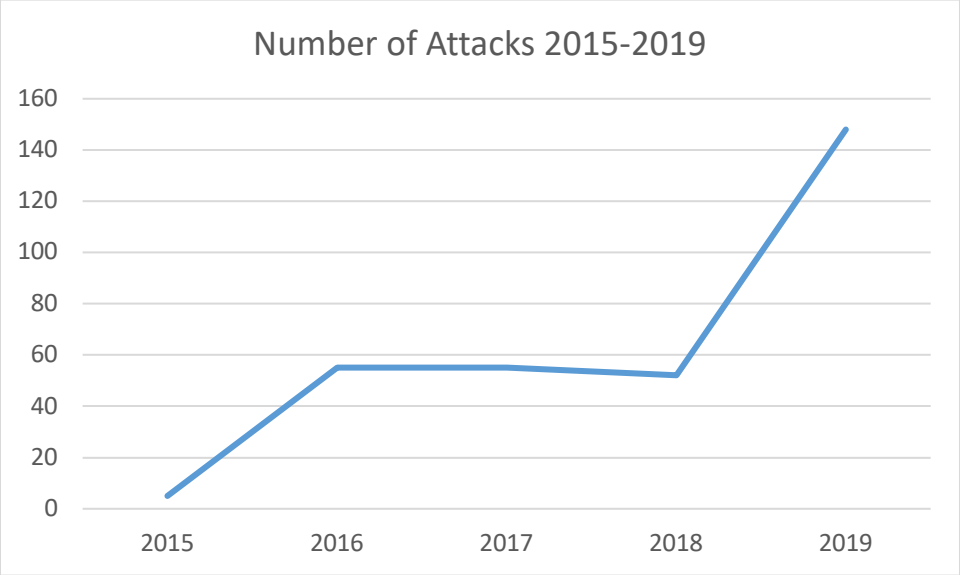
The dependent variable is the number of successful ransomware attacks on state and local institutions per year. This data comes from StateScoop.com, whose focus is on "news and events impacting technology decisions in state and local government" (Freed 2019). StateScoop maintain a database of every known public-sector ransomware attack in the United States since 2013 by compiling attacks which have been made public in the news.[29] StateScoop has attempted to track

[29] Initially on May 13, 2019, StateScoop reported on a dataset of 169 ransomware attacks, which was compiled by Allan Liska from Recorded Future, a cyber security company. Liska compiled most of the dataset by reviewing local

the target of the attack, strain of ransomware used, ransom amount demanded, and whether the victim paid or not. Unfortunately, for reasons, such as the potential reputation costs, victims have incentives not to publicly report or to not fully publicly report attacks. Allan Liska explains, "Ransomware attacks are not always publicly reported by state and local governments and there is no centralized reporting authority, similar to HIPAA requirements, for these agencies" (Liska 2019). In many cases the attacks were reported but the details on if the ransom was paid or how much was paid was not provided by the victim, likely to try to protect themselves from scrutiny that could damage their reputation. Further, StateScoop acknowledges that smaller events, which likely occur daily throughout the country, go unreported (Freed 2019). This underreporting means the data only reflects a subset of attacks. In this case, it reflects attacks on the public sector which were large enough to be reported by the news. Despite this limitation, this is one of the most comprehensive data sets publicly available on ransomware attacks.

papers and local television news reports, as "most of these incidents are not "big enough" to be considered national news […] (Liska 2019). StateScoop has taken up the mantel to continue tracking ransomware attacks since Lisa's initial report. I spoke with Colin Wood, the managing editor from StateScoop, on August 19, 2020. He explained that their first step was to contact some cybersecurity companies to try to obtain additional information on ransomware attacks. Since that time, they have continued to update the dataset based on local news and television reports. They use Google alerts, which update them as new stories are posted online. Then they sift through articles to compile as much information about the attack as possible to update their dataset.

Figure 5.1: Number of Ransomware Attacks 2015-2019



Data Source: Freed, Benjamin. "Ransomware Attacks Map Chronicles a Growing Threat." *StateScoop*, 22 Oct. 2019, statescoop.com/ransomware-attacks-map-state-local-government/.

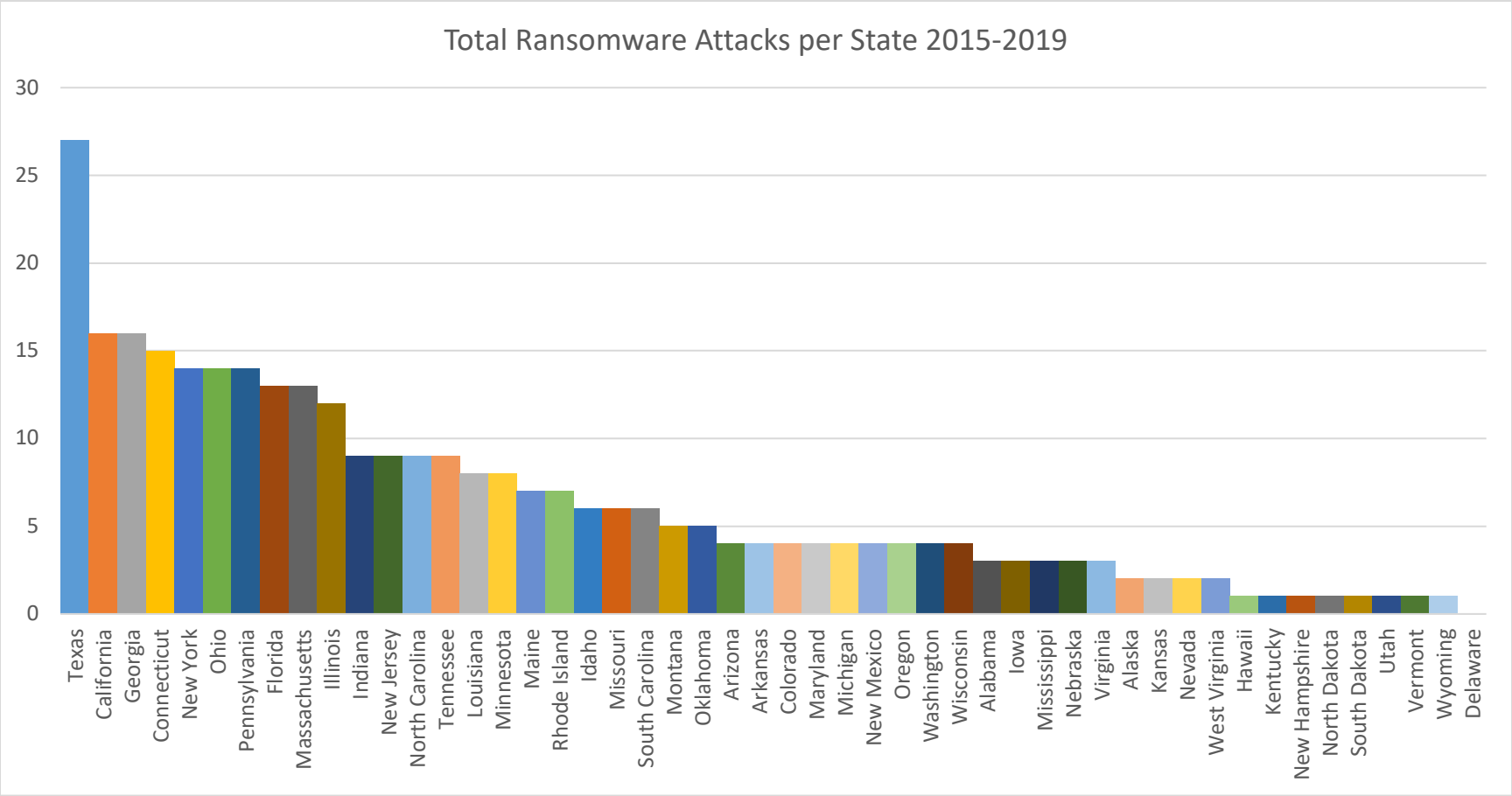
This study focuses on the timeframe of 2015-2019. The total number of recorded attacks during this time period is 315. Figure 5.1 shows the number of attacks dramatically increases over time. In 2015 there were only five reported attacks, but by 2019 the number had exploded to 148 attacks. That is over a 2900% increase in just five years. This largely reflects the global growth in ransomware attacks which rose from 3.8 million attacks in 2015 to 187.9 million attacks in 2019 (Clement 2020). This rise also reflects the change in ransomware strategy over this time period from indiscriminate attacks focused mainly on individual computer users to targeted attacks on businesses and government entities. In 2019 in particular, many attacks focused on state and local government entities, which are generally underprepared due to budgetary constraints (Gates 2019).

The attacks affected all corners of the United States. Figure 5.2 shows the breakdown of total ransomware attacks per state from 2015-2019. The average number total of attacks per state was just over six with a standard deviation of around five. Delaware was the only state that did not

report an attack during the 2015-2019 time period. Texas suffered the most attacks at twenty-seven. They also were hit by the most attacks in a single year with seventeen in 2019. Texas is followed in total attacks by California and Georgia with 16, Connecticut with 15, and New York, Ohio, and Pennsylvania with 14. Overall, states were either affected by roughly the same number of attacks per year or trended upward as time went on.

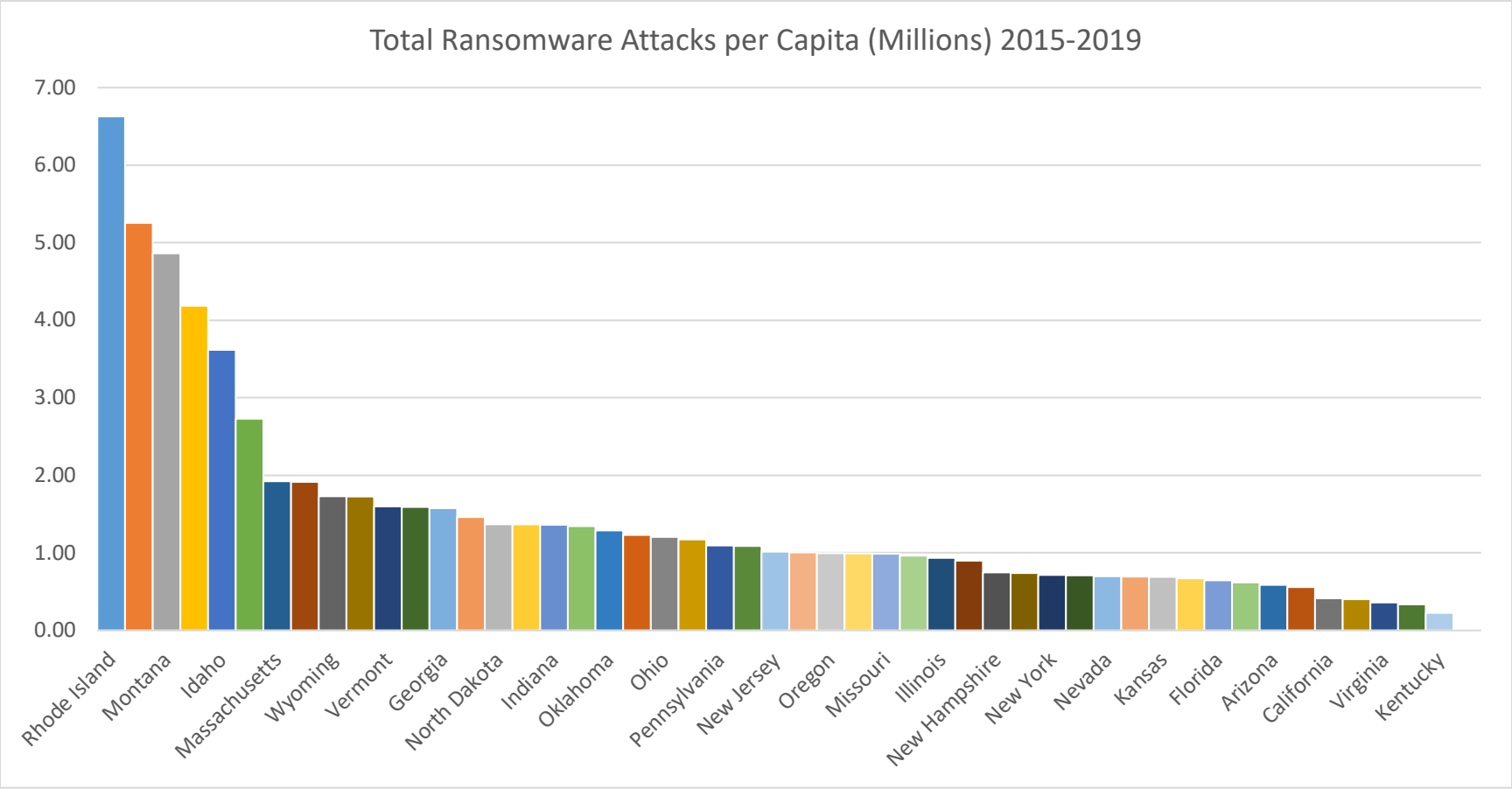
Given the large variation in population size per state, it is useful to also examine the total ransomware attacks per capita. Figure 5.3 displays the total ransomware attacks per capita in the millions from 2015-2019. Examining the number of attacks this way allows us to control for larger states, which are more likely to suffer more attacks simply due to their size. Texas and California, which have the two largest populations, appear far better as both had less than one attack per million people. Rhode Island had the most attacks per capita, with around 6.6 attacks per million people. They were followed by Maine, Montana, and Connecticut, who each had over 4 attacks per million people. Most states had around one or less attacks per million people.

