



2022 CYBER LEGISLATION IN REVIEW

A Year Analyst Report from The Institute for
Critical Infrastructure Technology

Author: Shaila Rana, PhD,
Contributing Researcher, ICIT

ICIT | Institute for Critical
Infrastructure Technology
The Cybersecurity Think Tank

2022 Legislation in Review

January 2023

Copyright 2022, The Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

Contents

Introduction.....	3
Federal Legislation.....	3
The Strengthening American Cybersecurity Act of 2022:.....	3
Significance of The Strengthening American Cybersecurity Act of 2022.....	4
Cyber Incident Reporting for Critical Infrastructure Act of 2022.....	4
Significance of Cyber Incident Reporting for the Critical Infrastructure Act of 2022	5
Better Cybercrime Metrics Act	5
Significance of Better Cybercrime Reporting Act	6
National Cybersecurity Preparedness Consortium Act.....	6
Significance of the National Cybersecurity Preparedness Consortium Act	7
Federal Rotational Cyber Workforce Program Act	7
Significance of the Federal Rotational Cyber Workforce Program Act.....	8
State and Local Cybersecurity Improvement Act	8
Significance of State and Local Cybersecurity Improvement Act	9
State Legislation	10
Recommendations.....	11
Summary.....	12
References.....	13

Introduction

Cybersecurity legislation is vital to address the growing number of cyberattacks that threaten the economic and national security of the United States. Consequently, 2022 was a significant year for cybersecurity legislation, with six major pieces of legislation signed into law. These laws focused on cyber incidents and ransomware attacks, reporting requirements, assigning cybersecurity responsibilities to CISA, the cybersecurity workforce, and state and local government cybersecurity programs. This paper addresses these significant pieces of legislation passed in 2022 at the federal level and cybersecurity legislation trends at the state level. The federal legislation discussed in this paper includes The Strengthening American Cybersecurity Act, the Cyber Incident Reporting for Critical Infrastructure Act of 2022, the Better Crimes Metric Act, the National Cybersecurity Preparedness Consortium Act, the Federal Rotational Cyber Workforce Program Act, and the State and Local Government Cybersecurity Act.

Federal Legislation

The Strengthening American Cybersecurity Act of 2022:

The Strengthening American Cybersecurity Act of 2022 is an important piece of cybersecurity legislation signed into law in March 2022. This act is also known as the Federal Information Security Modernization Act of 2022 (*S.3600 - Strengthening American Cybersecurity Act of 2022*). The goal of this legislation is to address cybersecurity threats against both critical infrastructure and the federal government of the United States. Ultimately, this act gives responsibilities to the Cybersecurity and Infrastructure Security Agency (CISA) to perform ongoing and continuous assessments of the federal government's overall cybersecurity posture. Moreover, this act details the accountabilities and responsibilities of federal agencies to address cybersecurity incidents, including ransomware attacks. Under this legislation, agencies have a specified time frame to determine if an individual is affected by a cybersecurity breach based upon a risk assessment. Agencies must provide written notice to individuals potentially affected by this incident (*S.3600 - Strengthening American Cybersecurity Act of 2022*). Overall, this act addresses reporting requirements as it deals with cybersecurity incidents and ransomware attacks. Furthermore, this act establishes an interagency council to standardize federal reporting of cybersecurity threats, a task force on ransomware attacks, and a pilot program to identify information systems vulnerable to incidents and ransomware attacks (*S.3600 - Strengthening American Cybersecurity Act of 2022*). Essentially, the Strengthening American Cybersecurity Act requires reporting and other actions to address cybersecurity threats, including providing information related to cyber incidents and ransom payments. The overarching mission of this law is to protect national security and enforce cybersecurity management. An important outcome of this law is the creation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

