An Analysis of Cybersecurity Legislation and Policy Creation on the State Level

Adam Alexander, Paul Graham, Eric Jackson, Bryant Johnson, Tania Williams, and Jaehong Park

University of Alabama in Huntsville, Huntsville AL 35488, USA,
{aha0007, pag0006, eaj0010, bej0003, tania.williams, jae.park}@uah.edu

Abstract. To best create an effective cybersecurity strategy, it is imperative to understand the policy discussions and trends on a federal and state level. Effective cybersecurity legislation is vital to maintaining our country's infrastructure and protecting our citizenry. Since cybersecurity is often decided on the state level, states need to be aware of the trends in cybersecurity legislation. The purpose of this research was to conduct an analysis of cybersecurity policy from across the United States in an effort to assist the State-level understanding on their cybersecurity risk profile. This analysis included an examination of common trends in cybersecurity legislation. It involved researching cybersecurity policies from all 50 states and the federal government. After creating this baseline, the next phase of the research was to find and record relevant metadata for each policy. This data contained additional data, such as did it pass, who were the supporters, was it revised and other information that is useful to cybersecurity policy creators. The final goal of the research was to provide a searchable tool that could be utilized to fashion a successful cybersecurity bill and a summary of cybersecurity trends from 2011 to Spring 2018.

Keywords: cybersecurity, policy, legislation, United States, states, Federal Government

1 Introduction

It is critical that individual states enact policy dealing with cybersecurity. The National Governors Association, in hopes of addressing the cybersecurity deficit found in states across the nation, drafted A Compact to Improve Cybersecurity [1]. This compact includes a commitment to build cybersecurity governance, to prepare and defend the state from cybersecurity events, and to grow the na- tion's cybersecurity workforce. However, meeting such a commitment is difficult without an understanding of existing attempts of cybersecurity legislation from across the country.

As technology advances and cyber threats continue to grow, updating our country's cybersecurity policy is an important and daunting task. Our collective security infrastructure is woefully out-of-date and security policies differ from state to state. Therefore, the governor of Indiana signed executive order 17-11 in January of 2017, creating a council to "develop, maintain and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevanttothestrategicvision"ofthe state [2].

The role of this research was to provide the state with an analysis of existing cybersecurity policy from across the United States proposed from 2011 to present (as of Spring 2018). The research identified trends in policy (whether a policy was adopted or not after proposal). This research will serve as a baseline for the State of Indiana when crafting their policy and will provide valuable insight to other states who might choose to use the research.

In order to assist the States of Indiana in fulfilling the compact by developing their cybersecurity policy, we conducted a policy analysis using the following research questions:

- Whatpolicyhasbeenpassedsuccessfully/unsuccessfullyinotherstatesfrom 2011 to present (Spring 2018)?
- Who were the supporters of the policy?
- Whattypeofsupportdidtheproposedpolicyreceive,andifitdidnotpass, why?
- Howcansuchinformationbepresentedto Indianastakeholdersinaclear and concise manner?
- Whattrendsareevidentamongthestatesregardingcybersecuritypolicy?

In order to ensure that all policy was evaluated systematically, we developed a data collection form. Additionally, we organized the research by the 20 ex- isting Indiana committees, streamlining the examination and evaluation of the data. We examined similar trends analysis research and found, while research exists, the scope of the research was narrower. For example, Lowry examined the regulation of mobile payments but only dealt with federal law, making the reporting of such trends much easier [3]. Additionally, we were able to locate studies of trends resulting from one piece of legislation but did not find any previous work dealing with trends regarding state legislation. We provided a baseline for other large scale legislative trends analysis. Additionally, our database of na- tional cyber-related policies provides a valuable resource for other states as they seek to improve their cybersecurity posture.

2 Related Works

In 2007, the government of Estonia was hit by a cyber-attack that paralyzed the country, shutting down its largest bank, rendering credit cards useless, knocking media outlets offline, and crippling the country's telephone communications [4]. Could such an attack happen in the United States? Former cybersecurity czar Richard Clarke maintains that "few national governments have less control over what goes on in its cyberspace than Washington" and that "America's ability to defend its vital systems from cyber-attack ranks among the world's worst"

[5].Thisthreatofcyber-attackisnotlimitedthefederalgovernment.Individual states also must consider the threat of weak cybersecurity.