Figure 5.2: Total Ransomware Attacks per State 2015-2019



Data Source: Freed, Benjamin. "Ransomware Attacks Map Chronicles a Growing Threat." *StateScoop*, 22 Oct. 2019, statescoop.com/ransomware-attacks-map-state-local-government/.

Figure 5.3: Total Ransomware Attacks per Capita (Millions) 2015-2019



Data Source: Freed, Benjamin. "Ransomware Attacks Map Chronicles a Growing Threat." *StateScoop*, 22 Oct. 2019, statescoop.com/ransomware-attacks-map-state-local-government/.

Primary Independent Variables

The primary independent variables are based on state cybersecurity legislation. As discussed previously, these variables were derived from the cybersecurity legislation dataset from the National Council of State Legislatures (NCSL). The NCSL database catalogs all bills proposed on cybersecurity legislation at the state level. The database is descriptive in nature, providing information on the details of the bills, their current status, and whether they have been enacted or failed due to various reasons, such as being vetoed by the governor. They data they use in most cases attributed to state, territory, and commonwealth websites which contain the full bill's language.

The first primary independent variable is the total cybersecurity legislation enacted during the time period, while the five others are based off the cybersecurity legislation trends discussed in detail in Chapter 4, election, breaches, insurance, crime, and training laws. I expect that the laws will have little effect until at least the following year so I have lagged all six of the primary independent variables by one year. The data used in the study includes 659 proposed bills from all 50 states, although some states did not propose any cybersecurity legislation. Of the proposed bills, 148 were enacted into law, while 511 bills failed to be enacted into law. The variable *enacted* is coded 1 if the bill was enacted and 0 if the bill failed. The data were then compiled by state and year, so in a single year a state could have multiple laws enacted. Each of these variables are cumulative to account for the fact that laws on the books should continue to affect ransomware attacks even past the first year after enactment.

There are limitations to coding the data using these keywords. First, some laws which should have been included in a category may have been missed if the NCSL's description did not include one of the keywords used in the search. This error could be because the description used a

synonym or other wording, but also could be that the NCSL did not use the same terms used in the actual law. A second limitation, is that the keywords could potentially include some laws which did not actually match the category. However, sorting by year and then alphabetically by state I reviewed the first 10 cases that one of the five variables was coded as '1' and the final 10 cases. This review constituted about 30% of the data and provided a wide mixture of the five variables and variety of states. All 20 cases reviewed were good matches for their respective categories. While both of these potential issues were concerns, this is a more methodical approach to coding the variables.

Control Variables

To account for other possible explanations, I include five control variables in the models. The first three variables come from The Council of State Governments' Book of the States database. The Book of the States is a collection of data on all fifty states that has been compiled since 1935. The models include two variables on the dominant political party in the state legislature and of the state governor. Capturing this political data is important as the literature provides some evidence that at the federal level Republicans tend to favor decentralized cybersecurity, while Democrats favor centralized cybersecurity (Kelly 2012). Further, Pylant (2020) finds that the centralized framework is more successful at the state level. Both legislature, who creates the laws, and the governor, who can approve or veto the laws, are important as many proposed laws were vetoed. To create the variable on the dominant party of the legislature, the overall percentage of Republicans in both the state house and senate was used as this captures the Democrats as well as they would be the inverse. Likewise, the governor's political party variable was coded as 1 for Republican and 0 for Democrat. Similar to the legislation variables, both of these variables were

lagged by a year as the effects of their decisions would likely not be relevant until the following year, but unlike the legislation variables there was data for 2014 which could be included.

The third variable, which was also derived from the Book of the States, is the estimated cybersecurity expenditure per state. This variable is important as the amount spent on cybersecurity should reflect what level of cybersecurity a state has. However, the data on cybersecurity expenditures is limited. The Book of the States includes data on total state expenditures per year, although 2019 was not included yet and was estimated by applying the average increase per state of the previous years to the total in 2018. According to some sources, the cybersecurity expenditure is roughly 2% of the IT budget (Robinson and Subramanian 2016), which is estimated at 2.5% of a state's overall budget (News Staff 2018).[30] Unfortunately, this estimation does not capture the true variations between states' cybersecurity budgets as some states may spend a larger or smaller percentage on cybersecurity. Yet this estimate does give an approximation that can help to control for the money spent on cybersecurity by states.

The final two control variables are population size and internet usage per household. Both variables are important as larger populated states and more technologically diffused states have more opportunity for attacks which needs to be controlled for. The population data was taken from the US Census website's "National Population Totals and Components of Change: 2010-2019" data set, while the number of households with internet data was obtained from the National Center for Education Statistics. The average population per state from 2010-2019 was used, as the most important factor was the variation between states. Similarly, the number of households with internet access was kept constant, but this was also due to availability of information as the only

[30] News Staff (2018) provides estimates for the IT budget for ten states in 2018. I used this information with the Book of the States data on total expenditures to determine that the ten states spent on average around 2.5% of their overall budget on IT.

year available was for 2016. I took the natural log of these variables to help adjust for the skew caused by states with substantially larger population and internet sizes.

Methodology and Results

To test my hypotheses I used a series of ordinary least squares (OLS) regression models. In each of the models, the dependent variable was the number of ransomware attacks per state per year. Each model utilized all of the control variables listed above, with only one of the primary independent variables on cybersecurity legislation per model. This design allowed me to test each cybersecurity legislation hypothesis independently to see how those laws affected the dependent variable. Then I include a seventh model which includes all five of the trends at once to control for any effect they may have on the other trends. I ran these seven models three separate ways. The first set of models was the base model which tested the hypotheses for the full 2015-2019 period. Table 5.1 shows the results of the first seven models. In the second and third models I changed the time period to focus in on the two distinct periods, the initial period from 2015-2018 and the final period in 2019 when ransomware attacks against state and local entities were in full bloom. Table 5.2 presents the results of the second series of models. The third set of models looks only to explain the variation in the dependent variable in 2019. This series of models is to account for the cumulative effect of similar types of laws as well as help to isolate the number of ransomware attacks which grew exponentially over the 2015-2019 time period. The result of the third set of models are found in Table 5.3. Finally, I present the results of running the 2019 models using a Poisson regression to help verify that the type of model used does not affect the results.

Table 5.1: OLS Models Regressing Cybersecurity Legislation Output on the Number of Ransomware Attacks per State from 2015-2019

Regression Results							
	Dependent variable:						
	n_ransom_attacks						
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
n_enacted_laws	0.185***						
	(0.054)						
n_insurance_laws		1.468***					1.334**
		(0.477)					(0.515)
n_training_laws			0.649***				0.230
			(0.211)				(0.295)
n_election_laws				0.959**			0.724
				(0.463)			(0.522)
n_crime_laws					0.467		0.323
					(0.314)		(0.338)
n_breach_laws						0.502	0.055
						(0.432)	(0.468)
population_avg_log	0.809	0.427	0.845	0.508	0.368	0.394	0.621
	(1.785)	(1.789)	(1.795)	(1.808)	(1.815)	(1.818)	(1.787)
internet_log	-0.354	-0.021	-0.455	-0.013	0.111	0.073	-0.221
	(1.778)	(1.782)	(1.790)	(1.800)	(1.808)	(1.811)	(1.783)
estimated_cybersecurity	0.012	0.019**	0.018**	0.015*	0.016*	0.017*	0.016*
	(0.009)	(0.009)	(0.009)	(0.009)	(0.009)	(0.009)	(0.009)
Republican_governor	0.014	-0.086	-0.012	-0.046	0.033	-0.026	-0.063
	(0.272)	(0.274)	(0.273)	(0.276)	(0.279)	(0.278)	(0.275)
Legislature_Rep	-0.076	-0.034	0.161	0.218	-0.030	0.137	-0.062
	(0.664)	(0.666)	(0.664)	(0.672)	(0.683)	(0.675)	(0.675)
Constant	-6.470*	-5.305	-5.750*	-6.690**	-6.250*	-6.166*	-5.474*
	(3.291)	(3.320)	(3.310)	(3.345)	(3.354)	(3.361)	(3.308)
Observations	250	250	250	250	250	250	250
R^2	0.204	0.197	0.196	0.180	0.173	0.170	0.221
Adjusted R^2	0.184	0.177	0.177	0.160	0.152	0.149	0.189
Residual Std. Error	1.821 (df = 243)	1.829 (df = 243)	1.829 (df = 243)	1.848 (df = 243)	1.856 (df = 243)	1.859 (df = 243)	1.816 (df = 239)
F Statistic	10.353*** (df = 6; 243)	9.916*** (df = 6; 243)	9.901*** (df = 6; 243)	8.877*** (df = 6; 243)	8.463*** (df = 6; 243)	8.292*** (df = 6; 243)	6.798*** (df = 10; 239)
Note:							*p<0.1; **p<0.05; ***p<0.01

Table 5.2: OLS Models Regressing Cybersecurity Legislation Output on the Number of Ransomware Attacks per State from 2015-2018

Regression Results							
	Dependent variable:						
	n_ransom_attacks						
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
n_enacted_laws	0.006						
	(0.062)						
n_insurance_laws		1.161**					1.254**
		(0.486)					(0.524)
n_training_laws			0.154				-0.112
			(0.225)				(0.285)
n_election_laws				N/A[31]			
n_crime_laws					0.068		0.148
					(0.306)		(0.343)
n_breach_laws						0.219	0.341
						(0.412)	(0.453)
population_avg_log	-0.877	-0.911	-0.836	-0.884	-0.891	-0.890	-0.972
	(1.304)	(1.284)	(1.303)	(1.300)	(1.303)	(1.302)	(1.297)
internet_log	1.172	1.178	1.114	1.179	1.187	1.174	1.236
	(1.298)	(1.278)	(1.298)	(1.293)	(1.297)	(1.295)	(1.293)
estimated_cybersecurity	0.010	0.011*	0.010	0.010	0.010	0.010	0.010
	(0.007)	(0.006)	(0.007)	(0.007)	(0.007)	(0.007)	(0.007)
Republican_governor	0.138	0.123	0.146	0.136	0.141	0.135	0.122
	(0.200)	(0.196)	(0.199)	(0.198)	(0.200)	(0.199)	(0.198)
Legislature_Rep	0.109	0.036	0.102	0.117	0.100	0.107	-0.013
	(0.491)	(0.480)	(0.486)	(0.484)	(0.492)	(0.486)	(0.491)
Constant	-2.595	-2.160	-2.431	-2.596	-2.601	-2.452	-2.031
	(2.423)	(2.395)	(2.432)	(2.417)	(2.423)	(2.437)	(2.429)
Observations	200	200	200	200	200	200	200
R^2	0.143	0.167	0.145	0.143	0.143	0.144	0.170
Adjusted R^2	0.116	0.141	0.118	0.121	0.116	0.117	0.131
Residual Std. Error	1.188 (df = 193)	1.171 (df = 193)	1.186 (df = 193)	1.185 (df = 194)	1.188 (df = 193)	1.187 (df = 193)	1.178 (df = 190)
F Statistic	5.356*** (df = 6; 193)	6.461*** (df = 6; 193)	5.445*** (df = 6; 193)	6.457*** (df = 5; 194)	5.363*** (df = 6; 193)	5.408*** (df = 6; 193)	4.329*** (df = 9; 190)
Note:			*p<0.1; **p<0.05; ***p<0.01				

[31] The election laws variable had no result for this time period because there were no election laws passed between 2015—2017.

The first series of models did not support the hypotheses, but did show a weakness in the data. Most independent variables were found to be statistically significant, but their relationship with ransomware attacks was positive, which is the opposite direction predicted. Enacted legislation, insurance legislation, training legislation, and the variable comprising all five cybersecurity legislation trends were found to be statistically significant at the 99% level. Election legislation and estimated cybersecurity expenditure were found to be statistically significant in some models at the 95% level, although estimated cybersecurity expenditure was found to be significant at the 90% level or not significant in some models. The adjusted r-squared value was between 0.149 to 0.184 in the various models, meaning the models were able to explain around 15-19% of the variation in the dependent variable. However, the variables were positively related with ransomware attacks, which is the opposite direction predicted.

There are certainly a variety of possible reasons that the model outcomes were opposite of the hypotheses. Certainly one factor is due to the limitations of the data. There were few attacks and few laws at the beginning of the short time period, which created a challenge for the legislation variables to explain both this early period and the later period which saw a much higher volume of attacks and more laws. This change was due to the sudden shift in the targets for ransomware attacks by the ransomware criminals from more indiscriminate attacks to more targeted attacks against state and local entities.

To investigate the relationship of the variables further, the second and third model took a more limited approach and only attempted to explain the variation in the number of ransomware attacks during two periods: the initial period from 2015-2018 and the final period in 2019. The initial period is the time when ransomware attacks were really only beginning to become more widespread against organizations as opposed to individual computer users. Ransomware only

achieved the level and method of encryption described by Young and Yung (1996) in 2013, only two years prior to this period. Thus, organizations were only beginning to realize the threat of ransomware and ransomware developers were only beginning to realize that organizations were now potentially lucrative targets. Further, during the 2015-2018 period, the shift from indiscriminate attacks to targeted attacks, and importantly targeted attacks against state and local government institutions, occurred. Thus, this period is one of both growth in ransomware attacks and growth in cybersecurity legislation. This legislation is in many ways reactionary during this period. It is reactionary to both ransomware and other cybersecurity threats, such as security breaches. Complicating modeling attempts, the reactionary nature is not dependent upon geography, meaning a state may enact laws based on another state or organization suffering an attack.

