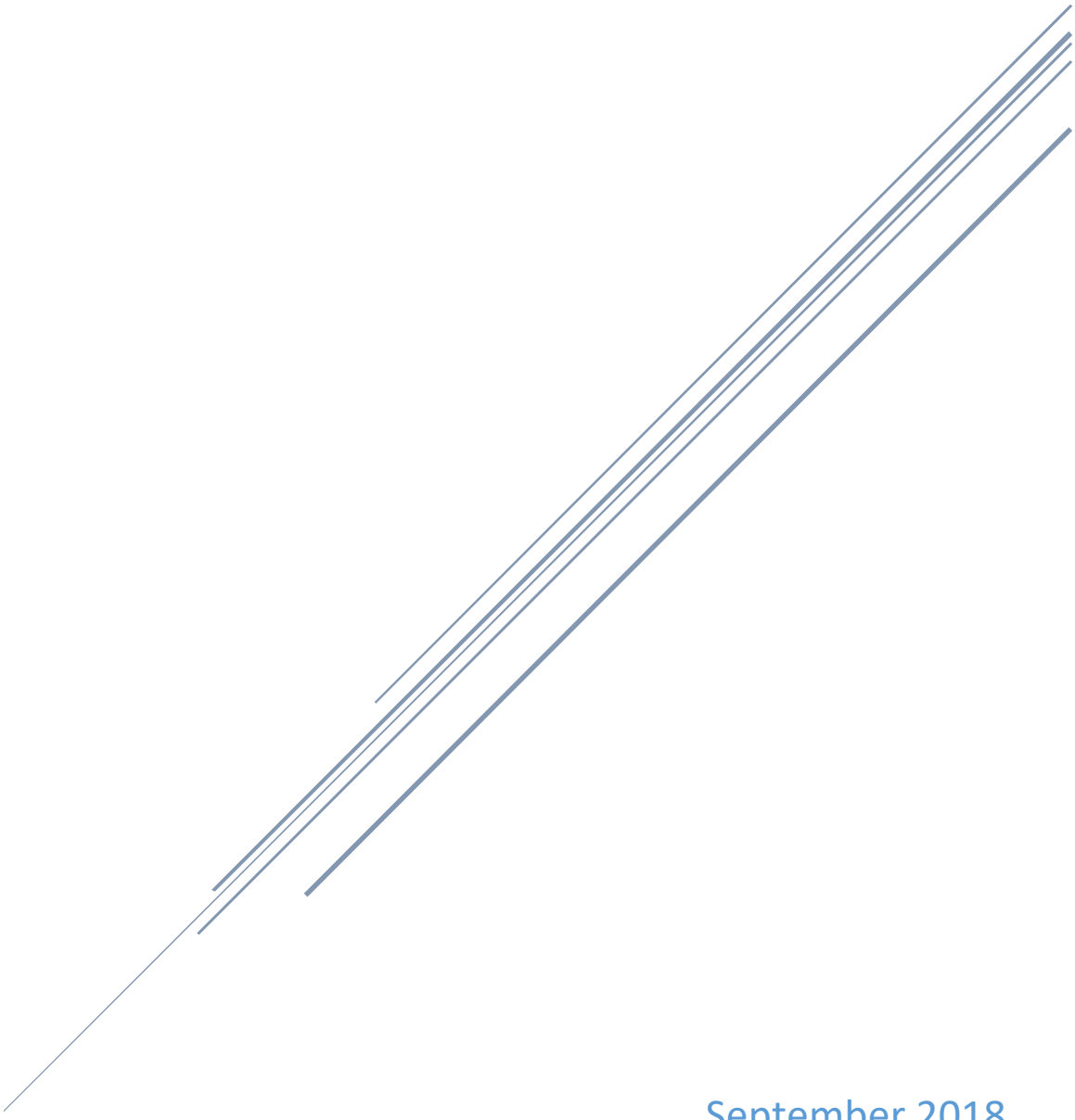
POLICY WORKING GROUP STRATEGIC PLAN

Chair: Chetrice Mosley | Co-Chair: Tracy Barnes



September 2018

Indiana Executive Council on Cybersecurity

Policy Working Group Plan

Contents

Committee Members

Committee Members

Name	Working Group Representation	Workgroup Position	IECC Membership Type
Lt. Governor Chief of Staff Tracy Barnes	Policy Co-Chair	Co-Chair	Voting
Chetrice Mosley	Policy, Cyber Summit, and Strategic Resources Chair	Chair	IECC Director
John Hammond	Governor's Office	As Needed	Voting
Micah Vincent	Governor's Office	As Needed	Voting Proxy
Superintendent Doug Carter	Government Services Chair	Full Time	Voting
Owen LaChat	Finance Chair	Full Time	Voting
Mark T. Maassel	Energy Chair	Full Time	Voting
John Lucas	Water/Wastewater Chair	Full Time	Voting
Joni K. Hart	Communications Chair	Full Time	Voting
Mark A. Lantzy	Healthcare Chair	Full Time	Voting
Director Danielle Chrysler	Defense Industry Chair	Full Time	Voting
Secretary Connie Lawson	Elections Chair	Full Time	Voting
Secretary Jim Schellinger	Economic Development Chair	Full Time	Voting
Commissioner Fred Payne	Workforce Development Chair	Full Time	Voting
CIO Dewand Neely	PII Chair, Cyber Sharing Chair, Pre- to Post-Incident Co-Chair	Full Time	Voting
Stephen A. Key	Public Awareness and Training Chair	Full Time	Voting
Executive Director Bryan Langley	Emergency Services and Exercise Chair	Full Time	Voting
MG Courtney Carr	Pre- to Post- Incident Chair	Full Time	Voting
Attorney General Curtis Hill	Legal/Insurance Chair	Full Time	Voting
Rhonda Cook	Local Government Chair	Full Time	Voting
Chuck Cohen	Government Services Chair Proxy	As Needed	Voting Proxy
FBI Assistant Special Agent in Charge John Davidson	Government Services Co-Chair	As Needed	Non- Voting

Tom Fite	Finance Co-Chair	As Needed	Advisory
Robert I. Richhart	Energy Co-Chair	As Needed	Voting Proxy
Jon F. Weirick	Water/Wastewater Co-Chair	As Needed	Voting Proxy
Daniel J. Solero	Communications Co-Chair	As Needed	Voting Proxy
Mitchell Parker	Healthcare Chair Proxy	As Needed	Advisory
Jacob Butler	Healthcare Co-Chair	As Needed	Advisory
Kyle Werner	Defense Co-Chair	As Needed	Voting Proxy
Beth Dlug	Elections Co-Chair	As Needed	Voting Proxy
David Roberts	Economic Development Chair Proxy	As Needed	Voting Proxy
Jeff Tucker	Workforce Development Chair Proxy	As Needed	Voting Proxy
Dr. John Keller	Workforce Development Co-Chair	As Needed	Advisory
Ted Cotterill	PII Chair Proxy	As Needed	Advisory
Valita Fredland	PII Co-Chair	As Needed	Advisory
Robert Dittmer	Public Awareness and Training Co-Chair	As Needed	Voting Proxy
Carlos Garcia	Emergency Services and Exercise Co-Chair	As Needed	Advisory
Joe Romero	Emergency Services and Exercise Co-Chair Proxy	As Needed	Advisory