States, which hold databases full of health records, driving records, crimi- nal records, professional licenses, tax information, and birth certificates, must have procedures in place to protect this personally identifiable information. The states also often have jurisdiction of cyber-related crimes and are entrusted with cybersecurity education [6]. As Glennon notes, “Every state has enacted laws directed at protecting state governments and businesses specifically from cyber- intrusions”[6].Ontopofthis,statesalsobearmuchoftheburdenofregulation; however, as Sales states, law and policy of cybersecurity are undertheorized and most governments concern themselves with criminal law but are reluctant to see cybersecurity management in regulatory terms [5].

Bosch also notes issues with regulation, stating a reliability standard, such as those created through the Federal Power Act,“does not fully address Smart Grid cybersecurity from an interoperabilityperspective”[7].Alternatively,henotes thedifficultyofcraftingthestandards tobeginwith,citingthefailedGRIDAct of2010,whichthefederallegislativebranchcouldnot agreeonhowthegrid’s cybersecurity concerns should be addressed [7].

As every state is unique, so must each state take a different approach to cybersecurity. Schneider, in his call for government support of cybersecurity, noted as social values differ, governments should not expect uniform sets of cybersecurity goals; instead government interventions designed to achieve goals in some geographic region . . . must also accommodate the diversity in goals and enforcement mechanisms found in other regions [8]. When states craft their cybersecurity legislation, it is necessary to build on the experience of other states and to understand national policytrends.

AsGodaranotes,crimehasseena“revolutionaryshiftfromthemainactor, the criminal, to certain non-actors in the cyber world called ‘intermediaries’. To what extent an intermediary can be held liable for the crimes committed in cyber space is a question which is mooted all over the world” [9]. Godara’s research compares legislative and judicial trends in different countries. Her work was limited to rulings regarding intermediary liability in the United Kingdom, United States, and India. When examining legislation in the United States, her approach was to limit her study to federal court cases and sought to analyze fewer than ten rulings.

Bulger, Burton, O’Neill, and Staksrud also examine legislative trends in their examination of how different countries seek to protect children online [10]. In their research, they examined the United States, South Africa, and the European Union. The research targeted key crimes and then reported each country’s laws regarding these crimes. Again, the authors chose to research only federallaws and did not examine legislation from individual states.

Neither Godara nor Bulger et al. considered failed legislation when examining these trends [9, 10]. While both research examples relate to trends in cybersecu- rity, they do not provide an approach to handling the large volume of legislation relating to cybersecurity produced by individual states.

3 Data Collection and Analysis Process

In this section, we first discuss how we collected bills, what kind of metadata we used to identify and classify those bills. Then, after brief discussion on the database we used, we discuss how we examined and analyzed those collected bills.

3.1 Finding and Classifying a Bill

First, we examined digital archives to look for proposed legislation relating to cybersecurity. As stated before, each state usually had a digital archive of bills the researcher could examine using a keyword search. Once that location had been exhausted, secondary locations were searched. For each policy found, we recorded the following information:

- Location (1 of 50 states, Washington D.C., or the U.S. Congress)
- Type of policy (see classifications below)
- Bill name and/or number
- Source (where the bill can be found)

For the policy type, the following classifications were used:

- Government Service
- Finance
- Defense
- Energy
- Water/Wastewater
- Communications
- Healthcare
- Elections
- Economic Development
- Workforce Development
- Personal Identifiable Information
- Public Awareness and Training
- Education
- Emergency Services and Exercise
- Cyber Sharing
- Cyber Organizations (Center)
- Cyber Pre-Thru Post Incident
- Legal/Insurance
- Local Government
- Other critical infrastructure

These classifications were originally the 20 groups that make up the Indiana Executive Council on Cybersecurity and provided an clear way for the end user to reference trends and policies when using the final document as reference.

Data from primary online sources comprised the bulk of the information collected for the trends analysis. Most states provided some type of searchable archive. However, in cases where such databases were not available, we uti- lized second party databases to collect policy information. These second party databases included sites such as Find Law and Legiscan.