This second set of models can be found above in Table 5.2. Due the limitations described above, these estimates from these models are almost entirely not significant. The only primary independent variable that is statistically significant is insurance laws at the 95% level. This model also finds the estimated cybersecurity expenditure significant at the 90% level. Yet, both of these have a positive relationship with the number of ransomware attacks. Based on above analysis, this result appears to support the argument that this period was largely reactionary in that ransomware attacks increased the likelihood states would pass laws.

There is evidence that this reactionary, initial period begins to change in 2019 which had a much larger amount of attacks on state and local targets as ransomware criminals put them directly in their crosshairs. The results, found in Table 5.3, were mixed, but found some evidence that cybersecurity legislation may have a negative relationship with the number of ransomware attacks. The hypotheses H4, and H6 were supported, as the variables were statistically significant and had

a negative relationship to the number of ransomware attacks as predicted. The models with the enacted legislation variable (H6) and breach legislation variable (H4), and the seventh control model had adjusted r-squared values of 60.7%, 69.6%, and 67.1% respectively, which means they explain around two thirds of the variation in the dependent variable. The F statistic is statistically significant in all three models, meaning we can reject the null hypothesis for these models.

The total amount of enacted laws (H6) was found to be statistically significant at the 95% level, while the total amount of breach laws (H4) per state was statistically significant at the 99% level. The estimated cybersecurity expenditure was also significant at the 99% level, while the Republican governor variable was found to be significant in some models at the 90% level. All of these variables had negative relationships with ransomware attacks, which was expected, at least, with the legislation variables. However, the main hypothesis (H1) that training legislation would have a negative effect on ransomware attacks was inconclusive as there was no statistical significance for this variable.

In Table 5.4 I present the results of the 2019 models using a Poisson regression to verify that the choice of regression model does not alter the results. The results support the findings of the OLM models for 2019. While the coefficients for the variables are smaller, they remain negative and statistically significant for the same variables as in the OLM models for 2019. The enacted legislation variable (H6) remains statistically significant at the 95% level, while the total amount of breach laws (H4) per state was statistically significant at the 99% level. The estimated cybersecurity expenditure was also significant at the 95% and 99% level depending on the model, while the Republican governor variable was found to be significant in some models at the 90% and 95% level depending on the model. All of these variables had negative relationships with ransomware attacks, which was expected, at least, with the legislation variables.

Table 5.3: OLS Models Regressing Total Cybersecurity Legislation Output on the Number of Ransomware Attacks per State in 2019

Regression Results							
	Dependent variable:						
	n_ransom_attacks						
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
n_enacted_laws	-0.214**						
	(0.094)						
n_insurance_laws		-0.125					-0.166
		(0.816)					(0.758)
n_training_laws			-0.516				0.078
			(0.362)				(0.431)
n_election_laws				-0.487			-0.415
				(0.612)			(0.653)
n_crime_laws					-0.473		-0.285
					(0.506)		(0.475)
n_breach_laws						-2.933***	-2.889***
						(0.668)	(0.733)
population_avg	0.00000*	0.00000*	0.00000	0.00000*	0.00000*	0.00000**	0.00000**
	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)
internet	-0.00000	-0.00000	-0.00000	-0.00000	-0.00000	-0.00000	-0.00000
	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)
estimated_cybersecurity	-0.150***	-0.149***	-0.155***	-0.138***	-0.150***	-0.140***	-0.133***
	(0.041)	(0.044)	(0.043)	(0.045)	(0.043)	(0.036)	(0.041)
Republican_governor	-1.272*	-1.230	-1.195	-1.178	-1.415*	-1.288**	-1.291*
	(0.700)	(0.760)	(0.725)	(0.742)	(0.753)	(0.616)	(0.679)
Legislature_Rep	-1.369	-1.343	-1.774	-1.574	-1.073	-2.278	-2.149
	(1.612)	(1.720)	(1.691)	(1.713)	(1.720)	(1.433)	(1.576)
Constant	3.060***	2.789**	3.068***	2.884**	2.845**	3.371***	3.351***
	(1.048)	(1.124)	(1.093)	(1.099)	(1.094)	(0.927)	(0.997)
Observations	50	50	50	50	50	50	50
R^2	0.655	0.614	0.631	0.619	0.621	0.733	0.738
Adjusted R^2	0.607	0.560	0.580	0.566	0.569	0.696	0.671
Residual Std. Error	2.029 (df = 43)	2.148 (df = 43)	2.100 (df = 43)	2.133 (df = 43)	2.127 (df = 43)	1.786 (df = 43)	1.857 (df = 39)
F Statistic	13.634*** (df = 6; 43)	11.395*** (df = 6; 43)	12.260*** (df = 6; 43)	11.658*** (df = 6; 43)	11.761*** (df = 6; 43)	19.689*** (df = 6; 43)	11.009*** (df = 10; 39)
Note:	*p<0.1; **p<0.05; ***p<0.01						

Table 5.4: Poisson Models Regressing Total Cybersecurity Legislation Output on the Number of Ransomware Attacks per State in 2019

Regression Results							
	Dependent variable:						
	n_ransom_attacks						
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
n_enacted_laws	-0.088**						
	(0.034)						
n_insurance_laws		0.131					0.249
		(0.229)					(0.235)
n_training_laws			-0.175				-0.00001
			(0.112)				(0.139)
n_election_laws				-0.189			0.064
				(0.197)			(0.198)
n_crime_laws					-0.256		-0.187
					(0.173)		(0.186)
n_breach_laws						-0.726***	-0.766***
						(0.199)	(0.223)
population_avg	-0.00000	0.000	-0.00000	-0.00000	0.00000	-0.00000	-0.000
	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)
internet	0.00000	0.00000	0.00000*	0.00000	0.00000	0.00000	0.00000
	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)	(0.00000)
estimated_cybersecurity	-0.027***	-0.029***	-0.029***	-0.024***	-0.030***	-0.018**	-0.021**
	(0.007)	(0.007)	(0.007)	(0.009)	(0.007)	(0.008)	(0.009)
Republican_governor	-0.400*	-0.485**	-0.417**	-0.410*	-0.528**	-0.384*	-0.545**
	(0.209)	(0.224)	(0.209)	(0.212)	(0.214)	(0.215)	(0.238)
Legislature_Rep	-0.484	-0.464	-0.513	-0.475	-0.327	-0.525	-0.552
	(0.533)	(0.553)	(0.538)	(0.544)	(0.544)	(0.570)	(0.601)
Constant	1.040***	1.017***	1.014***	0.976***	1.016***	0.908***	1.040***
	(0.321)	(0.341)	(0.327)	(0.326)	(0.328)	(0.342)	(0.357)
Observations	50	50	50	50	50	50	50
Log Likelihood	-94.367	-98.221	-97.072	-97.883	-97.150	-91.328	-89.958
Akaike Inf. Crit.	202.734	210.442	208.144	209.765	208.301	196.656	201.915
Note:				*p<0.1; **p<0.05; ***p<0.01			

Analysis

The results of the models are mixed. This section will focus on analyzing and explaining these results. First, I briefly address the original models, which attempted to describe the variation of the dependent variable during the entire period of 2015-2019 and then in the initial period of 2015-2018. I address why these models do not support the hypotheses. In part this was due to data limitations and the sudden rise in ransomware attacks against state and local institutions. Then I move on to the third model explain the results. I address why breach laws are significant, while training laws are not supported by the model. I also discuss the other findings.

The first two series of models attempted to explain the variation in the dependent variable over the 2015-2019 period and the initial period of 2015-2018. In both sets of models the variables which were found to be statistically significant were also positively correlated with ransomware attacks. The positive relationship was likely a reflection of the short time period with limited attacks and legislation at the onset of the study period, but then a drastic increase at the end of the period. As described above, the initial period was largely reactionary, as states began to develop cybersecurity legislation in response to the rapidly emerging threat from ransomware and other cybersecurity threats. Further, it was a period which saw great changes in the tactics and targets chosen by ransomware criminals. In 2015 there were only five cybersecurity laws passed throughout the fifty states. To explain ransomware attack variation in the first few years of the study period, we would need data on legislation going back further, which was not readily available for this study. As time went on, states enacted more laws, but then ransomware attacks rose so suddenly and dramatically that the total attacks almost doubled just in 2019. This sudden change is due to a shift in targets from more indiscriminate attacks to targeting specific sectors or entities, such as state and local governments.

Another potential reason for the mixed results is the level of implementation or enforcement of the legislation. The data from the NCSL on legislation provides the type of legislation and the amount of enacted legislation. However, there is no measure of the implementation or enforcement of the legislation in the models. A law that has been enacted but has not enforcement mechanisms or is simply disregarded would not be expected to have any effect on the number of ransomware attacks. There is literature which stresses the importance of implementation and enforcement. Sutherland (2017) finds that South Africa has adopted important cybersecurity polices, such as a National Cybersecurity Policy Framework, but the legislation is "being implemented only slowly, with very limited reporting and Parliamentary oversight" (Sutherland 2017). In other words, South Africa has enacted sufficient cybersecurity laws, but is still behind in cybersecurity due to poor enforcement. This poor implementation and enforcement could also be occurring amongst the 50 states included in this study. Unfortunately, there was no readily available measure of enforcement or implementation of the legislation used in this study, which potentially affected the results.

To investigate the relationship between the variables further, I setup a third series of models which focused in on 2019, the year with the most attacks. These models also used the cumulative total per state for each legislation variable for the 2015-2018 time period, which allowed the difference in attacks between states that had enacted cybersecurity legislation and those that had not to be seen more clearly. The results are mixed, but the models provide some evidence in support of two of the hypotheses. One of the models supports the hypothesis that total enacted cybersecurity legislation per state reduces the number of ransomware attacks per state. Based on the results, for every five pieces of enacted legislation a state can expect to reduce the number of ransomware attacks by one. However, the relationship between the number of enacted

cybersecurity laws and ransomware is not clear from the model. It is possible that states that pass more cybersecurity laws are more focused on cybersecurity and therefore have increased cybersecurity measures in place. More research is needed to determine how cybersecurity legislation may effect a state's cybersecurity.

One potential avenue for further investigation are breach laws, which also had a statistically significant, negative relationship with the number of ransomware attacks in 2019. For every additional breach law, a state had almost three less ransomware attacks. Yet, training laws, which the literature suggested would be most effective in preventing ransomware attacks, was not found to be statistically significant. Why were breach laws significant, but not training laws? Interestingly, the two variables actually had a fair amount of overlap in legislation. Of the ten breach laws, three of them were also included in the training variable: Illinois H.B. 2371 in 2017, Michigan H.B. 4323 in 2017, and Florida H.B. 1033 in 2016. These laws required both training and that state entities prevent breaches. The other training legislation is mostly on education and workforce development, such as through scholarships. While important, these are long term programs whose effects would not likely manifest until at least four years later, which is the typical length of a bachelor's degree.

On the other hand, the breach laws continue to focus on breach prevention and require entities to report or disclose breaches. These types of laws place the ownership into the subject of the law's hands. Moore (2010) argued that one reason cybersecurity is not prioritized is due to misaligned incentives. Costs of failed cybersecurity often do not fully fall on the organization that failed. Instead, these costs are spread out amongst other actors, but primarily society as a whole (Moore 2010). The breach legislation helps to correct this by holding the entity responsible to prevent breaches and disclose any breaches. This corrects the misaligned incentives by placing the

costs back on the organization that failed. The incentive to avoid these costs push these entities to employ better cybersecurity measures, which would certainly include training, up to date antivirus software, and good cyber hygiene. Thus, by holding organizations responsible these breach laws cause them to raise their cybersecurity standards.

Interestingly, some of these models found that states with Republican led governors had less ransomware attacks. A Republican governor would reduce the number of ransomware attacks by just over one. This finding is contrary to the expectation, as at the federal level Republicans favored a decentralized framework (Kelly 2012), which Pylant (2020) found to be less effective than a centralized framework at the state level. It could be that at the state level Republicans have different preferences, but if they do favor a decentralized framework then this finding could challenge Pylant (2020). More research on these topics is certainly needed.

While the results of the models are mixed, this dissertation is still an important first step in pulling together data on cybersecurity legislation and ransomware attacks. The study certainly has not resolved the issue of ransomware, but has opened up numerous avenues for potential future research. Some of these will be discussed in more detail in the final chapter, but first the next chapter will explore the relationship between breach laws and ransomware further.