Tad Stahl	Cyber Sharing Chair Proxy	As Needed	Advisory
Ronald W. Pelletier	Economic Development and Cyber Sharing Co-Chair	As Needed	Voting
Col. Jeffery Hackett	Pre- to Post- Incident Chair Proxy	As Needed	Voting Proxy
Douglas Swetnam	Legal/Insurance Chair Proxy	As Needed	Voting Proxy
Stephen Reynolds	Legal Insurance Co-Chair	As Needed	Advisory
Stephanie Yager	Local Government Co-Chair	As Needed	Voting
Scott Miller	Strategic Resources Co-Chair	As Needed	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - National Governors Association Whitepapers
  - State-to-State Examples
  - INSuRE Program (In Progress)
  - Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
  - National Conference of State Legislators Cybersecurity Taskforce Resources and Whitepapers

- **Research Findings**
  - In our research, we were unable to find a comprehensive, deep analysis of federal and state policy around cybersecurity since 2011 which included not just legislation that passed, but legislation that failed as well.
  - The INSuRE project develops a partnership among Centers of Academic Excellence in Information Assurance Research (CAE-R), the National Security Agency (NSA), the Department of Homeland Security, and other federal agencies in order to design, develop and test the research network. INSuRE is a self-organizing, cooperative, multi-disciplinary, multi-institutional, and multi-level collaborative research project that can include both unclassified and classified research problems in cybersecurity.
  - The mission of the National Conference of State Legislators Cybersecurity Task Force is to engage members in policy discussions, educate members and extend networking opportunities to legislative leaders on cybersecurity issues through a series of well-defined programs, webinars on key definitions and critical cyber policy issues as well as supporting private-public networks. The lifespan of this task force would be two years with the option to extend for one additional year.

- **Working Group Deliverable**
  - Complete an analysis of federal policy and state policies related to cybersecurity in the last 5 years.

- **Additional Notes**
  - There is currently Indiana Legislation being proposed (HB1112) that the Policy group is aware. The Council will continue to track this and any additional state legislation that may happen this year.

- **References**
  - Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* - https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
  - INSuRE Program - http://insurehub.org/
  - National Governors Association - https://www.nga.org/cms/home
  - The memo, State Cybersecurity Budgets, provides a brief review of how states budget financial resources for cybersecurity and the current levels of funding in many states.