3.2 Creating a Collaborative Database

While many tools were available for storing and managing the research, we sought one that would allow us to collaborate seamlessly and would allow us toshareourdatawithendusers withoutrequiringspecializedsoftwareorpaid licensing. Wealso sought a product that was versatile enough to allow for link- ing fields together and even sharing data from one table to another using foreign keys. The tool also needed to have several sorting and filtering options. We used an online product called Airtable to meet our needs [11]. This tool, which creates sortable tables of the metadata can be found at the following address: https://airtable.com/shrCcYzKJGH1jyvrx.

After deciding on a tool, we fine-tuned the database design, listing necessary fields and then organized them to streamline the data entry process, identifying primary and foreign keys.

We formatted our information to prepare it for analysis. While reading the bills, the following information was collected in the database: Bill number, State, Type of policy, Type of legislation, Originator(senate, house, joint, or governor's office), Year introduced, Status, Link to online source, Related legislation, De- scription, Political party affiliation, Bill sponsor, and Link to vote count.

3.3 Trends Analysis

The next step was to begin the preliminary analysis of the data. Each state had its own cybersecurity policies. The number of each classification for every state was analyzed to discover what was most important to that state. We also made an effort to determine states that were currently active in developing cybersecurity programs.

Additionally, vetoed bills and failed legislation were examined. Some states, while successful in passing legislation in the house and senate, failed to garner the support of the state's governor. Since the reasons for such occurrences could be valuable, we wanted to analyze these instances. Failed legislation also merited special consideration. If a certain classification had a high number of bills written but the bills did not pass to become policies, then it can be inferred, while enough people thought the bill would be a good idea, an even greater number of people had negative thoughts about the bill to keep it from passing. This trend was explored to find out why.

We considered the influence of federal legislation. While states are respon- sible for crafting their own legislation, we wished to determine if the federal government's actions played a role in determining when and what cybersecurity topics were addressed on the state level.

States who proved to be cybersecurity pioneers were identified. Cybersecurity is more of a priority for some states than others. By examining the progression of cybersecurity legislation by state per year, patterns showing states who exhib- ited steady policy creation were evidenced. The states showing consistent policy creation over time were determined to be cybersecurity pioneers.

Bipartisan policy creation was also considered. One of the primary goals in the trends analysis was to determine factors that played a role in the successful passage of legislation. This included the success of a political party in getting a bill adopted. As data collection progressed, it became evident that bipartisan efforts garnered different results than partisan efforts.

Following the trends analysis, the final step was the analysis of results. The following questions were addressed:

- Are there states that could be considered pioneers to cybersecurity legisla- tion?
- To what degree does the federal government's actions influence state legis- lation?
- Are there paths that a bill takes that influences its success?

4 Cybersecurity Legislation Analysis

We identified 500 pieces of legislation relevant to cybersecurity within our eight year sample size. We surveyed 454 policies from all fifty states and Washington, D.C., as well as an additional 46 policies from the federal government.

4.1 States Currently Active in Passing Cybersecurity Legislation

In order to determine which states are actively developing their cybersecurity program, all 50 states were examined and the number of policies by year were recorded by state, as shown in Figure 1.

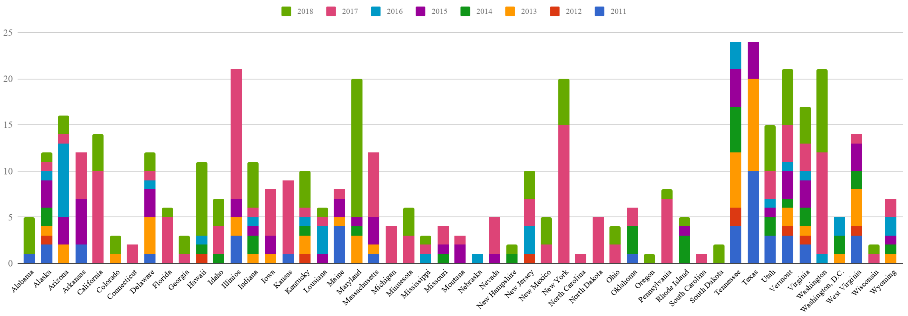

Fig. 1. The quantity of policies developed by each state per year between 2011 and 2018

Looking at the state policy by year, it was apparent that most states had between 1-10 cybersecurity policies. There were seven out of fifty states that had 20 or more policies.

