Advances In Multidisciplinary & Scientific Research
A Multidisciplinary & Interdisciplinary Journal
Volume 8, No 3, September 2022 Series

Evaluating State Cybersecurity Laws and Regulations in United States

Yamcharoen P[1], Bayewu, A.[2], Ojo T.P[3] & Fatoye O.E[4]
[1]Washington University of Science and Technology, Vienna, VA, 22182, USA
[2]Northumbria University, New Castle, NE1 8ST, UK
[3] University of Indianapolis, Indianapolis, IN, 46227, USA
[4]Lead City University, Ibadan, Oyo State, Nigeria
E-mails: [1]ami.yamcharoen@wust.edu; [2]omowunmisesekinatf@yahoo.com; [3]titilikesyou@gmail.com
[4]olusolafatoye@gmail.com;

ABSTRACT

In the United States, cybersecurity laws and regulations are necessary to protect vital infrastructure, sensitive information or individuals' personal privacy. The present state of cybersecurity law and regulation at both national and local levels is assessed in this review paper. The report gives an overview of the key legislation and initiatives, analyses their efficiency, and reveals new trends. The research method comprises a thorough analysis of academic literature, government publications, official websites, legal sources, news items and experts' reports. The paper begins by pointing out the importance of cybersecurity in today's interconnected world, where cyber threats are constantly evolving and posing major risks to individuals, organizations and national governments. The report draws attention to studies which show that businesses have suffered financially and may face disruption in the core infrastructure as a result of cybercrime. Key legislation, such as the Federal Information Security Modernization Act, and the role of agencies such as the Cybersecurity and Infrastructure Security Agency (CISA), and the National Institute of Standards and Technology (NIST), are covered in the overview of federal cybersecurity legislation and regulations. The scope, effectiveness and implications of such national measures to address cyber security challenges shall be assessed in the evaluation. New trends in cybercrime legislation, such as an increase in data breach reporting requirements and a focus on security of essential infrastructures are identified in the review paper. It examines legislative efforts to strengthen cybersecurity capabilities in key sectors such as healthcare. Consideration shall be given to the strengths and weaknesses of the existing legal framework, as well as recommendations for strengthening cybersecurity laws and regulations.

Keywords: Cybersecurity Laws, Cybersecurity Regulations, Federal Legislation, State Initiatives, Data Breach Notification, Legislative Efforts.

Aims Research Journal Reference Format:
Yamcharoen P., Bayewu, A., Ojo, T.P. & Fatoye O.E. (2022): Evaluating State Cybersecurity Laws and Regulations in United States. Advances in Multidisciplinary and Scientific Research. Vol. 8. No. 3, Pp 47–56. www.isteams.net/aimsjournal.
dx.doi.org/10.22624/AIMS/V8N3P4

1. INTRODUCTION: AN OVERVIEW OF STRESS

Cyber security is now a key issue for today's integrated world, where digital technology plays an important role in many sectors of daily life, including government, trade, health care and communication. The urgent need for a strong cyber security framework has been underlined by the

increased dependence of ICT systems and proliferation of cyber threats. There is a geometric increase in the adoption of digital technology to improve an organization's cybersecurity. The importance of cybersecurity laws and regulations will help industries to protect their critical infrastructure and sensitive assets from data breaches, malware activities, and hacking from threat actors.

A framework to secure organization infrastructure will help the security team or stakeholders track internal and external organization levels of compliance with the state laws and regulations related to their industry. The security team and stakeholders will enforce that cyber laws and regulations regulate the activities of employees and third-party stakeholders in protecting the organization's network assets, infrastructure, and sensitive information from cyber-attacks and cyber threats. In this paper, importance of cyber security and its impact on individuals, organizations and economies and some critical industry cybersecurity state laws and regulations will be discussed, and a framework to protect the critical information of these organizations will be identified and discussed.

In cyber space, the threat environment is changing significantly and presents serious risks to confidentiality, integrity and availability of Digital Information. Hacks, data breaches, extortion attacks and identity theft have been used by cyber criminals and criminal actors to carry out several activities which lead to significant loss of revenue, reputational damage or interruptions in critical infrastructure. The worldwide average annual costs of cybercrime for businesses have risen by 29% in 2020 to $13.0 million per enterprise (Andronache, A., 2019). The need for effective cybersecurity measures to counter these risks is highlighted in this disturbing trend.