CHAPTER VI

CASE STUDY: BREACHES LEGISLATION

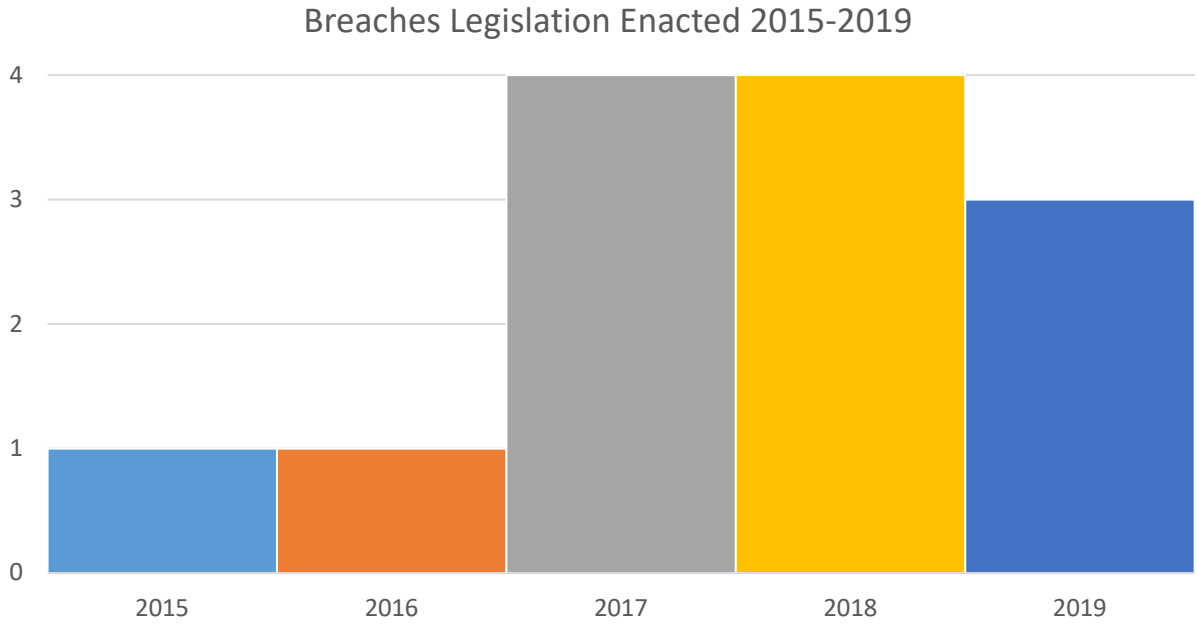
The results in the last chapter found support for the hypothesis (H4) that state legislation on cybersecurity breaches is negatively associated with the likelihood that the state experiences a ransomware attack. In this chapter I explore state legislation on cybersecurity breaches in more detail to further explore this relationship. First I briefly re-summarize the theoretical reasons that breaches legislation is negatively associated with the number of ransomware attacks. Second, I discuss the California's cybersecurity breach laws in more detail, as California has long been a leader in this area of cybersecurity legislation. Finally, I examine how California's laws have enacted change that further supports the outcome of the model.

Theoretical Underpinnings of Breaches Legislation

As discussed in Chapter 2, data breaches are attacks by cybercriminals on government or business networks to steal data containing personal information or proprietary information to use or sell on the black market. These attacks differ from hacking of an individual user because they involve the theft of mass amounts of personal or proprietary data that is being stored by a third party, such as a government or business organization. Breaches can occur through hacking, phishing, theft, inside jobs, or negligence. While data breaches have occurred for some time, the most significant ones began occurring since 2005 as most companies had converted to electronic records by that time. For example, Target had 70 million records compromised in 2013, and Yahoo had one billion records compromised in 2016 (De Groot 2019).

To address this serious cyber issue states have enacted legislation requiring companies to provide reasonable protection of personal data and requiring organizations to disclose breaches to the parties. There were a total of thirteen of these laws enacted in the study period. As seen in Figure 6.1, one law was passed in 2015 and 2016, then four were passed in 2017 and 2018, and finally three more were passed in 2019. California and Florida passed the most breach related laws with two each. The remaining laws were spread out amongst Arizona, Arkansas, Delaware, Illinois, Michigan, Nebraska, New Hampshire, North Carolina, and Virginia each passing one law. These laws address concerns over the storage of voter or consumer credit information, disclosing breaches of voter or consumer credit information, and yearly reviews of breaches to address any weakness in cybersecurity measures to prevent future breaches (NCSL 2020).

Figure 6.1: Breaches Legislation Enacted 2015-2019



Data Source: NCSL, "Cybersecurity Legislation 2019," *NCSL* [data file], 2020, accessed August 15, 2020, retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

These laws may be effective tools to encourage better cybersecurity and prevent future cyberattacks, such as ransomware, because they shift the costs of a cybersecurity failure back onto the organization that failed. Moore (2010) argued that one reason cybersecurity is not prioritized is due to misaligned incentives. Costs of failed cybersecurity often do not fully fall on the organization that failed. Instead, these costs are spread out amongst other actors, but primarily society as a whole (Moore 2010). The breach legislation helps to correct this by holding the entity accountable to prevent breaches and disclose any breaches. This corrects the misaligned incentives by placing the costs, such as monetary through payments for damages caused and reputational through the bad publicity resulting from a breach, back on the organization that failed. The incentive to avoid these costs push these entities to employ better cybersecurity measures, which would certainly include training, up to date antivirus software, and good cyber hygiene. Thus, by holding organizations responsible these breach laws can cause them to raise their cybersecurity standards.

California's Breaches Legislation

California has been a leader in cybersecurity breach legislation and as a leader should be examined in more detail to better understand how these laws might improve cybersecurity, especially against ransomware. As previously mentioned in the history on cybersecurity legislation, California was ahead of the curve on requiring companies to disclose security breaches that affected personal information of Californians. In 2003 California passed the Notice of Security Breach Act to address these concerns and "punish firms for cyber security failures" (Singh 2016). This law was passed prior to the rise of more severe cybersecurity breeches starting around 2004 to 2005.

During the 2015-2019 time period, California appears to be continuing to lead the pack on this issue. The two newest laws, Assembly Bill No. 1678, Chapter 96 (AB 1678) and Assembly Bill No. 1859, Chapter 532 (AB 1859), add to the code on security breaches by explicitly stating that entities holding voter registrations information and consumer credit report information must maintain adequate security and disclose any breaches (NCSL 2020). AB 1678 empowers the Secretary of State for California to "adopt regulations that describe the best practices for storage and security of voter registration information received by an applicant" (California 2018). In other words, any entities taking or storing voter registration information will have instructions and requirements from the state on how best to secure this data. This aspect of the law should increase cybersecurity by establishing minimum standards that must be met by organizations holding this information. AB 1678 also requires that entities that take or hold voter registration data, "shall, following discovery or notification of a breach in the security of the storage of the information, disclose the breach in security to the Secretary of State. The disclosure shall be made in the most expedient time possible and without unreasonable delay" (California 2018). This requirement holds these entities responsible by requiring they disclose breaches. This part of the law should increase cybersecurity by transferring some of the costs of a cybersecurity failure back on the entity responsible for protecting that information. The law's weakness is that it only affects entities that receive or hold voter data and it does not prescribe any specific penalties or sanctions on entities that fail to properly secure data.

On the other hand, AB 1859 focuses on consumer credit reporting agencies. This law builds on existing California law, which already requires consumer credit reporting agencies to adopt reasonable cybersecurity measures to protect consumers' data. AB 1859 makes the law more specific by requiring the entities to implement software updates that address security

vulnerabilities in a timely manner and to take "reasonable compensating controls to reduce the risk of a breach caused by computer system vulnerability until the software update is complete […]" (California 2018). Further, the law holds these entities responsible for addressing these vulnerabilities whether the entity knows of the vulnerability or "reasonably should know" (California 2018). In other words, these companies must employ good cyber hygiene as they are required to promptly update and secure any vulnerabilities that become known. Promoting good cyber hygiene should enhance cybersecurity by reducing the ability for attackers to use known vulnerabilities.

Results of Breaches Legislation

California has developed laws to address security breaches, which match up with suggestions from cybersecurity experts, such as encouraging good cyber hygiene. While the state has been a leader in this area since 2003, finding direct evidence of any one of the state's laws is difficult as there have been few studies on the results of these laws. However, one way we can examine this effect is through a counterfactual. This section will first look at cybersecurity legislation through a counterfactual and then look at a new law passed in California that has wide-reaching effects.

First we should imagine what the world would look like if the legislation on cybersecurity, in particular breaches, did not exist. Would there be more ransomware attacks? It is difficult to know for certain, but the research presented in the previous chapters suggests there likely would be more ransomware attacks. Organizations, including state and local governments, have historically tended to not focus resources on cybersecurity. According to some sources, the cybersecurity expenditure is roughly 2% of the IT budget (Robinson and Subramanian 2016). Moore (2010) attributes this lack of attention to cybersecurity to a misalignment of incentives. For

example, when a data breach occurs often the data compromised is personal identifiable information an organization was storing on its customers. This information is often then sold on the dark web and used in identity theft crimes. Yet, if one or more of an organization's customer's identies were stolen there is very little, if any cost to the organization, but a potentially great cost to the customer. Thus, without outside incentive an organization has less concern for certain aspects of cybersecurity because there is virtually no cost for cybersecurity failure. These outside incentives come from cybersecurity legislation.

One important piece of legislation addressing these misaligned incentives is the California Consumer Privacy Act of 2018. This law was passed by California in 2018 and has disrupted the status quo enough to have a flurry of articles written on how companies must adapt to these new conditions. Below I examine this law in more detail, but first I touch on why it was not included in the NCSL database and, therefore, this study. Then I discuss the effects of the law to see how it is promoting increased cybersecurity both in California and around the globe.

The California Consumer Privacy Act of 2018 or Assembly Bill No. 375, Chapter 55, was passed in 2018. The law's focus is on the protection of California citizen's privacy and gives back ownership of an individual's data to the individual. Previously, companies have largely been able to obtain and sell consumer's data, which includes personal information, especially important marketing factors, without informing the consumer or providing any means for the consumer to opt out. The law gives power back to the consumer by requiring businesses to disclose what personal information is collected, the purpose for collecting it, and what types of third parties this data is shared with. Further, the law allows consumers to be allowed to opt out and request their personal information be deleted (California 2018).

The focus of this law is clearly on privacy, which is most likely the reason it was missed by the NCSL and not included in their database of cybersecurity legislation. However, the law also has provisions that would meet the definition of a breach law if it was in this study. First, the law requires that companies provide reasonable protection of personal information. Second, it requires that if the entity holding the personal information suffers a security breach, then it must disclose the breach. The law even includes penalties for failure up to $7,500 per incident (California 2018). Thus, the law would have been included in this study had it been in the NCSL database.

Since this law was not included there are certainly some implications for the model. First, while the NCSL provides a comprehensive database, the lack of inclusion of this law shows that at least one law was missed. There certainly could be additional laws which were not included that should have been. However, given the NCSL's close relationship with state legislatures, I believe the likelihood of substantial missing data is low. Second, the lack of this law could potentially skew the results of the models as this law has certainly had an effect on organizations. However, this effect should be minimal as the focus of this law is on businesses, but this dissertation focuses on ransomware attacks against state and local government institutions.

While the law was passed in California, it is affecting businesses throughout the United States and the world. Hildebrand, et al. (2020) explain, "In contrast to most United States data protection laws, which apply only to certain industries, the CCPA regulates organizations in any industry that meet the statutory requirements." Further, the law defines business broadly and includes companies that "Buys, sells, or receives for the business's commercial purposes the personal information of 50,000 or more California consumers, households, or devices per year" (Hildebrand, et al. 2020). In other words, a company does not need to be based or even do direct business in California. If a business buys, sells or receives personal information on California

residents or even their devices, such as cell phones, then it would be potentially subject to this law and its statutes.

Due to this widespread effect, companies throughout the world have had to take action. California did give companies time to take appropriate action. While the law was passed in 2018, it did not go into effect until January 1, 2020. This law has set off a flurry of articles from lawyers (Del Pizzo 2018), investors (Hildebrand 2020), and cybersecurity companies (De Groot 2020) on how companies should prepare to be in compliance with this law. Thus, the law has put the responsibility of cybersecurity on these companies and they are now taking it upon themselves to make sure they are in compliance by, among other things, ensuring their cybersecurity is up to California's standards.

CHAPTER VII

CONCLUSION

This dissertation focused on the effectiveness of state cybersecurity legislation at preventing the recently emerged threat of ransomware attacks. The results of the models are mixed. The initial models suggest that cybersecurity legislation may be reactionary. However, the models estimated using the 2019 subset of the sample provide some evidence that states which have taken more preventative measures through cybersecurity legislation, especially focused on security breaches, tend to experience fewer ransomware attacks. This chapter explores these findings further to offer policy recommendations. First, I summarize the dissertation's findings. Then, I discuss potential policy recommendations. Finally, I conclude with some final considerations and suggestions on future research based off these findings.

Summary of Findings

Ransomware has rapidly emerged as a major cybersecurity threat to state and local governments. From towns, like Colonie, to large cities, such as Baltimore, ransomware attacks have caused temporary loss of critical services, damages, time and resource consuming recovery efforts, and tarnished reputations. Ransomware was there at the onset of the spread of the Internet, but did not become a true threat until around 2013 with the development of the first true cryptoviral strains of ransomware. Since then, ransomware has become more advanced and targeted allowing criminals to increase ransom demands from a few hundred dollars to tens or even hundreds of thousands of dollars. The costs of these attacks have exploded from $325 million in 2015 (Morgan 2018) to more than $7.5 billion in 2019 in the United States (Emsisoft 2020). States have had little

time to prepare, especially as the target of these attacks shifted suddenly towards them in 2019. However, during this same time period many states were actively working towards better cybersecurity through various laws. The goal of this dissertation was to assess the effectiveness of these laws at preventing ransomware attacks to help policy makers' future efforts to counter this grave threat.