The dates of the policies were also important. If most policies were proposed before 2016, then the state would not be considered as developing their cyber- security program. Of the seven states with a large range of policies, only four states created most of their policies from 2016 until now. The four states are Illinois, Maryland, New York, and Vermont.

While a single policy can have multiple policy types, it is still worthwhile to look at the number for each type. Illinois, New York, and Vermont had a high number of legal/insurance policies which would support the argument that most of the new policies being created by developing states were of the type legal/insurance. Vermont also had a high number of government service policies, especially in 2018. Figure 1 shows these two states have a high number of policies spread out over the whole sampling period (2011-2018).

4.2 Vetoed Bills

In five instances, proposed legislation made it through both the senate and the house; however, the legislation failed to be finalized by a state's governor.

Two of the bills were vetoed by California governor Edmund G. Brown, Jr. Both were introduced in 2017 and were unanimously passed by the state's assembly and senate. Bill AB1306 detailed the scope of the California Cyberse- curity Integration Center, which was established by Governor Brown's executive order in 2015 [12]. Brown, in his Governor's Veto Message, expressed concern "that placing the Center in statute as this bill proposes to do, will unduly limit the Center's flexibility as it pursues its mission to protect the state against cyberattacks" [13]. As for vetoed bill AB531, which required the department of technology's office of information security to evaluate existing security policies and develop plans to address deficiencies, Brown stated that the bill's objectives were already required by AB 670 [14].

A bill was vetoed by Governor Susana Martinez from New Mexico. It received 36 to 3 majority votes of support in the state's senate and 37 to 5 majority votes of support in the state's house. HB 364, while dealing primarily with limiting the prescription of contact lenses and glasses, did deal with cybersecurity by restricting a resident's access to online services. Martinez stated in her House Executive Message No. 57 that the bill limited the use of emerging technologies related to the issuance of contact lenses and glasses [15]. She cited this as the reason she chose to veto the bill.

The other two bills were vetoed by Governor Douglas Ducey of Arizona. Bill SB1434 was vetoed in 2016 after receiving unanimous votes from both the senate and the house. The governor indicated that he vetoed the bill, which dealt with consolidated purchasing and shared services of technology, stating he felt the bill added an extra layer of bureaucracy [16]. HB2566, dealing with password policy, encryption standards, and data security, was vetoed in 2015. It had passed the senate with a vote count of 17 to 11 and passed the house with a vote count of 56 to 1. Ducey stated that his administration had already addressed the concerns outlined in the bill [17].

4.3 Failed Legislation

Figure 2 shows the twenty classifications used to identify bills and the status count of the policies classification. Although a policy can have multiple classifications, this explores the number of times a classification has a relation to a legislation record.

The label “In Progress” is for classifications that are identified to be intro- duced and still up for discussion, and “Failed” are bills that are inactive, died in chamber, died in committee, or vetoed. Of the twenty classification types used to identify the bills, most classification types tended to have more failed poli- cies than passed bills. We identified that legislation related to Cyber Sharing, Economic Development, and Education have much higher failure rates than the other classifications. The seven classifications that were an exception include: policies dealing with cyber organizations, elections, emergency services and ex- ercise, finance, government service, local government, and water/waste- water. Furthermore, policies that were related to Elections and Water/Wastewater have greater rates of success than the other classifications. Notably, out of the six state legislations dealing with Water/Wastewater, five were passed successfully, one remains in progress, and zero failed.