The digital age demands that sensitive data be protected at all costs. Individuals and organizations have huge amounts of private, financial or proprietary information stored in digitized formats that make them a convenient target for cyber criminals. The breach can have serious consequences, e.g., ID theft, monetary fraud or loss of business operations caused by the unauthorized disclosure of confidential data. For example, the breach of the Equifax database in 2017 exposed the personal information of approximately 147 million consumers, highlighting the devastating impact of such incidents (Satariano & Goldstein, 2017). For the protection of sensitive data and the protection of individual privacy, effective cybersecurity measures are essential.

In many sectors of the critical infrastructure, such as energy, transportation, health care and finance, a significant number of interconnected Digital Systems are relied upon. A disruption or compromise of these systems can have a significant impact on public safety, the economy stability and National Security. The potential for disruption of crucial services, disruptions in supply chains and loss of trust may be caused by the cyber-attacks aimed at vital infrastructure. For instance, in the face of a 2020 cyber-attack on America's Colonial pipeline that has led to fuel shortages along the Eastern seaboard, highlighting the vulnerability of critical infrastructure against cyber threats (Sangani, N., 2017). Cyber security is far more than an engineering concern; it also has important economic implications. Cyber incidents are likely to result in significant losses, which can range from actual costs for incident response, recovery and correction through indirect costs like reputational damage, loss of trust among customers or reduced productivity.

Cybercrime is estimated to cost the global economy 1 trillion dollars annually according to a report from the Center for Strategic and International Studies (Caron, M. S., 2019). Moreover, cybersecurity is an important aspect of national competitiveness given that business and investors are prioritizing a safe environment for the internet. Strong cyber security measures can help to foster innovation, drive economic growth and increase trust in digital transactions. This review is to assess the current state of cyber law and regulation in the United States. The purpose of the report is to provide an overall analysis of the current framework for legislation at national and state levels, as well as a review of relevant provisions, initiatives and new trends. This paper aims at identifying the strengths, weaknesses and areas of improvement in the regulation environment through a critical assessment of the effectiveness and adequacy of cybersecurity legislation.

2. LITERATURE REVIEW

A combination of federal initiatives and State Level efforts to deal with the emerging cybersecurity landscape is reflected in current USA laws and regulations. The coordination and direction of national efforts in cyber security is a crucial role played by Federal legislation such as FISMA and agencies like CISA. In parallel, to cope with regional challenges and the protection of consumer privacy and critical infrastructures, each State has adopted its own legislation. In order to strengthen the nation's cybersecurity defenses, legislative efforts are currently focused on trends that may arise such as notification of a data breach and securement of vital infrastructure.

2.1 Healthcare State Cybersecurity Laws and Regulations

There is a constant change in healthcare cybersecurity, and most organizations need help to comply with the rules and regulations. The healthcare regulatory bodies fine any organization that violates these rules. Unfortunately, it has been recorded that most businesses in this industry have paid millions of dollars as fines due to data breaches of client information. To provide quality healthcare, the organizations in this industry must ensure they have a capable and experienced cybersecurity expert to monitor and improve the organization's cybersecurity posture timely (Hasan, S. et. al., 2021). For healthcare businesses to keep their client safe while preventing data breaches and regulatory penalties, they need to comply with cybersecurity regulations, and below are the rules and regulations that cut across the healthcare industry in most states in the United States of America.

The Health Insurance Portability and Accountability Act allows the organization to shape its cybersecurity standards and best practices to meet the Health Insurance Portability and Accountability Act requirement. The HIPPA act requires healthcare institutions to share electronically protected health information with third parties in a secured and protected manner. The HIPP security rule is significant regulation for healthcare cybersecurity. The rule requires that a covered entity or an associate of a covered business entity abide by and follow the HIPAA security rule (Pipyros, K. et. al., 2018). However, the security rule is an open-ended process, and each healthcare institution will determine how it will be implemented in their organization. Most healthcare institutions are exposed to risk. It is essential to determine the risk level to understand better the risk and how it can be mitigated within the organization's cybersecurity framework. The security rule requires the healthcare institution to follow technical safeguards of electronically protected health insurance, administrative and physical protection of the institutional infrastructure and patient or client-sensitive information (Koch, 2016).