- **National Conference of State Legislators**
  - Conversation Guide: Executive Branch, Legislative Branch and Higher Education http://www.ncsl.org/documents/taskforces/NCSL_Cybersecurity_Conversation_Guide.pdf
  - Cybersecurity Legislation 2017
  - Data Security Laws for State Government
  - Statewide Chief Information Security Officers
  - Statewide Cybersecurity Task Forces
  - Cyber Education and Training
  - State Cybersecurity Training for State Employees
  - NCSL Law, Criminal Justice and Public Safety Standing Committee Policy on Homeland Security
  - Identity Theft Statutes
  - Security Breaches
  - Cybersecurity Legislation 2016
  - Computer Crime Statutes
  - Data Disposal Statutes
  - Spyware Statutes
  - Phishing Statutes
  - State Efforts to Protect the Electric Grid, April 2016 (NCSL report)
  - "Luring Cybersecurity Is Big Business," Sept. 2015 (article)
  - "States Must Have Cybersecurity Plan," Dec. 2014 (blog post)

- **External Resources**
  - AT&T Security Budget Development (Oct. 31, 2017)
  - The Tech Jobs Conundrum: Tools for Bridging the Confidence Gap (Sept. 2017)
  - Cybersmart Buildings: Securing Your Investments in Connectivity and Automation (Feb. 2017)
  - 2016 National Association of State Procurement Officials Cyber Liability Insurance whitepaper
  - 2016 NASCIO Cybersecurity Study
  - Congressional Cybersecurity Caucus
  - MS-ISAC (Multi-State Information Sharing & Analysis Center)
  - U.S. Department of Homeland Security, Cybersecurity Division
  - "House Set to Push Creation of National Commission on Security, Digital Integrity," Feb. 26, 2016 (blog article)
  - "Administration Announces Cybersecurity National Action Plan," Feb. 11, 2016 (blog article)
  - "What Federal Cybersecurity Legislation Means for the States," Nov. 13, 2015 (blog article)
  - Cyber Supply Chain Security and Potential Vulnerabilities within U.S. Government Networks, June 15, 2015

- **Federal Activities**
    - Cybersecurity Legislation in 115th Congress (March 16, 2017)
    - S. 516 State Cyber Resiliency Act Bill Summary (March 10, 2017)
    - HR 1224 is a new bill on the NIST cybersecurity framework. (March 6, 2017)
    - CISA Law: Section (C) Authorization for Sharing or Receiving Cyber Threat Indicators or Defensive Measures (March 6, 2017)
    - Cybersecurity Legislation in the 115th Congress (March 15, 2017)

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. In Indiana, as state legislation regarding cybersecurity has come up in the last several years, the appropriate state agency has provided resources as needed.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. N/A

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. An education on the topic of cybersecurity with policy makers is needed on a local, state, and federal level.
    b. There are many states that have addressed a variety of cybersecurity topics through legislation. These examples are not easily found collectively and objectively. That is why the IECC is working with partners to conduct primary research and analysis of all state and federal policy that has occurred since 2011.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. N/A

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. The memo, State Cybersecurity Budgets, provides a brief review of how states budget financial resources for cybersecurity and the current levels of funding in many states.
    b. National Conference of State Legislators - http://www.ncsl.org/ncsl-in-dc/task-forces/task-force-on-cybersecurity.aspx

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. National Governors Association Whitepapers
    b. State-to-State Examples
    c. INSuRE Program (In Progress)
    d. Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. The National Conference of State Legislators Cybersecurity Taskforce provides policy makers a variety of resources online.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Complete an analysis of federal policy related to cybersecurity since 2011 and any federal acts that affect cybersecurity today.
    b. Complete an analysis of state policies the last five years that have passed or been debated.

c. Provide as-needed and appropriate input to all policy recommendations presented by other IECC committees and working groups or are being discussed nationwide.
d. Increased understanding and awareness of cybersecurity threats with state and local policy makers.
e. Assist in providing policy guidelines that encourage safer municipality, corporate, and personal practices that protect the state and constituents.
f. Utilize resources allocated to the council for policy tracking and monitoring, especially through university partnerships.

9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?

a. Help state legislators and local government officials understand and address the growing security risk posed to Indiana and its various sectors.

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

a. N/A

11. What do we need to do to attract cyber companies to Indiana?

a. N/A

12. What are your communication protocols in a cyber emergency?

a. N/A

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. N/A

Deliverable: Policy Research Report

Deliverable: Policy Research Report

General information

1. **What is the deliverable?**
    a. State and federal research report on cybersecurity legislation

2. **What is the status of this deliverable?**
    a. Complete

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☒ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☒ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable:

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Compiling the policies and legislation that have been introduced since 2011 from all 50 state legislatures and Congress so that Indiana has material and other policies to reference in reviewing policy recommendations.