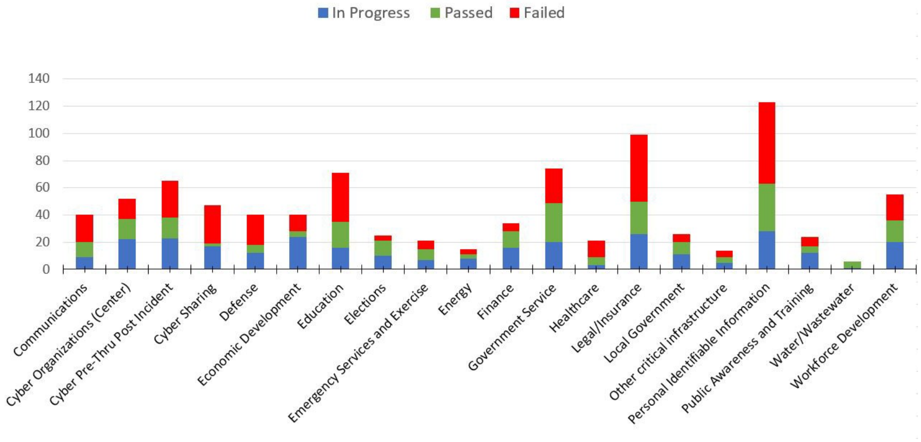

Fig. 2. The quantity of each policy type surveyed that is either still in process, was passed into law, or was failed for any reason

4.4 Influence of Federal Legislation

Figure 3 separates the federal legislation from the state legislation and shows the percentage each topic was covered in bills introduced at those levels within a time frame. In this figure, our eight year sample size was divided into two separate four year periods to show some slight changes in policy creation.

Much of the federal legislation from the U.S. Congress is focused on Defense, Cyber Pre-through-Post Incident, and in Cyber Sharing between organizations.

Federal legislation in those categories are consistently higher than all other cate- gories surveyed since 2011. For example, from 2011 to 2014, 61.1% of the federal legislation survey dealt at least some with Cyber Sharing. While those topics were addressed by some at the state level, our data does not show them being addressed by a large amount of states until 2017. Federal legislation appears to be driving state legislation to fill in the gaps where there are security concerns not addressed by the U.S. Congress atall.

In contrast to the federal legislation, state legislation heavily focused on top- ics such as Education, Personally Identifiable Information, Government Services, Legal/Insurance concerns such as defining cybersecurity crimes. These were top- ics that the U.S. Congress did not have many pieces of legislation on at all.

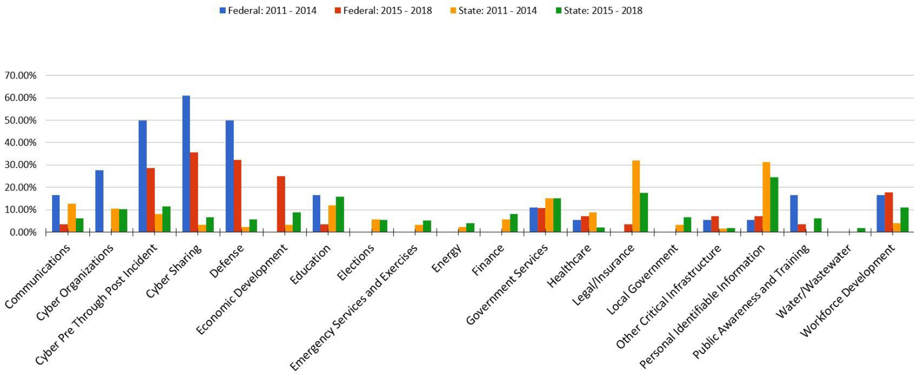

Fig. 3. The percentage of state and federal policies introduced in 4 year periods (2011-2014, and 2015-18) that deal each surveyed category

4.5 Cybersecurity Pioneers

Table 1 shows the number of policies when grouped by state and year. When analyzing the states and the number of policies they have proposed, it is easy to see that most states are not creating new policies. Of the 50 states, only 16 of them have at least 10 new policies since 2011. We used 10 policies as a cut off point since 10 policies provides enough sampling to determine the reg- ularity of policy creation. Pioneering states were Alaska(12), Arizona(16), Cal- ifornia(14), Delaware(12), Hawaii(11), Illinois(21), Indiana(11), Maryland(20), Massachusetts(12), New York(20), Tennessee(24), Texas(24), Vermont(21), Vir- ginia(21) Washington(21), and West Virginia(14) These states appear to be in 3 different classifications.