Significance of The Strengthening American Cybersecurity Act of 2022

Cybersecurity incidents have increased in both ubiquity and complexity as there is an increasing reliance on information technology. Opportunities for attackers continue to rise as they take advantage of misconfigurations, vulnerabilities, and security gaps that inevitably exist within IT architectures. The federal government is not immune to such attacks; instead, it is a prime target for attackers due to the sensitive nature of the information it holds. Furthermore, critical infrastructure is crucial to national security; subsequently, attackers may focus on attacks directed at disrupting communities. Thus, the Strengthening American Cybersecurity Act of 2022 addresses the rising threat and risks posed to the federal government, federal agencies, and critical infrastructure. This act attempts to address these cybersecurity incidents and ransomware attacks by creating reporting requirements to assist CISA in aggregating information to understand what these attacks are, what they look like, the attack vector, and defenses to stop future attacks. Another significant factor of this law that creates the Cyber Incident Reporting for Critical Infrastructure Act of 2022. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) creates accountability and responsibility for CISA to develop and implement regulations for reporting cyber incidents and ransomware payments.

Cyber Incident Reporting for Critical Infrastructure Act of 2022

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law by President Biden in March 2022. This legislation aims to improve cybersecurity and the security stance of the United States, similar to the Strengthening American Cybersecurity Act of 2022 (*H.R.5440 - Cyber Incident Reporting for Critical Infrastructure Act of 2021*). CIRCIA stems from the Strengthening American Cybersecurity Act of 2022 and gives responsibilities and accountabilities to the Cybersecurity and Infrastructure Security Agency (CISA). This act requires CISA to develop and implement regulations to report cyber incidents and ransomware payments. This act also details that CISA must deploy resources and assist victims suffering from cyberattacks (*H.R.5440 - Cyber Incident Reporting for Critical Infrastructure Act of 2021*). This legislation allows CISA to analyze incoming reporting to spot trends, patterns, and vital information surrounding cyber incidents and ransomware attacks. The data collected through this act enables CISA to share information with network defenders and warn victims of these attacks' nature. Consequently, the goal of CIRCIA is to protect critical infrastructure against cyber incidents and ransomware attacks that have severe economic and national security threats.

CIRCIA requires CISA to develop and implement regulations to report cyber incidents and ransomware attacks, including reporting ransom payments made to attackers. The benefits of these reporting requirements are that victims will receive assistance from government agencies to investigate the incident and provide remediation and incident response efforts. Highly trained investigators can respond to these cyber incidents through technical assistance, vulnerability mitigation, and incident recovery. In return, CISA will be able to receive timely information about cyber incidents, including the

actual incident, tactics, techniques, and procedures utilized in these cyberattacks. Since this act has been signed into law, CISA is gathering input from the public on the best approaches to implement these new rules and regulations. CISA is holding sessions to receive input on definitions and reporting requirements.

Significance of Cyber Incident Reporting for the Critical Infrastructure Act of 2022

Information is vital when it comes to addressing cyberattacks and cyber threats. Data collected from cyberattacks allow cybersecurity personnel to analyze and understand the ways in which attacks are conducted and any patterns that will assist in creating relevant security defenses. CIRCIA is an important piece of legislation aimed at aggregating data that can allow the federal government and network defenders to have crucial information surrounding cyber incidents and ransomware attacks. This law provides benefits in two ways: gathering information to create a deeper understanding of cyber incidents and aiding victims of cyber incidents. Timely reporting is another benefit of this legislation, as there will be requirements for a timeframe in which victims must provide information to CISA regarding a cyber incident or ransom payment. The timely reporting aspect of this law will allow CISA to have up to date information to understand the current attack vectors and trends in the current cyber landscape. As technology evolves and cybersecurity attacks and defenses evolve even faster, up to date and timely information is key to providing a solid defense against the plethora and ubiquity of cyberattacks and ransomware attacks that have been happening as of 2022. Overall, this law aims to protect critical infrastructure, which is a significant factor in upholding national security. However, this law can also be a strong motivator in the state and local legislative space to create similar requirements to be more inclusive of other industries.