The United States Department of Health and Human Services (HHS) collaborated with the healthcare industry to enact the HHS 405(d) regulation. This task group was created to establish industry guidelines, processes, best practices, and methodologies that healthcare institutions can use to protect their organization's infrastructure and improve their cybersecurity. Their collaborative effort yielded a framework known as Healthcare Industry Cybersecurity Practices (HICP) to help healthcare institutions implement cybersecurity best practices. The HICP tracks the changes in the best practices for endpoint protection, network management, cybersecurity policies, vulnerability management, medical device security, and others (Ten, C. et. al., 2008).

The Health Information Technology for Economic and Clinical Health Act (HITECH) guidelines will ensure and promote that healthcare institutions adopt and use healthcare technology meaningfully. An example is the electronic health records that ensure that patient data privacy and data security are enforced when sharing and storing protected health information electronically. HITECH addressed patient privacy issues, making the penalties for HIPAA violations more severe. HITECH was used to develop a tiered HIPAA violation system, and the implementation of the HITECH tightened breach notification. Cybersecurity auditor has adopted the HITECT system to conduct an annual audit for healthcare institutions (Coronado & Wong, 2014).

With the wide adoption of digital payment across the healthcare industry, the Payment Card Industry Data Security Standards (PCI DSS) process payment via patient credit cards. The PCI DSS protects patients' credit card information to ensure that providers protect patient privacy when initiating payment via the healthcare institution's electronic payment platform (Levi, M., 2017). The PCI DSS rule governs how the patient's credit card information is stored, processed, and transferred. This information must be protected and prevented from getting into the hands of threat actors. If a breach occurs, this will cause a financial crisis and identity theft, which will impact the patient's financial status negatively and damage the integrity of the healthcare organization (Sulistyowati et al., 2020).

With the evolution of Medical-Internet-of-Things (MIoT), hackers have targeted medical devices, and the attack is on a geometric growth. The Food Drug Agency (FDA) responded to the threats by creating a Quality System Regulation (QSR) rule to enforce standards and best practices to organizations that manufacture medical equipment and use this equipment. The manufacturer must design the equipment to prevent unauthorized access and conduct thorough risk management after manufacturing before selling to end users (Khan, S. K. et. al., 2022). The manufacturer must have a tracking system that will monitor the MIoT devices in their system and track the usage pattern by end users. Firmware that prevents threat actors from stealing sensitive patient data must be updated and upgraded timely. Threat actors will use weak or outdated firmware to attack the system and settle in the system to steal patient-sensitive data. This data breach will impact the patient and organization negatively because revenue will be lost, and patient identity will be stolen for personal gains (Kesan, J. P., & Hayes, C. M., 2017).

Some healthcare institutions in the mid-western part of the United States and other states have adopted the HITRUST alliance to boost internal organizational compliance. Most healthcare institutions have adopted the HITRUST framework to monitor the activities of the devices joining their network. Also, it monitors the organization configuration management, risk assessment management, and endpoint security (Poehlmann, N. et. al., 2021).

2.2 Financial State Cybersecurity Laws and Regulations

In the banking and financial sector of Indiana, California, Iowa, Kansas, Louisiana, Illinois, and Kentucky, data breach notification law requires related financial entities that conduct business in these states or has a license to store the personal information of the residents in these to inform the resident if their personal information has been compromised and in possession of an unauthorized person (Hasan, S. et. al., 2021). The organization compliance officer dedicated to reporting data breach issues to state regulatory bodies will act timely. In the states above, the attorney general's office must be notified immediately after discovering the breach. During the data breach investigation in the organization, if the consumer data was not compromised and with no harm, the compliance officer might not notify the office of the state's Attorney General. Should the data breach affect third parties, the organization or approved licensees by the state must be notified if their personal information is compromised (California Governor Office, 2022).

The compliance officer must notify if the compromised data is in an unauthorized individual's hands. The compliance officer will issue a written notice to the resident of the state, and a copy will be provided to the consumer protection section of the attorney general's office. If law enforcement requires an investigation, the compliance officer will sometimes issue a substitute notice (Sangani, N., 2017). The organizations in this industry will have their data breach notification procedure, which must be maintained as part of their information security standards and best practices as enforced by the state per the law. Organizations are expected to comply with the Federal Interagency Guidance Response Programs for consumer notice and unauthorized access to consumer information to prevent violation of data breach notification. Suppose the compliance officer needs to notify the office of the attorney general. In that case, an average of $5,000 fine per day will be charged to the affected individuals, and the attorney general office may issue a civil action to recover damages (Caron, M. S., 2019).