The previous literature was reviewed to see what previous research had found to answer this question. Overall, the field on cybersecurity legislation is immature, but there have been some notable contributions. Kelly (2012), Newmeyer (2012), Rosner (2017), Blomquist (2020), and Pylant (2020) debate if centralized, decentralized, or a hybrid cybersecurity framework is the best approach. While Hathaway (2013), Hathaway, et al. (2015), Spidareli (2015), and Rosner (2017), attempt to assess the effectiveness of cybersecurity legislation through qualitative measures. The literature lacks quantitative studies on cybersecurity effectiveness. Pylant (2020) helps to start to fill this gap by using quantitative analysis in assessing cybersecurity legislation based on states utilization of National Institute of Standards and Technology's (NIST) five key functions. Still through this research no previous studies were found that quantitatively examined the effectiveness of cybersecurity legislation at actually reducing cyber-attacks.

This dissertation set to fill this gap in the literature. I compared the state cybersecurity legislation from the National Conference of State Legislatures (NCSL) that was passed from 2015-2019 with data on the number of ransomware attacks per state from 2015-2019 from Freed (2019). There were five trends of legislation, including laws on training and security breaches, in the NCSL database. The literature suggested that legislation that increased training, up to date anti-virus software, and good cyber hygiene would be most successful at preventing ransomware attacks (Savage, et al. 2015; Pope 2016). I used a regression model to analyze their relationship

statistically. These models provide mixed evidence that states that enacted more cybersecurity laws suffered less ransomware attacks. However, analysis represents an important first step in pulling together data on cybersecurity legislation and ransomware attacks. The results revealed multiple avenues for future research.

For example, the model suggested that laws on cybersecurity breaches had a negative relationship with ransomware attacks. Based on these results, I reviewed this relationship in more detail. The literature suggests the success of these laws in preventing ransomware attacks can be attributed to the accountability and ownership required in the laws. The security breach laws focus on preparing for potential security breaches and requiring entities to disclose breaches within a certain time period. The key is that these laws allow the subjects of the law to develop their own cybersecurity while placing the ownership with these organizations and holding them accountable for their failures. This accountability changes the cost benefit analysis of the subjects, which without legislation is likely to hold cybersecurity lower as the costs of failure are not fully absorbed by the organization (Moore 2010). Thus, these laws change the "misaligned incentives" (Moore 2010) or the cost benefit analysis of these organizations by increasing the costs of cybersecurity failure. With higher costs for cybersecurity failure, these organizations then are incentivized to invest in cybersecurity initiatives, such as training, up to date anti-virus programs, and good cyber hygiene, themselves.

Policy Recommendations

As states and local leaders continue to adjust to the rapidly emerging threat of ransomware, it is important to provide them with any insights that could help them to develop the most effective policies to combat this threat. The previous literature on cybersecurity legislation generally does

not offer particular policy prescriptions, but does provide guidance on the types of policies which should be enacted. Yang, et al. (2020) find information sharing can increase an organization's cybersecurity investment. While Pylant (2020) argues that states should take a centralized approach to best provide the NIST's five key functions, "identify, protect, detect, respond, and recover."

Yet, one exception comes with Spidalieri (2015), who adapted Hathaway's (2013) cybersecurity criteria for nations to be used to assess states. Spidalieri (2015) provides major categories, such as cybersecurity strategic plan and incident response, based on Hathaway (2013), but further breaks down each category into more specific qualities that make effective cyber readiness. Similar to Pylant (2020), she recommends states adhere to the NIST framework. She also argues it is necessary to have competent authority, regular threat assessment, and good cyber hygiene (Spidalieri 2015). Still she does not prioritize these actions and her focus was on cybersecurity in general, not only on preventing ransomware.

To prepare for ransomware attacks, cybersecurity experts argue that there are three aspects which need to be addressed: prevention, mitigation, and recovery (Savage, et al. 2015; Pope 2016; Salvi and Kerkar 2016; Sittig and Singh 2016; Richardson and North 2017; Nadir and Bakhshi 2018; KnowBe4 2020). Due in part to data limitations, this dissertation focused on prevention, which aims to stop ransomware attacks before they cause damage. Methods of prevention include training, up to date antivirus programs, and good cyber hygiene (Savage, et al. 2015; Pope 2016). However, the cybersecurity literature agrees that no prevention strategy is invulnerable, so mitigation and recovery need to be planned for as well. These strategies should, among other things, include having secure offline backups (Pope 2016; Salvi and Kerkar 2016; Sittig and Singh

2016; Nadir and Bakhshi 2018; KnowBe4 2020) which can both mitigate an attack by reducing the amount of damage caused and provide a relatively quick recovery solution.

Now these specific aspects of cybersecurity defense have been thoroughly prescribed by cybersecurity experts and scholars previously, but legislators need to know the best way to transfer these recommendations into effective policy. This dissertation assessed state cybersecurity legislation effects on the number of ransomware attacks. Some of the regression models provide evidence that cybersecurity breach legislation have a negative relationship with the number of ransomware attacks. One possible reason for this decrease is that these laws have increased the accountability and ownership of the subjects of the laws, which changed their cost benefit analysis incentivizing them to invest in cybersecurity or face consequences for cybersecurity failures (Moore 2010). These laws left the actual cybersecurity decisions in the hands of the organizations, who surely engaged with cybersecurity experts.

The research presented here suggests that states should focus on laws which promote organizations to enhance their cybersecurity autonomously by making the cost cybersecurity failures to be carried by the organization as opposed to society. Legislators should enact laws which directly focus on this promotion, similar to the security breach laws which were implemented in this study period. These laws would require that organizations are responsible for the security of the data that they retain and enact penalties for failure to properly secure data. This would push organizations to enhance their cybersecurity to avoid the penalties. These companies would then turn to cybersecurity experts who would likely recommend training, up to date antivirus programs, and good cyber hygiene (Savage, et al. 2015; Pope 2016), which should reduce the impact of ransomware.

In addition to direct measures, indirect legislation that encourages adoption of cybersecurity insurance could also accomplish similar goals. As hinted at earlier in this study, the relationship between ransomware and insurance is complex. Ransomware and insurance have inadvertently entered into a symbiotic relationship. Due to increased ransomware attacks more organizations are buying cybersecurity insurance, but because insurance often suggests paying the ransom to avoid costly recovery, they make ransomware profitable leading to more ransomware attacks (Dudley 2019). Despite these complexities, cybersecurity insurance should better prepare organizations. The underwriting process to obtain insurance helps organizations identify cybersecurity weaknesses and best practices. The insurance company wants to limit its risk and will either make an organization with poor cybersecurity pay more in premium for insurance or even refuse to write a policy for the organization until they improve their cybersecurity (Nakashima 2015). However, within this study the model did not support that laws on insurance had an effect on ransomware attacks. Yet, most of these laws focused on regulations of the insurers, to make sure that they are properly securing their data, which means they would have little effect on the number of ransomware attacks in this study because only state and local institutions were included in the data. Thus, there is still reason to believe that, similar to the more direct legislation of the security breach legislation, encouraging the adoption of cybersecurity insurance would increase organization's cybersecurity. Certainly more research is needed on the effect of cybersecurity insurance legislation on cybersecurity.

While these two methods address cybersecurity in the near term, long term policy solutions should still be considered. In particular, training, education, and workforce development should be given serious consideration as long term policy prescriptions. While the variable, training legislation, which encompassed these methods was not found to have a statistically significant

effect, it was most likely due to the timeframe that these programs need to be effective. These types of programs include scholarships for cybersecurity degrees with requirements to work for the state or local institution for a certain amount of time upon completion of the degree. The benefit of these types of programs is that it addresses the lack of talented labor in many areas and due to the fact that private sector jobs can offer much higher pay (Robinson and Subramanian 2016). Given the long timeframe for these types of programs to become effective, these types of laws should still be considered now to help improve cybersecurity in the long term.

These three policy prescriptions will help states and local institutions to be more effective at preventing ransomware attacks. Of course, the additional measures to mitigate and recover from attacks are still critical to an overall strategy. In the end, the cybersecurity professionals should be entrusted and given the tools needed to implement multifaceted cybersecurity strategies. To help ensure organizations provide the level of focus needed for effective cybersecurity, states should enact laws which require organizations to protect their data and systems and punish them for failures. States should also consider laws which encourage cybersecurity insurance, which can help to accomplish the similar goals. Finally, to plan for long term cybersecurity, states should also consider laws which provide training, education, and workforce development.

Final Considerations

More state and local institutions will find their agency or city taken hostage by anonymous ransomware criminals unless effective policies are adopted which can help prevent these crippling attacks from occurring. This dissertation explored the cybersecurity legislation passed from 2015-2019. The results of the study were mixed, with models of the initial period suggesting cybersecurity legislation was reactionary during the 2015-2018 time period. The final models

focused on the number of ransomware attacks in 2019 and provided some support that cybersecurity legislation, and in particular security breach laws, may be negatively associated with the number of ransomware attacks. Thus, while the results of the models were mixed this dissertation was an important step in exploring the relationship between cybersecurity legislation and ransomware attacks.

This dissertation filled a hole in the literature by providing the first assessment of the effectiveness of cybersecurity legislation at preventing ransomware attacks. However, much more research on cybersecurity legislation is needed as the field is still developing. There are many potential avenues for additional research, but the results from the model found a few promising opportunities.

First, one of the limits of this dissertation was that the readily accessible data on cybersecurity legislation did not begin until 2015. From the review of cybersecurity legislation history, we know that California was the first state to enact its own cybersecurity legislation back in 2003. Cybersecurity legislation from prior to 2015 could help to better explain the number of ransomware attacks from 2015-2018. In addition, the model does not address implementation or enforcement of the laws. Thus, future research should focus on compiling data on the cybersecurity legislation passed prior to 2015 and including a measure of implementation and enforcement into the model.

Second, another potential research path would be to perform a deeper examination of state training laws. As mentioned above, state cybersecurity legislation existed prior to the 2015 time period. Many states have had cybersecurity training laws but many are voluntary. It would be interesting to see if states with mandatory training were more effective at reducing ransomware

attacks. If mandatory training is more effective, this would certainly be an important finding for legislators to consider in future laws.

Third, this dissertation investigated the theoretical ties between legislation on breaches and increased cybersecurity by organizations. The breach laws often state that organizations, such as businesses or government institutions, are responsible for reasonable measures to protect certain kinds of data. The laws theoretically accomplish this by requiring breaches to be reported to both a state government official and to the affected parties, which places some of the costs of a breach back on to the organization due to potential reputation costs. However, the link between the legislation and how the organizations have actually responded has not been fully investigated. Future research could focus on what changes organizations have actually made as a result of these laws. This research could be similar to Yang, et al. (2020) which studied the effects of the Cybersecurity Information Sharing Act (CISA) of 2015 publicly traded companies' cybersecurity investment. However, that study's focus left out how smaller businesses or other organizations reacted to that law. To broaden the implications future research could perform interviews of varying organizations to see what changes they made as a result of a particular cybersecurity law.

Finally, some of the models found support that having a Republican governor had a negative effect on ransomware attacks. However, political party was not a focus of this dissertation. More research is needed to better understand the relationship between political party and cybersecurity. As stated previously, there was some evidence that suggested Republicans at the federal level favored a decentralized approach to cybersecurity (Kelly 2012). Yet, Pylant (2020) argued that centralized or hybrid approaches were more effective for cybersecurity at the state level. Thus, additional research should also focus on if political parties are more likely to support centralized, decentralized, or hybrid approaches. This research could add to one of the

central debates in the cybersecurity legislation field by potentially supporting or challenging the previous studies.

Additional research on this topic is needed now as cybercriminals have not hesitated in their development of ransomware. Legislators need the best information to craft effective policies to combat this growing threat. States who continue to fail to take action on cybersecurity and ransomware should not be surprised if their agencies or cities are taken hostage.

WORKS CITED

Acharya, Arabinda and Amrit P. Acharya. “Internet of Things, Ransomware and Terrorism,” *Journal of Defense Management*, (2017)

Alexander, Adam, et al. “An Analysis of Cybersecurity Legislation and Policy Creation on the State Level.” *National Cyber Summit (NCS) Research Track*, edited by Kim-Kwang Raymond Choo et al., vol. 1055, Spring Nature, 2020, pp. 30–43. AISC.

Alexander, George. "The emergence of cybercrime and the legal response." *Journal of Security Education*, vol. 2, no. 2, 2007, 47-79.

Alintanahin, Kervin. “CryptoLocker: Its Spam and ZeuS/ZBOT Connection.” *TrendLabs Security Intelligence Blog*, 21 Oct. 2013, blog.trendmicro.com/trendlabs-security-intelligence/cryptolocker-its-spam-and-zeuszbot-connection/?_ga=2.22832575.562796642.1598838204-311834091.1598646088.

Althobaiti, Kholoud, Ghaidaa Rummani, and Kami Vaniea. "A Review of Human-and Computer-Facing URL Phishing Features." *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019.

Armerding, Taylor. “Obamas Cybersecurity Legacy: Good Intentions, Good Efforts, Limited Results.” *CSO Online*, CSO, 31 Jan. 2017, www.csoonline.com/article/3162844/obamas-cybersecurity-legacy-good-intentions-good-efforts-limited-results.html.