Better Cybercrime Metrics Act

The Better Cybercrime Metrics Act was signed into law in May 2022 (*Congressman Blake Moore's Bipartisan Better Cybercrime Metrics Act, 2022*). This legislation, introduced in 2022, establishes cybercrime reporting mechanisms. The Better Cybercrime Metrics Act is an important step forward in addressing cybercrime (*S.2629 - Better Cybercrime Metrics Act*). Congress utilized public polling to find that cybercrime is the most common crime in the US and that the federal government lacks a comprehensive cybercrime data and monitoring mechanism. This act also addresses the rise in cybercrime that has been reported after the COVID-19 pandemic. The lack of data aggregation regarding cybercrimes leaves the US unprepared to combat cybercrime, which inevitably threatens national security and economic security (*S.2629 - Better Cybercrime Metrics Act*). The outcome of this law is to require the Attorney General to acquire, collect, classify, and preserve national data on criminal offenses, including cybercrime (*S.2629 - Better Cybercrime Metrics Act*). The Attorney General must develop a taxonomy first to categorize different cybercrimes that are commonly faced by industries, businesses, and individuals. The created taxonomy will be vital for the FBI to classify cybercrime in a

national incident-based reporting system. Stakeholders will also be included in developing this taxonomy, including CISA and the Department of Homeland Security, law enforcement, criminologists and academics, cybercrime experts, and business leaders. Examples of taxonomies that can be utilized to create a cybercrime taxonomy include those developed by non-governmental organizations, international organizations, academia, and other relevant entities (*S.2629 - Better Cybercrime Metrics Act*).

Significance of Better Cybercrime Reporting Act

Aggregating data is key to understanding cybersecurity threats and the nation's overall cybersecurity posture. Thus, the Better Cybercrime Reporting Act will allow the US to have a more comprehensive way to collect data about cybercrime and be able to monitor the amount, types, and effects of cybercrimes. As mentioned earlier, public polling indicates that cybercrime is the most ubiquitous and common form of crime, which is unsurprising in the pervasive nature of technology in society. Cybercrime affects a plethora of different entities, industries, and individuals within the US. Consequently, this threatens national security and economic security, which is now being addressed through the introduction of this legislation. The creation of a taxonomy is an important factor in this act. A taxonomy will result in categorizing cybercrimes to better organize data to understand patterns and threats. This law will provide a better view of the current state of cybercrime to understand future goals and objectives, such as what to invest in, how to address cybercrimes, future legislation, and the potential for national assistance to protect against cybercrimes.

National Cybersecurity Preparedness Consortium Act

The National Cybersecurity Preparedness Consortium Act was signed into law in May 2022 (*Bills signed: S. 497 and S. 658, 2022*). This act allows the Department of Homeland Security (DHS) to work with one or more entities to develop, update, and deliver cybersecurity training to support homeland security (*S.658 - National Cybersecurity Preparedness Consortium Act of 2021*). The Secretary of Homeland Security can work with one or more consortia to support efforts that aim to address cybersecurity risks and incidents (*S.658 - National Cybersecurity Preparedness Consortium Act of 2021*). In order to address cybersecurity risks and incidents, the DHS can seek assistance from different entities to provide training and education to state, tribal, and local first responders to prepare for cybersecurity risks and incidents. Other provisions of this legislation include developing and updating the curriculum in existing training and education programs related to cybersecurity risks and incidents. The DHS may also provide technical assistance services, training, and educational programs to support preparedness for cybersecurity risks and incidents.

This law outlines that the DHS may conduct cross-sector cybersecurity training, education, and simulation exercises for state and local governments, tribal organizations, critical infrastructure owners and operators, and private industry (*S.658 - National Cybersecurity Preparedness Consortium Act of 2021*). As its namesake indicates, this act aims to assist states and tribal organizations in cybersecurity preparedness and develop cybersecurity information sharing programs to disseminate security information related to risks and incidents. Cybersecurity defenses and prevention of incidents are essential; thus, this act incorporates the DHS' ability to provide cybersecurity risk and incident prevention plans. These prevention plans include emergency and continuity plans to assist state governments and tribal organizations (*S.658 - National Cybersecurity Preparedness Consortium Act of 2021*). An important factor of this legislation is to include metrics to measure the overall effectiveness of the activities outlined in this act and how the DHS executes this assistance, cybersecurity training, and assistance with cybersecurity planning. The DHS and the Secretary of the DHS may work with one or more consortia to provide training, developing and revising the curriculum, and technical assistance, services, training, and educational programs (*National Cybersecurity Preparedness Consortium Act of 2021*).