6. **What metric or measurement will be used to define success?**
    a. Completion of an analysis of all 50 states and federal legislation.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. IECC's committees and members

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. N/A

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None

12. **Who should be main lead of this deliverable?**
    a. IECC Director

13. **What are the expected challenges to completing this deliverable?**
    a. Being able to complete a comprehensive analysis with limited resources and time.

Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability**?
    a. Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Select a resource to complete initial research report	Cybersecurity Program Director	100%	January 2018	Selected INSuRE Partner
Conduct research and create a tool to use for future policy analysis	INSuRE Program Partner: University of Alabama	100%	February – April 2018	Cybersecurity Program Director will serve as the Technical Director of the project
Provide Lt. Governor's Office with update on project	Cybersecurity Program Director	100%	March 2018	
Final report and tool completed	INSuRE Program Partner: University of Alabama	100%	April 27, 2018	
Provide IECC with final report and access to tool	Cybersecurity Program Director	0	August 2018	
Update table, additional analysis, and executive summary of changes	IECC approved intern (in-state or public/private partner) or university partnership	0	Once a year	Oversight by Chair and Co-Chair of IECC Policy Working Group
Present IECC with updated executive summary and tool	Cybersecurity Program Director	0	Once a year	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
2.5 FTE	1 FTE	Research and Policy	Grant, public, or private contribution	State of Indiana	The FTEs is expected to be the students to assist with research a few months a year and the Cybersecurity Program Director providing guidance.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Airtable Tool	As the policy collection and sharing grows, there may be a need to add more records beyond the free version and use the advanced features	$10-20 per month depending on upgrade		State of Indiana		

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. As the IECC considers possible policy recommendations, it is imperative that we understand what policy has been discussed, passed, and failed in all 50 states and at the federal level. This will better inform our recommendations, and any that do go before the legislature will likely be more successful because the state will have learned from others. There is no report or tool currently available that comprehensively looks at all cyber policy introduced in all 50 states. This will not only be of benefit to Indiana but other states as well.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. As policy is being discussed, the State of Indiana does not want to pass any legislation that may have an unintended consequence that would increase the cybersecurity risks or impact the investigation of cybercrime. It would be difficult to estimate the costs of the risk reduction.

19. What is the risk or cost of not completing this deliverable?

a. The largest risk of not completing this deliverable is creating a policy that is not well informed, and then unintended consequences occur that would increase the cybersecurity risks or impact the investigation of cybercrime.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completion of the policy research will be one metric. Equally important is that the research and possible tool is useful for our policy efforts.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No

22. **Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
    a. Yes
    b. **If Yes, please list states/jurisdictions**
        i. No state has a publically published review of all cyber legislation introduced since 2011. One could assume those states have had a difficult time moving cyber policy forward, or have not been successful at doing so, and could have benefited from the lessons learned in this type of research project.

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. The scope of the project is so large that there is a likelihood that some policies have been missed.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    a. No

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. A resource should be devoted to updating this tool and analysis at least once a year so the information does not become stale and can continue to be useful.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. The Policy Working Group Chair has been working with the INSuRE program to complete the initial report and tool.

27. **Can this deliverable be used by other sectors?**
    a. Yes
    b. **If Yes, please list sectors**
        i. All sectors and all committees/working groups.

Communications

28. **Once completed, which stakeholders need to be informed about the deliverable?**
    a. IECC members, IECC leadership, Governor's Office, legislators and their staff, lobbyists, state agency policy directors, sector associations, key national associations, and other state partners

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None as of now.

Evaluation Methodology

Objective 1: IECC and partners will develop a report of state and federal cybersecurity legislation by August 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- INSuRE Cyber Policy Final Report

IECC Policy Working Group

INSuRE Cyber Policy Final Report

Spring 2018

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

Adam Alexander aha0007@uah.edu
Paul Graham pag0006@uah.edu
Eric Jackson eaj0010@uah.edu
Bryant Johnson bej0003@uah.edu
Tania Williams tw0063@uah.edu

Cybersecurity Capstone - IS692 - Spring 2018
University of Alabama in Huntsville
301 Sparkman Drive, Huntsville
AL, United States of America 35899

***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 of Indiana in understanding its 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 cyber security 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.**

***Index Terms*—cybersecurity, policy, legislation, United States, states, Federal Government**

I. Introduction

A. Problem Statement

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. This compact includes a commitment to build cybersecurity governance, to prepare and defend the state from cybersecurity events, and to grow the nation's cybersecurity workforce [1]. However, meeting such a commitment is difficult without an understanding of existing attempts of cybersecurity legislation from across the country.

B. Purpose Statement

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

- What policy has been passed successfully/unsuccessfully in other states from 2011 to present?
- Who were the supporters of the policy?
- What type of support did the proposed policy receive, and if it did not pass, why?
- How can such information be presented to Indiana stakeholders in a clear and concise manner?
- What trends are evident among the states regarding cybersecurity policy?