Arrigo, Michael F. “HIPAA and HITECH Act Serve as Cybersecurity Standards for Healthcare.” *No World Borders*, 19 Dec. 2019, noworldborders.com/2019/12/18/hipaa-and-hitech-act-serve-as-cybersecurity-standards-for-healthcare/ .

Bailey, Liam M. D. “Mitigating Moral Hazard in Cyber-Risk Insurance.” *Journal of Law & Cyber Warfare*, vol. 3, no. 1, 2014, pp. 1–42. *JSTOR*, www.jstor.org/stable/26432557. Accessed 30 Jan. 2021.

Bain, Ben. “Obama Unveils New Cybersecurity Strategy.” *FCW*, 29 May 2009, fcw.com/articles/2009/05/29/web-obama-cyber-czar-strategy-speech.aspx.

Bajak, Frank and Ricardo Alonso-Zaldivar. “Suspected Ransomware Attack Hobbles Major Hospital Chain’s U.S. Facilities.” *PBS NewsHour*, 29 Sept. 2020, www.pbs.org/newshour/nation/suspected-ransomware-attack-hobbles-major-hospital-chains-u-s-facilities.

Barlow, John Perry. “A Declaration of the Independence of Cyberspace.” *Electronic Frontier Foundation*, 8 Feb. 1996, www.eff.org/cyberspace-independence.

Blannin, Patrick. “Islamic State’s Financing: Sources, Methods and Utilisation,” *Counter Terrorist Trends and Analyses*, Vol. 9, No. 5 (May 2018) pg 13-22.

Blomquist, David Michael. “Comparing Centralized and Decentralized Cybersecurity in State and Local Government.” *ProQuest Dissertations Publishing*, May 2020.

Bond, Michaelle. “1 In 4 Local Governments Will Fall to Ransomware, Experts Say.” *Government Technology State & Local Articles - E.Republic*, 9 Sept. 2019, www.govtech.com/security/1-in-4-Local-Governments-Will-Fall-to-Ransomware-Experts-Say.html.

“Book of the States.” *Book of the States | CSG Knowledge Center*, 2020, knowledgecenter.csg.org/kc/category/content-type/content-type/book-states.

Boutin, Jean-Ian. “The Evolution of Webinjects.” *Virus Bulletin Conference*, 2014, pp. 25–34.

Brito, Jerry, and Tate Watkins. "Loving the cyber bomb-the dangers of threat inflation in cybersecurity policy." *Harv. Nat'l Sec. J.* 3 (2011): 39.

California, Senate, House. “Bill Text - AB- 375 Privacy: Personal Information: Businesses.” *California Legislative Information*, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

California, Senate, House. “Bill Text - AB-1678 Elections: Voter Registration Information: Security: Campaign Literature and Communications.” *California Legislative Information*, 2018, leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB1678.

California, Senate, House. “Bill Text - AB-1859 Customer Records.” *California Legislative Information*, 2018, leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB1859.

Carbonite. “Case Study: Server Backup Town of Colonie.” *The ChannelPro Network*, 1 June 2020, www.channelpronetwork.com/download/white-paper/case-study-server-backup-town-colonie.

Cartwright, Edward, et al. “To Pay or Not: Game Theoretic Models of Ransomware.” *Journal of Cybersecurity*, vol. 5, no. 1, 2019, pp. 1–12., doi:10.1093/cybsec/tyz009.

Center for Digital Government. “Cybersecurity Modernization: How Agencies Can Transform Government While Controlling Business Risk.” *Dell EMC*, Dell EMC, 2018, www.dellemc.com/sq-al/collaterals/unauth/white-papers/solutions/cdg18_whitepaper_dell_emc_cybersecurity.pdf.

Check Point Software Technologies, LTD. “Prevent Cyber Attacks with 5th Gen Security Architecture.” *Prevent Cyber Attacks with 5th Gen Security Architecture | Check Point Software Technologies*, 2020, pages.checkpoint.com/checkpoint-infinity.html.

Chokshi, Niraj. “Hackers Are Holding Baltimore Hostage: How They Struck and What's Next.” *The New York Times*, The New York Times, 22 May 2019, www.nytimes.com/2019/05/22/us/baltimore-ransomware.html.

Chung, Marcus. “Ransomware Terrorism: Should We Be Worried?” *Security Boulevard*, 4 Mar. 2020, securityboulevard.com/2019/05/ransomware-terrorism-should-we-be-worried/.

CISA. “Cybersecurity Insurance.” *Cybersecurity and Infrastructure Security Agency CISA*, 2020, www.cisa.gov/cybersecurity-insurance.

CISA. “Security Tip (ST04-015): Understanding Denial-of-Service Attacks.” *Cybersecurity and Infrastructure Security Agency CISA*, 20 Nov. 2019, us-cert.cisa.gov/ncas/tips/ST04-015.

Clement, J. “Number of Ransomware Attacks per Year 2019.” *Statista*, 23 June 2020, www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/.

Clifford, Ralph D. *Cybercrime: the Investigation, Prosecution and Defense of a Computer-Related Crime*. Carolina Academic Press, 2001.

Clough, Jonathan. "A world of difference: the Budapest convention of cybercrime and the challenges of harmonisation." *Monash UL Rev.* 40 (2014): 698.

Connecticut, Senate, House. Public Act No. 17-223. 2017. Connecticut General Assembly, https://www.cga.ct.gov/2017/ACT/pa/2017PA-00223-R00HB-07304-PA.htm

CR, Srinivasan. “Hobby Hackers to Billion-Dollar Industry: the Evolution of Ransomware.” *Computer Fraud & Security*, 2017, pp. 7–9., doi:10.1016/s1361-3723(17)30081-7.

“Cyber Crime.” FBI, 3 May 2016, www.fbi.gov/investigate/cyber.

“Cyber Threat Source Descriptions.” *Cybersecurity and Infrastructure Security Agency CISA*, www.us-cert.gov/ics/content/cyber-threat-source-descriptions#terror.

Dedrick, Douglas. "The History of Driving Laws (1901-1960)." *Healing Law*, 18 Mar. 2020, healinglaw.com/blog/the-history-of-driving-laws-1901-1960/#:~:text=In the Beginning…&text=Once automobiles were made and,laws only regulated vehicle speeds.

Deere, Stephen. "CONFIDENTIAL REPORT: Atlanta's Cyber Attack Could Cost Taxpayers $17 Million." *AJC*, The Atlanta Journal-Constitution, 1 Aug. 2018, www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K/.

De Groot, Juliana. "The History of Data Breaches." *Digital Guardian*, 24 Oct. 2019, digitalguardian.com/blog/history-data-breaches#:~:text=The majority of the largest,reported as an inside job.&text=Target: 70 million records compromised,million records compromised in 2014.

De Groot, Juliana. "What Is the California Consumer Privacy Act?" *Digital Guardian*, 1 Dec. 2020, digitalguardian.com/blog/what-california-data-privacy-protection-act.

Del Pizzo, Nancy A. "How Will California Cybersecurity Laws Affect U.S. Business?" *American Bar Association*, 5 Nov. 2018, www.americanbar.org/groups/litigation/committees/intellectual-property/practice/2018/how-will-california-cybersecurity-laws-affect-us-business.

"Digest of Education Statistics, 2017." *National Center for Education Statistics (NCES) Home Page, a Part of the U.S. Department of Education*, Mar. 2018, nces.ed.gov/programs/digest/d17/tables/dt17_702.60.asp.

Dodge, Ronald, Kathryn Coronges, and Ericka Rovira. "Empirical benefits of training to phishing susceptibility." *IFIP International Information Security Conference*. Springer, Berlin, Heidelberg, 2012.

Donaldson, Jennifer. "The History of Seat Belts: Have They Always Been Effective for Men and Women?" *Safe Ride 4 Kids*, 21 Apr. 2020, saferide4kids.com/blog/history-of-seat-belts-effective/.

Driver & Vehicle Standards Agency. "History of Road Safety, The Highway Code and the Driving Test." *GOV.UK*, 2020, www.gov.uk/government/publications/history-of-road-safety-and-the-driving-test/history-of-road-safety-the-highway-code-and-the-driving-test.

Dudley, Renee. "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks." *ProPublica*, 27 Aug. 2019, www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks.

Duncan, Ian. "Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts." *Baltimoresun.com*, Baltimore Sun, 30 June 2019, www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html.

Emsley, Clive. "'Mother, What Did Policemen Do When There Weren't Any Motors?' The Law, the Police and the Regulation of Motor Traffic in England, 1900–1939." *The Historical Journal*, vol. 36, no. 2, 1993, pp. 357–381., doi:10.1017/s0018246x00019270.

Farmer, Liz. "The Next Big Technology to Transform Government." *Governing*, Sept. 2017, www.governing.com/topics/mgmt/gov-blockchain-technology-government-services.html.

Fernando, Matheesha, and Nalin Asanka Gamagedara Arachchilage. "Why Johnny can't rely on anti-phishing educational interventions to protect himself against contemporary phishing attacks?." *arXiv preprint arXiv:2004.13262* (2020).

Fitz-Gerald, Sean. "Virus Coaxes Man to Turn Himself in for Child Pornography." *Mashable*, Mashable, 28 July 2013, mashable.com/2013/07/28/virus-child-pornography/.

Flores, Rosa. “Palm Beach County Elections Office Allegedly Hit by Ransomware Attack in 2016.” *CNN*, Cable News Network, 13 Feb. 2020, www.cnn.com/2020/02/13/politics/palm-beach-county-elections-ransomware-attack/index.html.

Flowers, Angelyn, et al. “Cybersecurity and US Legislative Efforts to Address Cybercrime.” *Journal of Homeland Security and Emergency Management*, vol. 10, no. 1, 2013, doi:10.1515/jhsem-2012-0007.

Flynn, Payton A. “Cybersecurity: Utilizing Fusion Centers to Protect State, Local, Tribal, and Territorial Entities against Cyber Threats.” *Naval Postgraduate School*, 2016.

Franco, Jim. “Colonie's MIS Department Takes on Ransomware Hackers.” *Spotlight News*, 5 Feb. 2020, www.spotlightnews.com/news/2020/02/05/colonies-mis-department-takes-on-ransomware-hackers/.

Franco, Jim. “Town of Colonie Got Hacked; Looks to Avoid Paying Ransomware Demand of about $400,000.” *Spotlight News*, 17 Jan. 2020, www.spotlightnews.com/news/2020/01/17/town-of-colonie-got-hacked-looks-to-avoid-paying-ransomware-demand-of-about-400000/.

Freed, Benjamin. “Ransomware Attacks Map Chronicles a Growing Threat.” *StateScoop*, 22 Oct. 2019, statescoop.com/ransomware-attacks-map-state-local-government/.

Fries, Amanda. “Albany's Repair Cost after Ransomware Attack: $300,000.” *Times Union*, Times Union, 27 Sept. 2019, www.timesunion.com/news/article/Ransomware-attack-on-Albany-cost-300K-to-14473544.php.

Gates, Megan. “Cities Are the New Ransomware Target.” *ASIS Homepage*, 1 Sept. 2019, www.asisonline.org/security-management-magazine/articles/2019/09/cities-are-the-new-ransomware-target/.

“Global Cyber Strategies Index.” *Global Cyber Strategies Index | Center for Strategic and International Studies*, www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/global-cyber-strategies-index.

Gordon, Sarah, and Richard Ford. “On the Definition and Classification of Cybercrime.” *Journal in Computer Virology*, vol. 2, no. 1, 2006, pp. 13–20., doi:10.1007/s11416-006-0015-z.

Grabosky, Peter, and Sascha Walkley. "Computer crime and white-collar crime." *International handbook of white-collar and corporate crime*. Springer, Boston, MA, 2007. 358-375.

Hakmeh, Joyce, and Allison Peters. “A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet.” *Council on Foreign Relations*, 13 Jan. 2020, www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

Hallenback, Chris. “What New Cybersecurity Legislation Doesn't Include.” *Security Boulevard*, 30 June 2020, securityboulevard.com/2020/06/what-new-cybersecurity-legislation-doesnt-include/.

Halpern, Mollie, and Herbert Stapleton. “FBI, This Week: Reveton Ransomware.” *FBI: Audio*, FBI, 10 Aug. 2012, www.fbi.gov/audio-repository/news-podcasts-thisweek-reveton-ransomware/view.

Hampton, Nikolai, and Zubair A Baig. “Ransomware: Emergence of the Cyber-Extortion Menace .” *13th Australian Information Security Management Conference*, 2015, pp. 47–56., doi:10.4225/75/57b69aa9d938b.

Hastings, Justin V. *No Mans Land: Globalization, Territory, and Clandestine Groups in Southeast Asia*. NUS Press, 2011.