Significance of the National Cybersecurity Preparedness Consortium Act

Preparing for cybersecurity incidents is crucial to protecting national security, economic security, and security at the federal and state level. The attention to cybersecurity preparedness makes this legislation significant because it assigns responsibility to the DHS to assist state governments and tribal organizations to pay attention to and prepare for inevitable cybersecurity incidents. Cyberattacks do not just affect private industry; rather, state and local governments are frequent targets due to the nature of the information that they hold, the importance they play in communities, and the potential disruption they can cause to societies. Therefore, this legislation is a foundational way to coordinate a defense against and response to cybersecurity risks and incidents. The National cybersecurity Preparedness Consortium Act incorporates many different aspects, including cybersecurity training, cybersecurity information sharing programs, assistance with risk and incident prevention, and technical assistance services to achieve the overall goal of preparing the US against cyber risks and incidents. Overall, this legislation enables the DHS to utilize outside entities or consortia to conduct the requirements mentioned above to conduct cross-sector training, education, simulation exercises, and overall coordination to defend against and respond to cyberattacks.

Federal Rotational Cyber Workforce Program Act

The Federal Rotational Cyber Workforce Program Act was signed into law in June 2022. This legislation establishes a rotational cyber workforce program and allows certain federal employees to work at other agencies (*H.R.3599 - Federal Rotational Cyber Workforce Program Act of 2021*). This act authorizes an agency to determine whether a position involving IT, cybersecurity, or other cyber related

function is eligible for this rotational program (*H.R.3599 - Federal Rotational Cyber Workforce Program Act of 2021*). Specifically, this act aims to address the shortage of cybersecurity professionals working at the federal level. For this program to work, this act requires the Office of Personnel Management to issue a workforce operation plan, including policies, processes, and procedures to detail employees among rotational cyber workforce positions at other federal agencies (*H.R.3599 - Federal Rotational Cyber Workforce Program Act of 2021*). The Government Accountability Office is responsible for assessing the effectiveness of the program and the overall operation to see how many agencies participated and the overall experiences of employees that served in this rotational program (*H.R.3599 - Federal Rotational Cyber Workforce Program Act of 2021*).

Significance of the Federal Rotational Cyber Workforce Program Act

This legislation is significant because it addresses the shortage of cybersecurity professionals in the public and private sectors. This act aims to fill that gap of cybersecurity professionals by creating a rotational program in which federal agencies that are also experiencing this shortage can benefit from the expertise of IT and cybersecurity professionals. This law is significant because it may encourage agencies to see the benefits of having cybersecurity professionals and the advantages of protecting agency information architectures. The result of this rotational cyber workforce program may attract additional security professionals to federal agencies due to the interesting nature of the job and the potential for acquiring different skills and knowledge through a rotational program. Overall, this act is significant in addressing a shortage of cybersecurity professionals, attracting additional talent, and demonstrating the benefits of employing cybersecurity and IT professionals.

The Social Security Administration (SSA) has already begun creating a plan that includes participating agencies, program procedures including training, employee participation requirements, and approval of employee participation (*The President Signs S. 1097, the "Federal Rotational Cyber Workforce Program Act of 2021"*). The SSA has included provisions of their program, including training and education, career development, prerequisites for participation, performance measures, reporting requirements, and accountability devices (*The President Signs S. 1097, the "Federal Rotational Cyber Workforce Program Act of 2021"*). Hence, this demonstrates the significant impact this law has in addressing the current shortage of cybersecurity professionals.

State and Local Cybersecurity Improvement Act

The State and Local Cybersecurity Improvement Act was signed into law in June 2022 (*Press release: Bill Signed: s. 1097, S. 2520, and S. 3823, 2022*). This law requires CISA to establish state and local cybersecurity grant programs to address risks and threats to information systems of state, local, territorial, and tribal organizations (*H.R.3138 - State and Local Cybersecurity Improvement Act*). In

return, those seeking to apply for the grant must submit a cybersecurity plan for CISA to approve (*H.R.3138 - State and Local Cybersecurity Improvement Act*). This cybersecurity plan must include how the applicant will use funds to address cyber incidents, cyber risks, and cyber threats (*H.R.3138 - State and Local Cybersecurity Improvement Act*). CISA will grant funds for implementing, developing, or revising security plans. Additionally, CISA must establish a State and Local Cybersecurity Resilience Committee to advise and make recommendations to CISA on how to address cybersecurity risks and threats faced at the state, local, and tribal levels. Other requirements of this act include requiring CISA to maintain and develop a resource guide to identify, prepare, detect, protect against, respond to, and recover from cybersecurity risks and threats that must be made publicly available to state, local, and tribal organizations (*H.R.3138 - State and Local Cybersecurity Improvement Act*).