Early policy creation; however the state has not produced much legislation of late: In this category, the state created several policies earlier than

States with High Number of Policies 2016 - 2018				
Policy Type	**IL**	**MD**	**NY**	**VT**
Communications			5	3
Cyber Organizations	2	1	5	
Cyber Pre Through Post Incident	1	1		5
Cyber Sharing	1	1	3	
Defense		2		
Economic Development		5	5	1
Education	2	3	4	
Elections	1	2	1	
Emergency Services and Exercises			5	
Energy		1	3	3
Finance	1	2		
Government Services	3	2	3	4
Healthcare			1	
Legal/Insurance	3	3	7	5
Local Government	2		2	
Other Critical Infrastructure	1		1	
Personal Identifiable Information			3	4
Public Awareness and Training	1	1	5	
Water/Wastewater			2	
Workforce Development	2	5		
Total	20	29	55	25

Table 1. The quantity policies and their types that were passed between 2016 and 2018 in the states with the highest surveyed volume

2014 and then less after 2014. These states have dropped in their proactive ap- proach to cybersecurity and are not considered as pioneers. For example, Texas created the first bills for various types of policy. While creating several of bills early on, they have not been active in bill creation since 2015. The states of Ten- nessee, Texas, and West Virginia meet this criteria. Even though their number of policies are high, their concern for cybersecurity seems to have lessened.

Large policy creation; however, most of the policies have been created over the last 3 years: This grouping shows states that have created most of their cybersecurity policies over the past 3 years (2016-2018). These states, while recently producing more legislation, did not have the early policy adoption to be considered pioneers. Arizona, California, Delaware, Hawaii, Illinois, Indiana, Maryland, Massachusetts, New York, and Washington match this criteria. The higher policy producers worth nothing are Maryland (15 policies in 2018 alone), New York (20 policies in the past two years), and Washington (20 policies in the past two years also).

Steady policy creation: These high-producing policy creators consistently created bills over the sample years (2011-2018). As they consistently produced more cybersecurity policies than other states over the same sample time, it would suggest the states were pioneers in cybersecurity policy creation and not as reactive to other states through the years. As Figure 1 Number of Policies by State per Year shows, Alaska, Vermont and Virginia are the only states that match this criteria. Vermont has the most policies at 21 followed by Virginia at 17. Alaska did not have near as many with 12.

4.6 Bipartisan Success

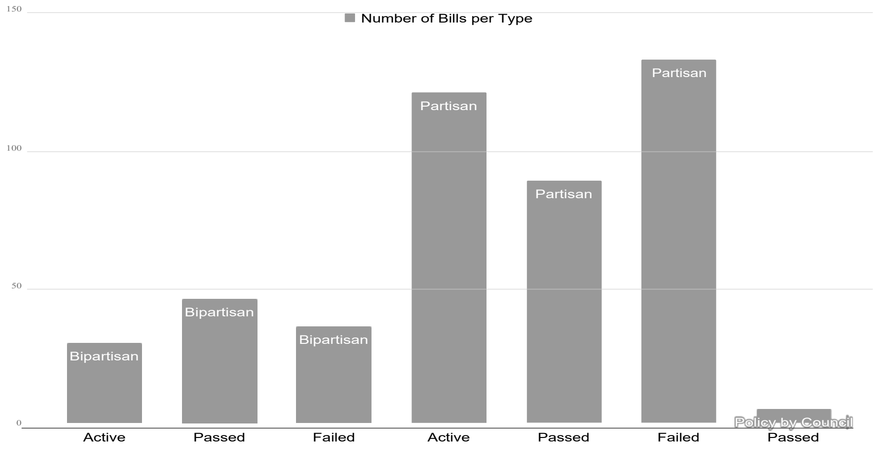

Fig. 4. Success of state level bipartisan legislation attempts as opposed to partisan legislation attempts

Of the 454 examples of state level cybersecurity legislation found, 109 records were bipartisan attempts. Of those attempts, 29 pieces of joint legislation were listed as actively being considered, meaning the outcome of the legislation was yet to be determined, and 45 of the bills that were introduced passed. When excluding legislation in progress, the resulting bipartisan success rate was 56%. In addition to bipartisan efforts, there were 5 records introduced by council, with all 5 passing. This success rate is significantly higher than partisan sponsored cybersecurity legislation on the state level, where, of the bills that were no longer actively being considered, only 88 passed, indicating a success rate of 40% (see Figure 4).