By providing the State of Indiana with a searchable database of successful and failed legislation from across the country, we will supply the state with information needed to create successful and effective cybersecurity legislation.

C. Motivation

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 relevant to the strategic vision" of the 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. 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.

Perhaps the greatest concrete problem regarding the research is the scope. It is challenging to do a thorough examination of all the states. We addressed the scope of our work by dividing the workload among the group members.

In order to ensure that all policy was evaluated systematically, we developed a data collection form for the team to use. Additionally, we organized the research by the 20 existing 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 legislations 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 national cyber-related policies provides a valuable resource for other states as they seek to improve their cybersecurity posture.

II. LITERATURE REVIEW

A. Need for Cybersecurity Legislation

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 [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]. This threat of cyber-attack is not limited the federal government. Individual states also must consider the threat of weak cybersecurity.

States, which hold databases full of health records, driving records, criminal 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]. On top of this, states also bear much of the burden of regulation; however, as Sales states, law and policy of cyber-security 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 interoperability perspective" [7]. Alternatively, he notes the difficulty of crafting the standards to begin with, citing the failed GRID Act of 2010, which the federal legislative branch could not agree on how the grid'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 is it necessary to build on the experience of other states and to understand national policy trends.

B. Trend Analysis Approaches

As Godara notes, crime has seen a "revolutionary shift from the main actor, 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 federal laws 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 cybersecurity, they do not provide an approach to handling the large volume of legislation relating to cybersecurity produced by individual states from 2011 to present.

III. PROGRESS

A. Plan Overview

1) Major Tasks:

- Performed search for state and federal bills.
- Classified state and federal bills.
- Collected metadata and input into collect tool.
- Identified cybersecurity trends from collection tool.
- Created a report detailing trends.

2) Contribution of Tasks to the Overall Utility of the Work: Each task was designed to bring us closer to solving our problem (help the State of Indiana create successful cybersecurity policies). After we classified the state bills, we collected metadata for each one. This task allowed us to

create trends based upon the metadata (passed/failed, detractors/supporters, etc.). Once these trends were identified, then a report was crafted to help committees for the State of Indiana come up with cybersecurity bills that are necessary to protect Indiana's interest and have a higher chance of passing.

3) Deliverables:

- Proposal
- Bi-weekly presentation
- Midterm Presentation
- Midterm Report
- Airtable sortable table with metadata including bill location [https://airtable.com/shrCcYzKJGH1jyvrx]
- Final Presentation
- Final Report

B. Schedule

- 2/1/2018 Met with the technical director and determined goals for the project
- 2/6/2018 Discussed draft proposal with Technical Director
- 2/9/2018 Submitted final proposal
- 2/9/2018 - 3/2/2018 Searched for policies and classification
- 3/2/2018 Prepared midterm report
- 3/2/2018 - 3/23/2018 Completed metadata upload
- 3/24/2018 - 4/13/2018 Identified trends and analysis
- 4/13/2018 - 4/27/2018 Created final report
- 4/27/2018 Submitted final report

C. Detailed Plan

1) Data Collection: After meeting with our technical director, we surveyed academic journals searching for any existing research on the topic. We also reviewed sample legislation, taking note of the metadata provided in the legislation and determining how this data could best be recorded in our database.

After developing a tool for recording pertinent information from state websites, we divided the workload of data collection and started gathering our information.

2) Finding and classifying a bill: Each researcher examined digital archives to look for proposed legislation relating to cyber security. As stated before, each state usually had a digital archive of bills the researcher can look through using a keyword search. Once that location had been exhausted, secondary locations were searched. For each policy found, a certain amount of metadata was located within the policy and recorded. This included the following data:

- Researcher's name (who found the policy)
- Location it belongs to (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)

The included classifications below:

- 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 easy way for the end user to reference trends and policies when using the final document as reference. The groups were fine-tuned by the technical director to provide an easier form of classification and more usability.

3) Locating alternative sources for research: 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, the researchers utilized second party databases to collect policy information. These second party databases included sites such as *Find Law* and *Legiscan*.

4) Creating a collaborative database: While many tools were available for storing and managing our research, we sought one that would allow us to collaborate seamlessly and would allow us to share our data with end users without requiring specialized software or paid licensing. We also sought a product that was versatile enough to allow for linking fields together and even sharing data from one table to another. The tool also needed to have several sorting and filtering options. We found an online product called Airtable to meet our needs [11].

After deciding on a tool, we then had to finetune our database design. We listed the necessary fields and then organized them in a logical way to streamline the data entry process.