Significance of State and Local Cybersecurity Improvement Act

It is important to address the background that led to this law being introduced and enacted in 2022. State and local governments are prime targets for cyberattacks, and the ubiquity of cyberattacks has been increasing at an alarming rate. In 2020, ransomware attacks crippled state and local agencies, like the public regulation commission, library systems, and police departments (*The "State and Local Cybersecurity Improvement Act," 2022*). In 2021, ransomware attacks forced schools to close and continued to threaten police departments and other vital agencies (*The "State and Local Cybersecurity Improvement Act," 2022*). Consequently, this forced the government to put more effort into building robust cybersecurity defenses. This act aims to improve the ability of state and local governments to detect and defend against cyber risks, threats, and attacks.

The significance of this new law is that it pays attention to the important role that state, local, tribal, and territorial governments play in national security. This grant program can allow these organizations and entities to pay more attention to cybersecurity preparedness and defense against cyberattacks. This law requires CISA to develop a strategy to improve the cybersecurity of state, local, tribal, and territorial governments and find federal resources for cybersecurity purposes (*The "State and Local Cybersecurity Improvement Act," 2022*). Moreover, this law is significant because it provides a way in which these agencies can seek funds to address cyber risks and threats and seek guidance from CISA regarding cybersecurity plans. Thus, this act offers a monetary means to implement cybersecurity preparedness. Inevitably, this law will attract attention to the benefits, significance, and necessity of implementing cybersecurity programs and shows it is not just a federal responsibility to protect national security. Rather, it takes the coordination of many different entities and organizations to work together to create a strong defense. Ultimately, this law addresses the rise in cyber threats, such as ransomware attacks, and their detrimental and paralyzing effects on governments and organizations.

State Legislation

At the state level, many laws were introduced addressing state governments' cybersecurity. In 2022, there was a lot of legislation surrounding cybersecurity legislation that failed in many states; however, thirty-one major cybersecurity laws were voted on and passed. Cybersecurity legislation was voted on and passed in 2022 in the following states: Alaska, Arizona, California, Florida, Idaho, Iowa, Illinois, Kentucky, Louisiana, Maryland, Missouri, New Hampshire, New Mexico, Oklahoma, Rhode Island, South Dakota, Tennessee, Utah, Virginia, Washington, and West Virginia (*Cybersecurity Legislation 2022*).

The majority of cybersecurity legislation that passed at the state government level dealt primarily with cyber incidents and ransomware attacks. Ransomware attacks were detrimental not just to federal governments, but state and local governments were strongly impacted as well. Consequently, it is natural that at least nine pieces of legislation passed that addressed cyber incidents and ransomware attacks at the state level and where these state governments paid the most attention regarding security legislation. This trend is similar to what was demonstrated at the federal level, with three major laws being passed addressing the increase in cyber incidents and ransomware attacks.

State governments also focused on cybersecurity legislation that dealt with reporting requirements. These laws focused on creating reporting requirements that enabled state governments and state entities to understand where to report cyber incidents. For example, legislation passed in New Hampshire defined cybersecurity incidents and reporting incidents to the Department of Information Technology (*New Hampshire House Bill 1277*). This is a significant trend that was also found at the federal level, including requirements that require federal agencies to report cyber incidents and ransomware attacks to CISA. Thus, this was also implemented within state governments to enable entities to report cyber incidents and attacks to aggregate data and better understand how to protect against future attacks.