Delayed notification of the Attorney General's office of a data breach might sanction the state government to withdraw the license to operate in the state. The affected individual might sue the organization for a data privacy compromise that might result in data theft. Consumer personal information compromised could cause a financial crisis if their social security numbers were used to apply for loans and credit cards. The cost of litigation and remediation will cause a huge revenue loss to the organization (Randazzo, M. R. et. al., 2005). The Consumer Data Protection Act (CDPA) is applicable in more than five states (Virginia, California, Indiana, New Jersey, Ohio, etc.) in the United States. This act targets retailing businesses processing more than 12,000 consumer data annually and generating more than $5,000,000 in revenue. The CDPA allows covered entities (organizations and licensed third-party businesses) to sell residents' personal information with formal notification and approval from the consumer.

The act prevents covered entities from using consumer social security numbers and other sensitive information for undisclosed reasons. Covered entities do not have the right to transfer or exchange consumer personal information for a marketing campaign. The consumer information must not be printed on means of hard copies that can easily be accessible by an unauthorized person (Nazarro, C., White, M., & Setterlund, E., 2017). The covered entities must not require the consumer to use their personal information to access a website without a unique identification number and password.

The security team must ensure that multi-factor authentication is deployed to prevent unauthorized users from accessing personal consumer data. The act prevents the covered entities from sending mail via physical or electronic that will contain consumer data either in the body of the mail or in the letter sent to the consumer address (Andronache, A., 2019). The covered entities must encrypt sensitive information when sending either electronic or physical mail to the consumer. To protect consumer data privacy, the act included data security to ensure that covered entities running a retailing business in the state deploy a rule for reporting cybersecurity incidents that might impact the privacy of the consumer data with a robust risk assessment to monitor the cybersecurity posture of the entities in real time. An unencrypted and unredacted mail sent to a consumer should be notified under the law of the state, as compliance oversees by the office of the attorney general (Waxman, M. C., 2011).

In the case of a data breach or data privacy compromise, the compliance officer of the covered entities must report the incident to the attorney general without delay to prevent sanction and fines from the office of the attorney general. Any data privacy compromise that might lead to identity theft or fraud must be reported by consumer reporting agencies covered by the state and a business associate of the covered entities in the state timely to the Attorney General (Kesan, J. P., & Hayes, C. M., 2017). On average, $120,000 in penalties is paid per violation and can be high as $10,000,000 or more in some states. This will cause a severe revenue loss to the organization, and the Attorney general office can seek a civil means to recover damages for the consumer. This will impact the financial status of the consumer if their information is used to apply for loans without their consent (Nazarro, C., White, M., & Setterlund, E., 2017).

2.3 Protecting Critical Information Resources

The security team and stakeholders must devise a means to protect their organization's infrastructure to ensure that consumer personal information is secure. Over the years, industries like banking and finance, retail, and healthcare have lost billions in revenue due to cyber-attacks and customer litigations because their data was compromised. Organizations in these industries must hire an experienced cybersecurity expert to ensure that they will deploy appropriate security solutions and enforce standards and best practices to improve the organization's cybersecurity (Hasan, S. et. al., 2021).

The security team must deploy an access control for adequate access management to ensure unauthorized individuals cannot access customer, transactional, and operational data. The security team must ensure that employees do not share their credentials or login details with anyone, and the human resource team, in collaboration with the IT team, will educate the new hire to desist from the act (Fausto et al., 2021). Also, credential de-commissioning will be initiated immediately after an employee resigns or retires. The security team will enforce password requirements and ensure passwords expire monthly to prevent security compromises. The security team will initiate role-level access and permission to prevent who has access to what. For third-party contractors, the security team will deploy a virtual private network (VPN) and MFA (multi-factor authentication) to prevent an intruder from accessing the organization's network (Kim, L., 2017).Timely risk analysis will be a routine that must be conducted to ensure a robust cybersecurity plan. It is advisable to have an internal cybersecurity auditor that will audit the activities of the employees and the activities of external traffic accessing the organization's network.