Hathaway, Melissa E. “Cyber Readiness Index 1.0.” *Hathaway Global Strategies LLC*, 2013.
Hathaway, Melissa, et al. “Cyber Readiness Index 2.0 a Plan for Cyber Readiness: A Baseline and an Index.” *Potomac Institute for Policy Studies*, 2015.
Heine, Jorge, and Ramesh Thakur. “Introduction: Globalization and Transnational Uncivil Society.” *The Dark Side of Globalization*, United Nations University Press, 2011, pp. 1–16.
Herjavec, Robert. “Cybersecurity CEO: The History Of Cybercrime, From 1834 To Present.” *Herjavec Group*, 18 July 2019, www.herjavecgroup.com/history-of-cybercrime/.
Hernandez-Castro, J., et al. “An Economic Analysis of Ransomware and Its Welfare Consequences.” *Royal Society Open Science*, vol. 7, no. 3, Mar. 2020, p. 190023., doi:10.1098/rsos.190023.
Hildebrand, Mary J., et al. “The California Consumer Privacy Act: An FAQ for Investment Managers - Privacy & Cybersecurity, Investment Management | Lowenstein Sandler LLP.” *Lowenstein Sandler*, 27 Feb. 2020, www.lowenstein.com/news-insights/publications/client-alerts/the-california-consumer-privacy-act-an-faq-for-investment-managers-privacy-cybersecurity-investment-management.
History.com Editors. “Connecticut Enacts First Speed-Limit Law.” *History.com*, A&E Television Networks, 13 Nov. 2009, www.history.com/this-day-in-history/connecticut-enacts-first-speed-limit-law.
History.com Editors. “First Electric Traffic Signal Installed.” *History.com*, A&E Television Networks, 13 Nov. 2009, www.history.com/this-day-in-history/first-electric-traffic-signal-installed.
Hlavac, Marek (2018). stargazer: Well-Formatted Regression and Summary Statistics Tables. R package version 5.2.2. https://CRAN.R-project.org/package=stargazer.
Hospelhorn, Sarah. “Analyzing Company Reputation After a Data Breach: Varonis.” *Inside Out Security*, 30 Mar. 2020, www.varonis.com/blog/company-reputation-after-a-data-breach/.
Hughes, Matthew. “A History of Ransomware: Where It Started & Where It's Going.” *MakeUseOf*, 27 July 2016, www.makeuseof.com/tag/history-ransomware-russia-reveton/.
Illinois, Senate, House. Public Act No. 100-0040. 2017. Illinois General Assembly, https://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=100-0040.
Ilves, Luukas K., Timothy J. Evans, Frank J. Cilluffo, and Alec A. Nadeau. “European Union and NATO Global Cybersecurity Challenges: A Way Forward.” *Institute for National Strategic Security, National Defense University*, vol. 6, no. 2, 2016, pp. 126–141.
Injury Facts. “Car Crash Deaths and Rates.” *Injury Facts*, 20 Feb. 2020, injuryfacts.nsc.org/motor-vehicle/historical-fatality-trends/deaths-and-rates/.
Jampen, Daniel, et al. “Don’t Click: towards an Effective Anti-Phishing Training. A Comparative Literature Review.” *Human-Centric Computing and Information Sciences*, vol. 10, no. 33, 2020, doi:https://doi.org/10.1186/s13673-020-00237-7.
Jane, Emma A., and Elena Martellozzo. “Introduction: Victims of Cybercrime on the Small ‘i’ Internet.” *Cybercrime and Its Victims*, Routledge, 2017, pp. 1–24.
Jensen, Matthew L., et al. "Training to mitigate phishing attacks using mindfulness techniques." *Journal of Management Information Systems* 34.2 (2017): 597-626.
Johnston, Ryan. “Possession of Ransomware Is Now a Crime in Michigan.” *StateScoop*, 5 Apr. 2018, statescoop.com/possession-of-ransomware-is-now-a-crime-in-michigan/.

Kanwisher, Carly, and Kim Mobley. “Impact of NAIC's Insurance Data Security Model Law.” *Johnson Lambert LLP*, July 2019, www.johnsonlambert.com/post/impact-of-naics-insurance-data-security-model-law/#:~:text=The NAIC Insurance Data Security Model Law&text=The Model Law's purpose is,consumers and markets from fraud.

Karakoç, Mesut. “Understanding the Barriers to Addressing Cybersecurity Challenges in American State and Local Governments.” *University of Delaware*, 2017.

Karimi, Faith. “Florida City to Pay $600K Ransom to Hacker Who Seized Computer Systems Weeks Ago.” *CNN*, Cable News Network, 20 June 2019, www.cnn.com/2019/06/20/us/riviera-beach-to-pay-hacker/index.html.

Kaspersky. “What Is Social Engineering?” *Usa.kaspersky.com*, Kaspersky, 26 Aug. 2020, usa.kaspersky.com/resource-center/definitions/what-is-social-engineering.

Keizer, Gregg. “Ransomware Plays Pirated Windows Card, Demands $143.” *Computerworld*, Computerworld, 6 Sept. 2011, www.computerworld.com/article/2510938/ransomware-plays-pirated-windows-card--demands--143.html.

Kelly, Brian B. “Investing in a Centralized Cybersecurity Infrastructure: Why ‘Hacktivism’ Can and Should Influence Cybersecurity Reform.” *Boston University Law Review*, vol. 92, no. 1663, 2012, pp. 1663–1711.

Khadam, Nadia. "Insight to Cybercrime." *Taipei University Law Review* 29.1 (2012): 55-80.

Kharraz, Amin, et al. "Cutting the gordian knot: A look under the hood of ransomware attacks." *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, Cham, 2015.

KnowBe4. “Ransomware.” *KnowBe4*, 2020, www.knowbe4.com/ransomware#ransomwaretimeline.

Kosseff, Jeff. “New York’s Financial Cybersecurity Regulation: Tough, Fair, and a National Model.” *Georgetown Law Technology Review*, vol. 1, no. 2, 2017, pp. 436–445.

Krasner, Stephen D. “Sovereignty.” *Foreign Policy*, no. 122, 2001, p. 20. doi:10.2307/3183223.

Kshetri, Nir. “Cybercrime and Cybersecurity in Africa.” *Journal of Global Information Technology Management*, vol. 22, no. 2, pp. 77–81.

Kumaraguru, Ponnurangam, et al. "Lessons from a real world evaluation of anti-phishing training." *2008 eCrime Researchers Summit*. IEEE, 2008.

Kumaraguru, Ponnurangam, et al. "School of Phish: A Real-Word Evaluation of Anti-Phishing Training (Cmu-Cylab-09-002)." (2009).

Liska, Allan. “Early Findings: Review of State and Local Government Ransomware Attacks.” *Recorded Future*, 10 May 2019, www.recordedfuture.com/state-local-government-ransomware-attacks/.

Marsh, Ben. “Maze Malware: The First Iteration of Leakware.” *EmergInRisk.com*, EmergIn Risk, May 2020, emerginrisk.com/wp-content/uploads/2020/05/Maze-Malware-The-First-Iteration-of-Leakware.pdf?utm_source=slipcase&utm_medium=affiliate&utm_campaign=slipcase.

Maryland, Senate, House. Senate Bill 204, Chapter 415. 2018. Maryland General Assembly, http://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0204?ys=2018rs.

McGee, Marianne Kolbasuk. “HHS: Most Ransomware Attacks Reportable Breaches.” *Careers Information Security*, 12 July 2016, www.careersinfosecurity.com/hhs-most-ransomware-attacks-reportable-breaches-a-9257.

McGuire, Mike, and Samantha Dowling. "Cyber crime: A review of the evidence." *Summary of key findings and implications. Home Office Research report* 75 (2013).

Meet The Press. "Meet the Press Transcript - March 15, 2015." *NBCNews.com*, NBCUniversal News Group, 15 Mar. 2015, www.nbcnews.com/meet-the-press/meet-press-transcript-march-15-2015-n323871.

Meland, Per Hakon, Yara Fareed Fahmy Bayoumy, and Guttom Sindre, "The Ransomware-as-a-Service Economy within the Darknet," *Computers & Security* (May 2020) pg 2.

Michael, Melissa. "Why These Online Criminals Actually Care About Your Convenience - F-Secure Blog." *F-Secure*, F-Secure, 18 July 2016, blog.f-secure.com/why-these-online-criminals-actually-care-about-your-convenience/?_ga=1.110524544.461697977.1455876699.

Mohurle, Savita, and Manisha Patil. "A Brief Study of Wannacry Threat: Ransomware Attack 2017." *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017, pp. 1938–1940.

Moor, James H. "What Is Computer Ethics?" *Metaphilosophy*, vol. 16, no. 4, 1985, pp. 266–275., doi:10.1111/j.1467-9973.1985.tb00173.x.

Moore, Stephen. "Arming Agencies for Ransomware Attacks in an Election Year." *GCN*, 13 Nov. 2019, gcn.com/articles/2019/11/13/ransomware-election-year.aspx.

Moore, Tyler. "The Economics of Cybersecurity: Principles and Policy Options." *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3-4, 2010, pp. 103–117., doi:10.1016/j.ijcip.2010.10.002.

Morgan, Steve. "Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019." *Cybercrime Magazine*, 20 Oct. 2018, cybersecurityventures.com/ransomware-damage-report-2017-part-2/.

Nadir, Ibrahim, and Taimur Bakhshi. "Contemporary Cybercrime: A Taxonomy of Ransomware Threats & Mitigation Techniques." *2018 International Conference on Computing, Mathematics and Engineering Technologies (ICoMET)*, 2018, doi:10.1109/icomet.2018.8346329.

Nakashima, Ellen. "Insurance Requirements Can Drive Stronger Cybersecurity, Treasury Official Says." *The Washington Post*, WP Company, 10 Sept. 2015, www.washingtonpost.com/world/national-security/insurance-requirements-can-drive-stronger-cybersecurity-treasury-official-says/2015/09/10/823c923c-57e3-11e5-8bb1-b488d231bba2_story.html.

"National Population Totals: 2010-2019." *The United States Census Bureau*, 30 Dec. 2019, www.census.gov/data/datasets/time-series/demo/popest/2010s-national-total.html#par_textimage_401631162.

NCSL, "About Us." *National Conference of State Legislators*, 2020, www.ncsl.org/aboutus.aspx.

NCSL, "Cybersecurity Legislation 2019," *NCSL.* 2020. https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx.

NCSL. "Telecommunications and Information Technology." *Telecommunications and Information Technology in Legislative Affairs*, 2020, www.ncsl.org/research/telecommunications-and-information-technology.aspx.

Newmeyer, Kevin P. "Who Should Lead U.S. Cybersecurity Efforts?" *Institute for National Strategic Security, National Defense University*, vol. 3, no. 2, Mar. 2012, pp. 115–126.

News Staff. “Estimated State IT Budgets for 2018.” *Government Technology State & Local Articles - E.Republic*, 26 Feb. 2018, www.govtech.com/biz/data/Estimated-State-IT-Budgets-for-2018.html.

Norris, Donald, et al. “Cybersecurity Challenges to American State and Local Governments.” AcademicConferencesandPublishingInternationalLimited, *Proceedings of the 15th European Conference on e-Government University of Portsmouth, UK*, 2015, pp. 196–202.

NortonLifeLock. *What Is a Computer Worm and How Does It Work?*, Norton, 6 July 2020, us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html.

Novinson, Michael. “Albany Airport Pays Ransom After Its MSP Was Hit By Ransomware.” *CRN*, 14 Jan. 2020, www.crn.com/news/security/albany-airport-pays-ransom-after-its-msp-was-hit-by-ransomware?itc=refresh.

Nwankwo, Wilson, and Kingsley Chiwuike Ukaoha. “Socio-Technical Perspectives On Cybersecurity: Nigeria‘s Cybercrime Legislation In Review.” *International Journal of Scientific & Technology Research*, vol. 8, no. 10, Oct. 2019, pp. 47–58.

Ogu, Emmanuel C., Chiemela Ogu, and Onyekwere U. Oluoha. “Global Cybersecurity Legislation - Factors, Perspective and Implications.” *International Journal of Business Continuity and Risk Management*, vol. 10, no. 1, 2020, p. 80-93, doi:10.1504/ijbcrm.2020.10027390

Osborne, Charlie. “MegaCortex Ransomware Slams Enterprise Firms with $5.8 Million Blackmail Demands.” *ZDNet*, ZDNet, 5 Aug. 2019, www.zdnet.com/article/megacortex-ransomware-slams-eu-firms-with-demands-of-up-to-5-8-million/.

Paganini, Pierluigi. “10 Biggest Cyber Espionage Cases.” *Security Affairs*, 11 Dec. 2017, securityaffairs.co/wordpress/66617/hacking/cyber-espionage-cases.html#:~:text=Operation Shady RAT is undeniably,2008 Olympic Games in Beijing.

Pal, Kaushik. “10 Ways Virtualization Can Improve Security.” *Techopedia.com*, Techopedia, 29 Apr. 2015, www.techopedia.com/2/31007/trends/virtualization/10-ways-virtualization-can-improve-security.

Palmer, Danny. “Ransomware: The Key Lesson Maersk Learned from Battling the NotPetya Attack.” *ZDNet*, ZDNet, 29 Apr. 2019, www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/.

Palo Alto Networks, Inc. “Use Case: Consolidate Network Security, Reduce Costs and Complexity.” *Palo Alto Networks*, 2017, www.paloaltonetworks.com/resources/whitepapers/consolidate-network-security-usecase.

Pope, Justin. “Ransomware: Minimizing the Risks.” *Innovations in Clinical Neuroscience*, vol. 13, no. 11-12, 2016, pp. 37–40.

Porup, J. M. “Does Cyber Insurance Make Us More (or Less) Secure?” *CSO Online*, 18 June 2018, www.csoonline.com/article/3280990/does-cyber-insurance-make-us-more-or-less-secure.html#:%7E:text=%22Moral%20hazard%22%20is%20the%20term,incentives%20that%20insurance%20can%20create.&text=That%20way%20the%20insured%20shares,cybersecurity%20controls%20in%20their%20enterprise.