Another trend demonstrated at the state government level was cybersecurity legislation that dealt with the creation of security programs. Across the US, there were five pieces of state legislation that dictate what entities at the state level need to create a cybersecurity program to address cyber risks and threats. An example is Kentucky HB 474, which passed legislation stating that insurance agencies must develop and maintain a comprehensive written security program (*Kentucky House Bill 474*). Therefore, this demonstrates the increasing need and attention to having cybersecurity programs in place to address risks and threats appropriately and in a standardized manner.

Other cybersecurity legislation trends at the state level include cybersecurity laws that deal with the cybersecurity workforce gap, the security of elections, and security surrounding the insurance

industry. These pieces of cybersecurity legislation that were passed at the state level in 2022 stem from the increasing number of attacks that are being faced at the state and local government levels.

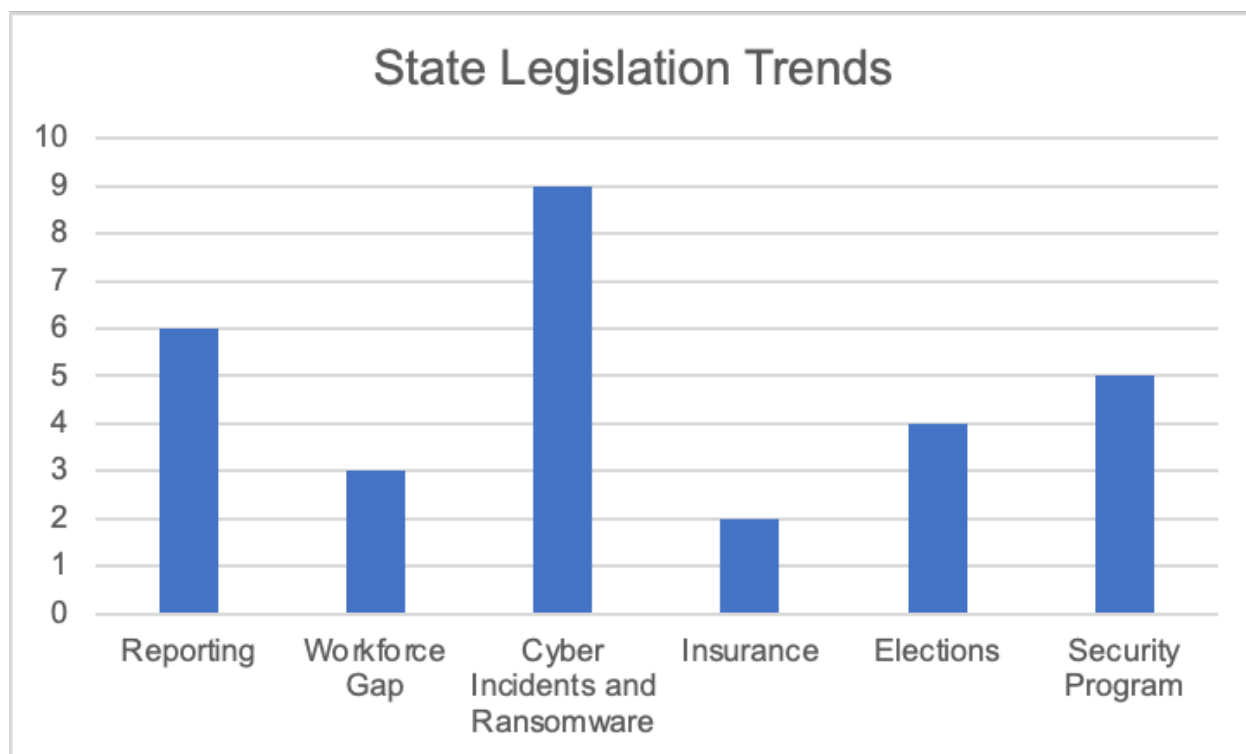


Figure 1: The number of passed state legislation by category

Recommendations

Cybersecurity legislation in 2022 focused on critical infrastructure, government agencies, and the responsibilities of CISA. This year's legislation also focused on the increased number of cyber incidents and the detrimental effect ransomware has on organizations in the public sector. Recommendations for future legislation in 2023 and beyond include continuing initiatives for critical infrastructure and federal and state governments. The data being reported to and collected by CISA should pave the way for key insights to create anti-cybercrime laws and consequences for cyber criminals to lower cyber incidents and ransomware attacks. The data collected by CISA will provide a better view and understanding of the current state of cybercrime to understand what sectors and controls should be invested in, how to warn people, and federal assistance for cyberattacks. Future laws focused on cybercrimes and the consequences of cybercriminals can serve as a deterrent for future cyber attackers. Although it is challenging to catch a cyber attacker, it may be useful to have future legislation in place that provides clear and severe penalties. These attacks should focus on the trends