Cybersecurity topics that garnered the most state level bipartisan sponsor- ship included those relating to personal identifiable information (22 records), government services (19 records), legal (17 records), and cyber pre through post incident (16 records). There were no examples of bipartisan sponsorship relating to general policies.

Idaho and Kansas were the two states with the most bipartisan sponsored legislation, both having 7 records with bipartisan support. Iowa, Texas, Wash- ington, and Wyoming also were close in this category, having 6 instances each of utilizing bipartisan sponsorship for cybersecurity legislation. States with no bipartisan support of cybersecurity legislation included Arkansas, California, Georgia, Louisiana, Missouri, Montana, New Mexico, New York, North Carolina, Oklahoma, and Wisconsin. Washington, D.C., also had no records in this area.

This data is being stored at the following link using Airtable. Please follow the link below toviewthetool[11].https://airtable.com/shrCcYzKJGH1jyvrx

5 Challenges

5.1 Varying Terminology

One problem with our research was how verbiage varied from state to state. For example, one state might choose to use the term *cyber security*, while other states might use terms such as *computer crime* or *online security.* To ensure that each state was researched thoroughly and consistently, the researchers agreed on a list of keywords to use in theirsearch.

5.2 Determining Relevance

Also, the relevance of the proposed legislation to the targeted analysis data was also a challenge. Desired topics were often buried deep within unrelated information, resulting in researchers having to read and index bills that were, at first glance, not relevant to the desired data set.

5.3 Tracing a Bill's Origin

Another problem dealt with how bills are created. At times a bill originates in the house, and at other times it can be created in the senate. Bill numbers vary depending on the origin, and they can actually compete with each other. Also, a bill will stall in a committee, or the current legislature may elect not to take up a discussion on the bill. A new bill can be created the following year in order to try to create the policy. These bills must be linked in the research to provide a good picture on policy creation.

Oftentimes a generic bill will pass and become policy. After passing the first bill, a second bill will revise the original policy to provide clarification or addi- tional direction. The original bill and the following bills must be linked in the research also.

6 Conclusion

Excluding federal legislation and active legislation, we found 305 examples of state level legislation relating to cybersecurity. Of those, 138 records passed and 167 failed or were determined to be inactive, demonstrating a success rate of 45%.

Policies concerning elections and water/wastewater had higher success rates than other classifications. Policy topics that exhibited higher than average failure rates were related to cyber sharing, economic development, and education.

During the time period sampled, there seemed to be little correlation between federal cybersecurity policy efforts and those of the states. If fact, the two entities tended to complement each other, with federal policy having a much different focus than the states. For example, federal policies dealt more with defense, while state policies dealt more witheducation.

States showing consistent push in cybersecurity legislation were Vermont and Virginia. These states created policy steadily over the time period and met the criteria to be considered pioneers in cybersecurity legislation.

We determined that one factor that seemed to increase a piece of legisla- tion’schanceof success was the willingness of legislators to cross party lines in initiating new legislation. Bipartisan bills had a success rate of 56%, while bills introduced along party lines only had a success rate of 40%. Popular biparti- san topics included personal identifiable information, government services, legal, and cyber pre through post incident. When compared to the overall success rate of 45%. It is evident that bipartisan support is a favorable predictor of a bill’s chance of passage.

7 Future Work

In order for the research to continue to be useful, it is critical that the database be maintained. As new cybersecurity related legislation is proposed and considered, it should be catalogued in the base. By keeping the database current, the picture of national cybersecurity trends will become more granular, and the increased data will allow for better trend analysis.

Additionally, it would be beneficial for future researchers to expand the re- search by correlating the passage of legislation to related major cyber events. For example, researchers could determine if the Equifax breach resulted in an increase of proposed legislation related to personally identifiable information. If a correlation is evident, this could serve as a predictor of future proposed legislation.

Researchers could also attempt to measure the impact of key successful legis- lation. An example of this future work could be in the area of workforce develop- ment. Researchers could ascertain if states that adopted workforce development legislation have seen an increase in available professionals.