“President Clinton: Working to Strengthen Cybersecurity,” *White House at Work*, https://clintonwhitehouse4.archives.gov/WH/Work/021600.html.

Pylant, Autum C. “Initiating a Collaborative Cybersecurity Governance Framework at the State Level.” *West Chester University*, 2020.

Qabajeh, Issa, Fadi Thabtah, and Francisco Chiclana. "A recent review of conventional vs. automated cybersecurity anti-phishing techniques." *Computer Science Review* 29 (2018): 44-55.

Rashid, Fahmida Y. "4 Reasons Not to Pay up in a Ransomware Attack." *InfoWorld*, InfoWorld, 14 Mar. 2016, www.infoworld.com/article/3043197/4-reasons-not-to-pay-up-in-a-ransomware-attack.html.

Rasmussen, Scott. "Centralized Network Security Management: Combining Defense In Depth with Manageable Security." *SANS Institute*, 28 Jan. 2002, www.sans.org/reading-room/whitepapers/bestprac/paper/659.

Reinsurance News. "Total WannaCry Losses Pegged at $4 Billion - Reinsurance News." *Reinsurance News*, 25 Sept. 2017, www.reinsurancene.ws/total-wannacry-losses-pegged-4-billion/.

Richardson, Ronny, and Max North. "Ransomware: Evolution, Mitigation and Prevention." *International Management Review*, vol. 13, no. 1, 2017, pp. 10–21.

Riley, Michael, and Jordan Robertson. "Russian Hacks on U.S. Voting System Wider Than Previously Known." *Bloomberg.com*, Bloomberg, 13 June 2017, www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

Robinson, Doug, and Srini Subramanian. Deloitte and NASCIO, 2016, *2016 Deloitte-NASCIO Cybersecurity Study*, www2.deloitte.com/global/en/insights/industry/public-sector/nascio-survey-government-cybersecurity-strategies-2016.html.

Robles, Frances. "When Ransomware Cripples a City, Who's to Blame? This I.T. Chief Is Fighting Back." *The New York Times*, The New York Times, 22 Aug. 2019, www.nytimes.com/2019/08/22/us/florida-ransomware-hacking-it.html.

Rosenau, James N. *Distant Proximities: Dynamics beyond Globalization*. Princeton University Press, 2003.

Rosner, Eric. "Cyber Federalism: Defining Cyber's Jurisdictional Boundaries." *Naval Postgraduate School*, 2017.

Rouse, Margaret. "What Is Redundancy? - Definition from WhatIs.com." *WhatIs.com*, TechTarget, 16 Apr. 2009, whatis.techtarget.com/definition/redundancy.

Rouse, Margaret. "What Is Server Virtualization?" *SearchServerVirtualization*, TechTarget, 7 Nov. 2019, searchservervirtualization.techtarget.com/definition/server-virtualization.

Salvi, Harshada U., and Ravindra V. Kerkar. "Ransomware: A Cyber Extortion." *Asian Journal of Convergence in Technology*, II, no. III, 2016.

Sarre, Rick, Laurie Yiu-Chung Lau, and Lennon YC Chang. "Responding to cybercrime: current trends." *Police Practice and Research*, vol. 19, no. 6, 2018, 515-518.

Savage, Kevin, et al. "The Evolution of Ransomware." *Symantec*, 6 Aug. 2015, pp. 1–56.

Schackelford, Scott J, and Zachery Bohm. "Securing Critical North American Infrastructure: A Comparatice Case Study in Cybersecurity Regulation ." *Canada-United States Law Journal*, vol. 40, no. 1, 2016, pp. 61–70.

Schjolberg, Stein. "The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva." *Journal of International Commercial Law and Technology*, vol. 1, no. 12, 2008, pp. 1–19.

Schneier, Bruce. "1834: The First Cyberattack." *Schneier on Security*, 31 May 2018, www.schneier.com/blog/archives/2018/05/1834_the_first_.html.

Scholte, Jan Aart. *Globalization: a Critical Introduction*. Palgrave Macmillan, 2005.

Scott-Cowley, Orlando. “Ransomware Payments Methods Used by Attackers.” *Veeam Software Official Blog*, 29 June 2020, www.veeam.com/blog/frequent-methods-for-ransomware-payments.html.

Seger, Alexander. "The Budapest Convention 10 Years On: Lessons Learnt." *ISP C* (2011): 167.

Segura, Jérôme. “Citadel: a Cyber-Criminal's Ultimate Weapon?” *Malwarebytes Labs*, 30 Mar. 2016, blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/#:~:text=In old times, a citadel,manage infected computers (bots).

SentinelOne. “The History of Cyber Security — Everything You Ever Wanted to Know.” *SentinelOne*, 10 Feb. 2019, www.sentinelone.com/blog/history-of-cyber-security/.

Shackelford, Scott, and Andraz Kastelic. “Toward a State-Centric Cyber Peace? Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity.” *SSRN Electronic Journal*, 2014, doi:10.2139/ssrn.2531733.

Siegel, Bill. “Ransomware Costs Double in Q4 as Ryuk Sodinokibi Proliferate.” *Coveware*, Coveware: Ransomware Recovery First Responders, 23 Jan. 2020, www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.

Singh, Hardeep. “A Glance At The United States Cyber Security Laws.” *Appknox*, 7 Jan. 2016, www.appknox.com/blog/united-states-cyber-security-laws.

Singh, Param and Rick McElroy. “Dark Web Ransomware Economy Growing at an Annual Rate of 2,500%.” *VMware Carbon Black*, 11 October 2017, www.carbonblack.com/blog/dark-web-ransomware-economy-growing-annual-rate-2500/.

Sittig, Dean F., and Hardeep Singh. “A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks.” *Applied Clinical Informatics*, vol. 07, no. 02, June 2016, pp. 624–632., doi:10.4338/aci-2016-04-soa-0064.

Smith, Aaron. “What Americans Knows About Cybersecurity.” *Pew Research Center: Internet, Science & Tech*, Pew Research Center, 17 Aug. 2020, www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/.

Sobers, Rob. “The Anatomy of a Phishing Email.” *Varonis*, 30 Mar. 2020, www.varonis.com/blog/spot-phishing-scam/.

Solomon, Kristine. “Got Random Political Campaign Spam in Your Inbox? It Could Lead to Identity Theft.” *Yahoo!Life*, 6 Sept. 2020, www.yahoo.com/lifestyle/campaign-spam-unsubscribe-spam-malwarebytes-144535324.html.

Spence, Nikki, MS, Niharika Bhardwaj, MBBS, MS, David P. Paul III, DDS, PhD, and Alberto Coustasse, DrPH, MD, MBA, MPH. “Ransomware in Healthcare Facilities: A Harbinger of the Future?” *Perspectives in Health Information Management,* 2018.

Spidalieri, Francesca. "State of the States on Cybersecurity." *Pell Center for International Relations* (2015).

Stromberg, Joseph. “When Was the First Traffic Light Installed? Today in 1914.” *Vox*, Vox, 5 Aug. 2015, www.vox.com/2015/8/5/9097713/when-was-the-first-traffic-light-installed.

Sullivan, Kieran. “11 Points to Consider When Virtualizing Security.” *Infosec Resources*, 30 Jan. 2018, resources.infosecinstitute.com/11-points-consider-virtualizing-security/#gref.

Sutherland, Ewan. "Governance of Cybersecurity – The Case of South Africa." *The African Journal of Information and Communication*, vol. 20, 2017, pp. 83–112., doi:10.23962/10539/23574.

Tehrani, Rich. "NotPetya: World's First $10 Billion Malware." *Apex Technology Services*, 28 Oct. 2017, www.apextechservices.com/topics/articles/435235-notpetya-worlds-first-10-billion-malware.htm#.

"The State of Ransomware in the US: Report and Statistics 2019: Emsisoft: Security Blog." *Emsisoft*, 20 July 2020, blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.

Tidy, Joe. "Police Launch Homicide Inquiry after German Hospital Hack." *BBC News*, 18 Sept. 2020, www.bbc.com/news/technology-54204356.

Townsend, Caleb. "A Brief and Incomplete History of Cybersecurity." *United States Cybersecurity Magazine*, 28 Jan. 2019, www.uscybersecurity.net/history/

Tran, Jasper L. "Navigating the Cybersecurity Act of 2015." *Chapman Law Review*, vol. 19, no. 2, 2016, pp. 483–499.

Trautman, Lawrence J. "Cybersecurity: What About U.S. Policy?" *SSRN Electronic Journal*, 2015, doi:10.2139/ssrn.2548561.

Trautman, Lawrence J., and Peter Ormerod. "Wannacry, Ransomware, and the Emerging Threat to Corporations." *SSRN Electronic Journal*, 2018, doi:10.2139/ssrn.3238293.

Tucker, Eric, Christina A. Cassidy, and Frank Bajak. "Ransomware Feared as Possible Saboteur for November Election." *The Denver Post*, The Denver Post, 2 Aug. 2020, www.denverpost.com/2020/08/02/election-2020-november-ransomware-mail-voting/.

United States, Congress, Fischer, Eric A. *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, Congressional Research Service, 2013. R42114.

Verizon. "Verizon's 2016 Data Breach Investigations Report Finds Cybercriminals Are Exploiting Human Nature." *Verizon*, 27 July 2017, www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human.

Waddell, Kaveh. "The Computer Virus That Haunted Early AIDS Researchers." *The Atlantic*, Atlantic Media Company, 10 May 2016, www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/.

Walker, Clive, and Ummi Hani Binti Masood. "Domestic Law Responses to Transnational Cyberattacks and Other Online Harms: Internet Dreams Turned to Internet Nightmares and Back Again ." *Notre Dame Journal of International & Comparative Law*, vol. 10, no. 1, 29 Jan. 2020, pp. 56–81.

Wash, Rick, and Molly M. Cooper. "Who Provides Phishing Training?" *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI 18*, 2018, doi:10.1145/3173574.3174066.

Weatherford, Holly, et al. NAIC and The Center for Insurance Policy and Research, 2020, *State Legislative Brief: The NAIC Insurance Data Security Model Law*, www.naic.org/documents/cmte_legislative_liaison_brief_data_security_model_law.pdf.

Weisbaum, Herb. "CryptoLocker Crooks Launch 'Customer Service' Site." *CNBC*, CNBC, 15 Nov. 2013, www.cnbc.com/2013/11/13/cryptolocker-crooks-launch-customer-service-site.html.

"What Is Ransomware?" w*ww.kaspersky.com*, Kaspersky, 11 June 2020, www.kaspersky.com/resource-center/definitions/what-is-ransomware.

Whitney, Lance. "Consumers Have Little Patience for Businesses Hit by Cyberattack." *TechRepublic*, TechRepublic, 29 Apr. 2020, www.techrepublic.com/article/consumers-have-little-patience-for-businesses-hit-by-cyberattack/.

Wills, Leonard. "A Very Brief Introduction on Cybersecurity Regulations/Standards: Part 1." *American Bar Association*, 30 Jan. 2020, www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2020/a-very-brief-introduction-on-cybersecurity-regulations-standards-1/.

Yang, Agnes, Young Jin Kwon, and Sang-Yong Tom Lee. "The Impact of Information Sharing Legislation on Cybersecurity Industry." *Industrial Management & Data Systems*, 17 Aug. 2020, doi:10.1108/imds-10-2019-0536.

Young, Adam, and Moti Yung. "Cryptovirology: Extortion-Based Security Threats and Countermeasures." *Proceedings of the IEEE Symposium on Security and Privacy*, 1996, doi:10.1109/secpri.1996.502676.

Young, Adam L., and Moti Yung. "Cryptovirology: The Birth, Neglect, and Explosion of Ransomware." *Communications of the ACM*, vol. 60, no. 7, July 2017, pp. 24–26., doi:10.1145/3097347.

Zetter, Kim. "What Is Ransomware? A Guide to the Global Cyberattack's Scary Method." *Wired*, 14 May 2017, www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/.

Zimba, Aaron, and Mumbi Chishimba. "Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures." *International Journal of Computer Network and Information Security*, vol. 11, no. 1, Jan. 2019, pp. 26–39., doi:10.5815/ijcnis.2019.01.03.

VITA

Joseph Skertic
Joseph.skertic@yahoo.com

Education

Old Dominion University [May 2012 - Current]
Ph.D. International Studies: American Foreign Policy and Comparative Politics

Regent University [December 2009 - May 2012]
M.A. Government: International Politics and American Government
Certificate in Terrorism and Homeland Defense

Christopher Newport University [August 2005 - December 2009]
B.A. Political Science
B.A. Philosophy and Religious Studies

Teaching Experience

Graduate Teaching Assistant
Old Dominion University [September 2015 – December 2015]

Graduate Teaching Assistant
Old Dominion University [May 2016 – August 2016]

Other Experience

Senior Property Claims Adjuster
Chubb Insurance [May 2018 – Present]

Immediate Solutions Customer Service Representative
Chubb Insurance [May 2017 – May 2018]

Senior Assistant Manager
Cinemark [June 2008 – May 2016]

Graduate Research Assistant
Virginia Modeling, Analysis, and Simulation Center [January 2014 – November 2014]