5) Importing Database Information: 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

- Description
- Political party affiliation
- Bill sponsor
- Link to vote count information

6) Trend Analysis: Our next step was to begin the preliminary analysis of our data.

a) By State: 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.

b) Vetoed Bills: 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.

c) Failed Legislation: 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.

d) Influence of Federal Legislation: While states are responsible 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.

e) Cybersecurity Pioneers: 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 exhibited steady policy creation were evidenced. The states showing consistent policy creation over time were determined to be cybersecurity pioneers.

f) Bipartisan Policy Creation: One of our primary goals in our 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.

7) Analysis of Results: After the trends were examined, then the following questions were addressed.

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

IV. RESULTS

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.

A. 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.

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

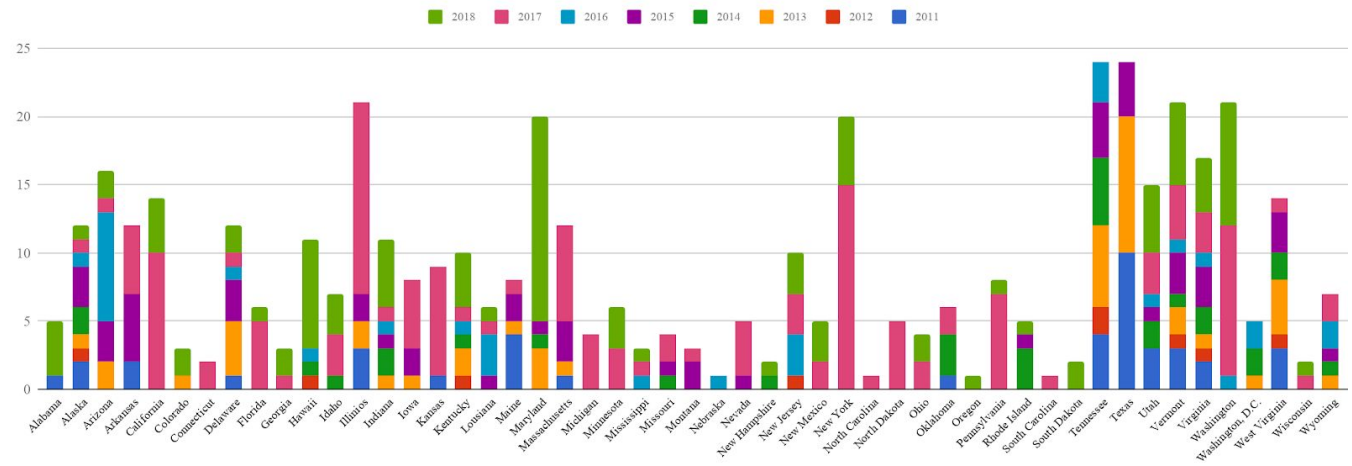


Figure 1. The quantity of policies developed by each state per year between 2011 and 2018.

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 cybersecurity 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.

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		
	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.

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).

B. 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 Cybersecurity 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 cyber security 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].

C. 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.

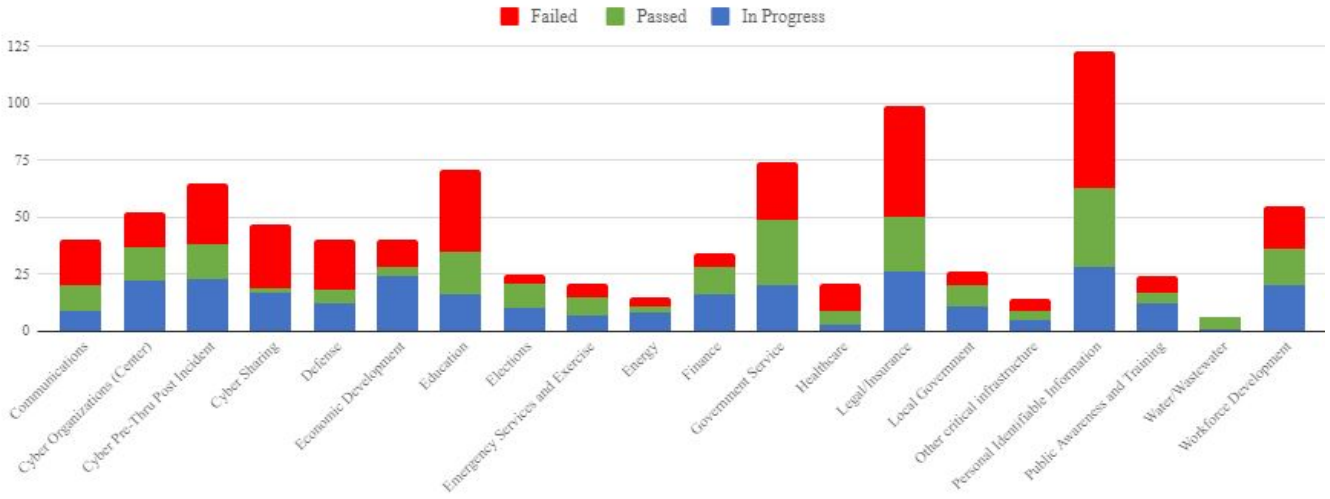


Figure 2. The quantity of each policy type surveyed that is either still in process, was passed into law, or was failed for any reason.