observed as of 2022, including ransomware attacks and attacks aimed at affecting the availability of critical infrastructure and governmental organizations. As demonstrated in 2022, legislation focuses on addressing the gap found in the cybersecurity professional workforce. Thus, future legislation should further address this gap and create additional incentives to attract a cybersecurity workforce to participate in the public and private sectors. All in all, future legislation in upcoming years should address cybersecurity's role in daily life for US citizens, along with national and economic security.

Summary

In 2022, six major cybersecurity laws were passed, including the American Strengthening Act, the Cyber Incident Reporting for Critical Infrastructure Act, the Better Crimes Metric Act, National Cybersecurity Preparedness Consortium Act, the Federal Rotational Cyber Workforce Program Act, and State and Local Government Cybersecurity Act. The aforementioned legislation addresses cyber incidents, reporting requirements, a rotational cyber workforce program, and state and local government cybersecurity programs. These major pieces of legislation create a strong year for addressing cybersecurity requirements that continue to grow in importance throughout the years. State governments also passed various cybersecurity laws, with most laws focusing on cyber incidents and ransomware, reporting requirements, and security programs at the state level. With the increasing reliance on technology and IT systems for critical infrastructure and federal and state governments coupled with the growing cyberattacks and ransomware attacks, it is essential that legislation address these security risks. The outcome of legislation this year allows for the federal government to have a better understanding of the type of attacks occurring, the ubiquity of these attacks, and future data that will allow for crucial insights for how better to protect national and economic security in the United States.

References

- Alaska House Bill 3. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/AK/bill/HB3/2021>*
- Arizona Senate Bill 1598. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/AZ/bill/SB1598/2022>*
- California Assembly Bill 183. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/CA/bill/AB183/2021>*
- California Senate Bill 154. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/CA/bill/SB154/2021>*
- Congressman Blake Moore's Bipartisan Better Cybercrime Metrics Act. Representative Blake Moore. (2022, May 6). Retrieved November 27, 2022, from <https://blakemoore.house.gov/media/press-releases/congressman-blake-moores-bipartisan-better-cybercrime-metrics-act-signed-law>*
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA). Cybersecurity and Infrastructure Security Agency CISA. (n.d.). Retrieved November 27, 2022, from <https://www.cisa.gov/circia>*
- Cybersecurity Legislation 2022. National conference of State Legislatures. (n.d.). Retrieved November 27, 2022, from <https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2022637922035.aspx#:~:text=Require%20government%20agencies%20to%20implement,security%20incidents%2C%20including%20ransomware%20attacks>.*
- Florida House Bill 7055. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/FL/bill/H7055/2022>*
- Florida Senate Bill 1694. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/FL/text/S1694/2022>*
- H.R.3138 - State and Local Cybersecurity Improvement Act. (n.d.). Retrieved November 27, 2022, from <https://www.congress.gov/bill/117th-congress/house-bill/3138/text>*
- H.R.3599 - Federal Rotational Cyber Workforce Program Act of 2021. (n.d.). Retrieved November 27, 2022, from <https://www.congress.gov/bill/117th-congress/house-bill/3599>*
- H.R.5440 - Cyber Incident Reporting for Critical Infrastructure Act of 2021. (n.d.). Retrieved November 27, 2022, from <https://www.congress.gov/bill/117th-congress/house-bill/5440>*
- Idaho House Bill 621. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/ID/bill/H0621/2022>*

Iowa House Bill 719. LegiScan. (n.d.). Retrieved November 30, 2022, from
<https://legiscan.com/IA/bill/HF719/2021>