Furthermore, a thorough examination of failed legislation would aid legisla- tors when crafting legislation. By surveying bill sponsors, researchers could iden- tify key barriers to cybersecurity legislation, allowing policy makers the ability to better craft and propose bills. Also, researchers could compare failed legisla- tion from one state to similar successful legislation in another state to determine why similar legislation failed in one state but found successinanother.

Acknowledgement

Wewould like to thank the State of Indiana and INSuRE Program for their support and valuable inputs.

References

1. National Governors Association, Meet the threat: A compact to improve State Cybersecurity, 2017. [Online]. Available: https://www.in.gov/cybersecurity/files/NGA%20Cyber%20Compact.pdf
2. Holcomb, Eric J., “Exec. Order No. 17-11. Continuing the Indiana Executive Council on cybersecurity. State of Indiana Executive Department. Jan. 9, 2017. [Online]. Available: http://www.in.gov/gov/files/EO 17-11.pdf
3. Lowry, C., “What’s in your mobile wallet? An analysis of trends in mobile payments and regulation, Federal Communications Law Journal, vol. 68, no. 2, pp. 353-384, 2016. [Online]. Available: http://bi.galegroup.com.elib.uah.edu/essentials/article/GALE%7CA493323880/d7c701a94f8c8d9685b93203ad d71fee?u=avl uah
4. Sales, N. A., “Regulating cyber-security, Northwestern University Law Review, vol. 107, no. 4, pp. 1503-1568, 2013.
5. Clarke, R., “War From Cyberspace, The National Interest, vol. 104, pp. 31-36. 2009. [Online]. Available: http://www.jstor.org.elib.uah.edu/stable/42897693
6. Glennon, M. J. “State-level cybersecurity, Policy Review, vol. 171, pp. 85-102, 2012.
7. Bosch, C., “Securing the smart grid: Protecting national security and privacy through mandatory, enforceable interoperability standards, Fordham Urban Law Journal, vol. 41, no.4, pp. 1349-1406, 2014.
8. Schneider, F., “Impediments with policy interventions to foster cybersecurity, Communications of the ACM, vol. 61, no.3, pp. 36-38, March 2018.
9. Godara, S., “Role of ’intermediaries’ in the cyber world: a comparative study of the legislative policies & recent judicial trends, VIDHIGYA: The Journal Of Legal Awareness, vol. 8, no. 1, pp. 69-80, 2013.
10. Bulger, M., Burton, P., O’Neill, B., and Staksrud, E., “Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online, New Media & Society, vol. 19, no. 5, pp. 750-764. 2017.
11. Brown, Edmund G. Jr., “Exec. Order No. B-34-15 (2015). Establishing the California Cybersecurity Integration Center, CA.Gov, 2015. [Online]. Available: https://www.gov.ca.gov/2015/08/31/news19083/
12. “State of Cybersecurity, Airtable [Online]. Available: https://airtable.com/shrCcYzKJGH1jyvrx
13. Brown, Edmund G. Jr., “Governor’s Veto Message, Califor- nia Legislative Information, Oct. 11, 2017. [Online]. Avail- able: http://leginfo.legislature.ca.gov/faces/billStatusClient.x html?bill id=201720180AB1306
14. Brown, Edmund G. Jr., “Governor’s Veto Message, Califor- nia Legislative Information, Oct. 14, 2017. [Online]. Avail- able: http://leginfo.legislature.ca.gov/faces/billStatusClient.x html?bill id=201720180AB531
15. Martinez, Susana, “House Executive Message No. 57, New Mexico Secretary of State, Apr. 7, 2017. [Online]. Available: http://sos.state.nm.us/uploads/files/HB364-2017-V etoe d.pdf
16. Ducey, Douglas A., “Re:Senate Bill 1434, Office of the Governor, May 18, 2016. [Online]. Available: https://azgovernor.gov/sites/default/files/sb 1434 veto letter.pdf
17. Ducey, Douglas A., “RE: House Bill 2566, Arizona State Legislature, Apr. 9, 2015. [Online]. Available: https://www.azleg.gov/govlettr/52leg/1R/HB2566.pdf