The label "In Progress" are for classifications that are identified to be introduced 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 policies 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 exercise, 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.

D. 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 seperate 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

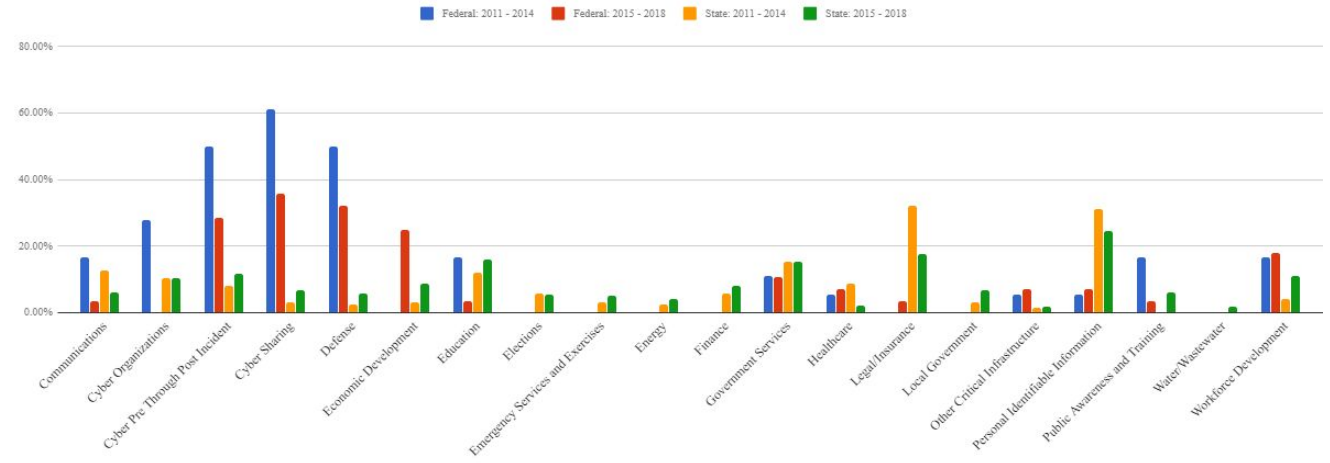


Figure 3. The percentage of state and federal policies introduced in 4 year periods (2011-2014, and 2015-18) that deal each surveyed category.

in Cyber Sharing between organizations. Federal legislation in those categories are consistently higher than all other categories 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 at all.

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

E. 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 regularity of policy creation. Pioneering states were Alaska(12), Arizona(16), California(14), Delaware(12), Hawaii(11), Illinois(21), Indiana(11), Maryland(20), Massachusetts(12), New York(20), Tennessee(24), Texas(24), Vermont(21), Virginia(21) Washington(21), and West Virginia(14) These states appear to be in 3 different classifications.

1) Early policy creation; however the state has not produced much legislation of late: In this category, the state created several policies earlier than 2014 and then less after 2014. These states have dropped in their proactive approach 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 Tennessee, Texas, and West Virginia meet this criteria. Even though their number of policies are high, their concern for cybersecurity seems to have lessened.

2) 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 cyber security 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).

3) Steady policy creation: These high-producing policy creators consistently created bills over the sample years (2011-2018). As they consistently produced more cyber security 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.

F. Bipartisan Success

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 sponsorship 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, Washington, 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.

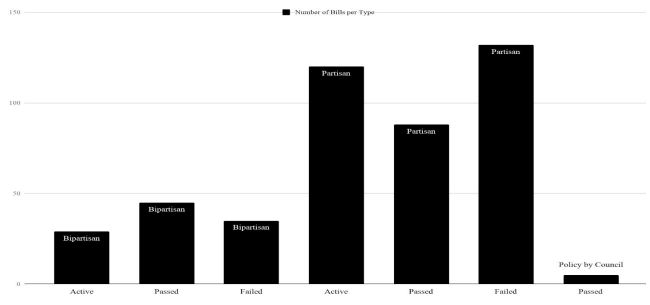


Figure 4. Success of state level bipartisan legislation attempts as opposed to partisan legislation attempts.

This data is being stored at the following link using Airtable. Please follow the link below to view the tool [11].

https://airtable.com/shrCcYzKJGH1jyvrx

V. Challenges

A. 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 their search.

B. 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.

C. 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 additional direction. The original bill and the following bills must be linked in the research also.

VI. Conclusion

Excluding federal legislation and active legislation, we found 305 examples of state level legislation relating to cyber security. 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 with education.

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 legislation's chance of 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 bipartisan 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.