Kentucky House Bill 474. LegiScan. (n.d.). Retrieved November 28, 2022, from
<https://legiscan.com/KY/text/HB474/id/2512747>

Kentucky House Resolution 77. LegiScan. (n.d.). Retrieved November 30, 2022, from
<https://legiscan.com/KY/bill/HR77/2022>

Maryland Senate Bill 207. LegiScan. (n.d.). Retrieved November 30, 2022, from
<https://legiscan.com/MD/bill/SB207/2022>

Maryland Senate Bill 754. LegiScan. (n.d.). Retrieved November 30, 2022, from
<https://legiscan.com/MD/text/SB754/2022>

Maryland Senate Bill 812. LegiScan. (n.d.). Retrieved November 30, 2022, from
<https://legiscan.com/MD/text/SB812/2022>

Missouri House Bill 1878. LegiScan. (n.d.). Retrieved November 30, 2022, from
<https://legiscan.com/MO/text/HB1878/id/2585332>

National Cybersecurity Preparedness Consortium Act of 2021 . (n.d.). Retrieved November 27, 2022,
from <https://www.govinfo.gov/content/pkg/COMPS-16894/pdf/COMPS-16894.pdf>

New Hampshire House Bill 1277. LegiScan. (n.d.). Retrieved November 28, 2022, from
<https://legiscan.com/NH/bill/HB1277/2022>

New Mexico House Bill 2. LegiScan. (n.d.). Retrieved November 30, 2022, from
<https://legiscan.com/NM/bill/HB2/2022>

Rhode Island House Bill 7732. LegiScan. (n.d.). Retrieved November 30, 2022, from
<https://legiscan.com/RI/bill/H7732/2022>

Rhode Island Senate Bill 2809. LegiScan. (n.d.). Retrieved November 30, 2022, from
<https://legiscan.com/RI/text/S2809/2022>

S.2629 - Better Cybercrime Metrics Act. (n.d.). Retrieved November 27, 2022, from
<https://www.congress.gov/bill/117th-congress/senate-bill/2629>

S.3600 - Strengthening American Cybersecurity Act of 2022. (n.d.). Retrieved November 27, 2022, from
<https://www.congress.gov/bill/117th-congress/senate-bill/3600>

S.3600: Strengthening American Cybersecurity Act of 2022. (n.d.). Retrieved November 27, 2022, from <https://www.congress.gov/bill/117th-congress/senate-bill/3600/all-info>

S.658 - National Cybersecurity Preparedness Consortium Act of 2021. (n.d.). Retrieved November 27, 2022, from <https://www.congress.gov/bill/117th-congress/senate-bill/658/text>

The President Signs S. 1097, the “Federal Rotational Cyber Workforce Program Act of 2021.” Social Security Legislative Bulletin. (n.d.). Retrieved November 27, 2022, from https://www.ssa.gov/legislation/legis_bulletin_062122.html

The “State and Local Cybersecurity Improvement Act.” House Committee on Homeland Security. (2022, November 18). Retrieved November 27, 2022, from <https://homeland.house.gov/imo/media/doc/State%20and%20Local%20Cyber%20Act%20Fact%20Sheet.pdf>

The United States Government. (2022, June 21). *Press release: Bill signed: S. 1097, S. 2520, and S. 3823.* The White House. Retrieved November 27, 2022, from <https://www.whitehouse.gov/briefing-room/legislation/2022/06/21/press-release-bill-signed-s-1097-s-2520-and-s-3823/>

The United States Government. (2022, May 12). *Bills signed: S. 497 and S. 658.* The White House. Retrieved November 27, 2022, from <https://www.whitehouse.gov/briefing-room/legislation/2022/05/12/bills-signed-s-497-and-s-658/>

Utah House Bill 280. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/UT/text/HB0280/id/2515491>

Virginia House Bill 30. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/VA/bill/HB30/2022>

Virginia Senate Bill 764. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/VA/comments/SB764/2022>

Washington Senate Bill 5693. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/WA/bill/SB5693/2021>

West Virginia Senate Bill 529. LegiScan. (n.d.). Retrieved November 30, 2022, from <https://legiscan.com/WV/bill/SB529/2022>