VII. 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 research 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 legislation. An example of this future work could be in the area of workforce development. 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 legislators when crafting legislation. By surveying bill sponsors, researchers could identify key barriers to cybersecurity legislation, allowing policy makers the ability to better craft and propose bills. Also, researchers could compare failed legislation from one state to similar successful legislation in another state to determine why similar legislation failed in one state but found success in another.

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/d7c701a94f8c8d9685b93203add71fee?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," *California Legislative Information*, Oct. 11, 2017. [Online]. Available: http://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201720180AB1306
[14] Brown, Edmund G. Jr., "Governor's Veto Message," *California Legislative Information*, Oct. 14, 2017. [Online]. Available: http://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?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-Vetoed.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

TEAM INFORMATION

A. Biographical Sketches

Adam Alexander received his B.S degree in computer science from William Paterson University in Wayne, NJ in 2012. He holds a current Security+ certification. He is in his second year at the University of Alabama in Huntsville (UAH) pursuing a Master of Cybersecurity: Computer Science Track and is set to graduate in May of 2018. Alexander worked for one year as a systems administrator at a software company called Advent. The following three years were spent at MFX Fairfax working as computer technician and eventually being promoted to VDI technician. He has recently interned for TSMO's Army Red team and has participated in several Pen-testing operations.

Paul Graham received his B.S.B.A. degree in management from UAH in 2010. He holds current Security+ and Network+ certifications. He is pursuing a Master of Cybersecurity: Business Track and is set to graduate in May of 2018. Over the last seven years, Graham has worked as a government contractor for the D.O.D. Missile Defense Agency (MDA) in various IT positions. For the last two years, he has been a network design and implementation engineer and collaborated on solutions to improve the MDA's network security posture enterprise-wide. For three years before that, he provided account administration for multiple network domains.

Eric Jackson received his B.S. degree in Computer Science/Software Engineering from the University of Central Florida (UCF) in 2001. He holds a current Security+ certification as well as multiple certifications from Microsoft including Developer of Web Applications, Application Lifecycle Management, and SQL server. He is pursuing a Master of Cybersecurity from UAH with an emphasis on Computer Science.

Jackson worked for a government contractor in Florida for seven years developing simulators for the military. In 2008 he moved to Alabama and has worked as a contractor for NASA since. He is the development team lead, and his duties range from mentoring, server management (IIS), software development/architecture, and interacting with the

customers and government representatives. For the past several years, security has taken a more prevalent role in development. He is responsible for navigating policies, mitigating security scans, and providing a solid framework for use security in the applications.

Bryant Johnson received his B.S. degree in Computer Engineering from UAH in 2016. He also holds a current Security+ certification. He is a CyberCorps: Scholarship for Service student pursuing a Master's in Cybersecurity: Computer Engineering Track at UAH. His experience includes electronics, computer hardware, networking, software design and development.

Currently, Johnson works as a government civilian Computer Engineer for the Aviation and Missile Research, Development, and Engineering Center (AMRDEC) in Huntsville, Alabama, where he performs failure analysis on integrated circuits.

Tania Williams received her B.S. degree in English and professional writing from the University of North Alabama (UNA) in 1994, her Master of Education degree from UNA in 2000, and her Education Specialist Degree in Teacher Leader from UNA in 2015. She is currently pursuing a Master of Cybersecurity from UAH and holds a current Security+ certification.

Williams works for UAH's Center for Cybersecurity Research and Education as a research scientist assisting with the development of cybersecurity curriculum for various cybersecurity camps, including camps at the US Space and Rocket Center (US Cyber) and at UAH (GenCyber). She also is a teacher at Lauderdale County High School, where she teaches cybersecurity, robotics, and English. She is a CyberPatriot coach, a recent Teacher of the Year recipient, and a Fund for Teachers Fellow. Additionally, she has experience teaching on the college level, having served as an associate professor at Northwest Shoals Community college and Faulkner University.

B. Team Tasking

Team members assumed multiple roles to successfully achieve the goals of the project; regular communication of the project's goals was required from all member. Duties included providing expertise, completing deliverables, and documenting the process. While specific tasks varied throughout the course, each person contributed to the overall project objectives by following the outlined detailed plan on assigned datasets:

- Adam Alexander: Alabama, California, Colorado, Connecticut, Delaware, Florida, Georgia
- Paul Graham: Alaska, Arizona, Arkansas, Delaware, Hawaii, Idaho, Indiana, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, U.S. Congress
- Eric Jackson: Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico
- Bryant Johnson: New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota
- Tania Williams: Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming, Washington D.C.

Notably, individuals performed tasks and filled extra roles where responsibility was not specifically dictated. Eric Jackson and Adam Alexander assumed the role of liaisons to the technical director and communicated progress/objectives to the course professor. Tania Williams led the documentation effort, performed the literature review, and established the collaborative database. Paul Graham and Bryant Johnson supported the document review, data management, and analysis.