The security will ensure that an updated inventory list summarizes each asset's vulnerability and risk level on the organization's network (Koch, D. D., 2016). Once the vulnerabilities have been identified, the security team can create a redundancy should an attack occur to prevent the business operation from shutting down (Matrix, n.d). A legacy system can be replaced and integrated into a centralized network intrusion and detection system to help the security team to monitor the network vulnerability in real time. Safeguard will address identified vulnerabilities, and data transmission within and outside the network must be encrypted and secured (Subramania & Wyatt, 2022).

The security team will ensure that network infrastructure is secured and protected using end-to-end encryption to prevent threat actors from deciphering the organization's information. Industry-approved physical and software firmware and anti-virus must be deployed to prevent malware, viruses, and bugs from entering and settling into the network (Sulistyowati, D. et. al., 2020). An automatic system that will notify the security team of updates and available patches should be installed on the network to reduce the vulnerability of the network assets. Whenever the security team operation center has detected an attack, the security team should adopt network segmentation to reduce the impact of the attack and mitigate the damage the risk might cause to the organization's infrastructure (Kim, 2017). In collaboration with the IT team and the human resource team, the security team must enforce weekly or monthly cybersecurity programs across the organization to expose the employees and contractors to be familiar with the industry pattern of attacks. The cybersecurity awareness program will be mandated and reviewed timely to ensure that employees and contractors abide by the organization's cybersecurity best practices and standards (Khan, S. K. et. al., 2022).

3. METHODOLOGY

A thorough examination of relevant literature, government reports, official websites and academic articles was carried out in the research. A diverse range of perspectives and observations on the subject was gathered from several sources. A comprehensive evaluation of academic literature on cybersecurity laws and regulations in the United States was carried out. To identify relevant peer reviewed articles, papers, conferences, and book chapters, scholarly databases such as Google Scholar, Xplore, ACM Digital Library, and JSTOR have been used. The following keywords were used for the literature search: cybersecurity laws, Cybersecurity Regulations, Federal Cyber Security Laws, State Level Initiatives of Protecting Cyber Safety, Variations thereof.

In addition, to obtain information on laws and initiatives at the Federal and State level concerning cyber security, officials' reports and documents from Government Agencies and Regulatory Authorities have been reviewed. A valuable source of legislative information, policy documents, and guidelines was the official websites of government bodies such as the United States Congress, the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and state government websites.To obtain current information on emerging trends, legal developments and actual world examples of cybersecurity incident and their implications, the industry reports, news articles or trusted media outlets have been consulted. The practical application and impact of cyber law and regulations have been helped to be better understood by these sources.

4.CONCLUSION

In this paper, the healthcare state cybersecurity laws for most states in the United States have adopted the HIPAA. They must comply with the security rule to ensure that patient data are stored, processed, and transferred securely. All hospitals operating in all the states in the United States have adopted the PCI DSS as their secure payment method platform to prevent patient credit card information is protected and prevent from getting into the hands of the threat actors (Randazzo, M. R. et. al., 2005). Most states in the United States must protect consumer personal information in the banking and finance sector.

The method of notification of data breach has been spelled out by the Attorney General's office and the appropriate sanction and penalties for violation. Consumer data protection is a widely adopted act by most states for retailing businesses that process more than 12,000 consumer data annually and generate more than $5,000,000 in revenue. The consumer data protection act will guide the covered entities on using and protecting consumer data from a data breach (Kim, L., 2017). To prevent the network infrastructure of the industries discussed in this paper, the security team must deploy robust cybersecurity solutions and develop standards and best practices that employees and contractors of these organizations must follow.

REFERENCE

1. Andronache, A. (2019). *Aligning cybersecurity management with enterprise risk management in the financial industry* (Doctoral dissertation, Brunel University London).
2. California Governor's Office of Emergency Services. (2022). *Critical infrastructure protection:*
3. *Keeping infrastructure strong and secure*.
4. Caron, M. S. (2019). The transformative effect of AI on the banking industry. *Banking & Finance Law Review*, *34*(2), 169-214.
5. Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an
6. effective plan. *Biomedical instrumentation & technology*, *48*(s1), 26-30.
7. Fausto, A., Gaggero, G., Patrone, F., Girdinio, P., & Marchese, M. (2021). Toward the integration of cyber and physical security monitoring systems for critical infrastructures. *Sensors, 21*(6970), 6970. https://doi.org/10.3390/s21216970
8. Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.
9. Kesan, J. P., & Hayes, C. M. (2017). Strengthening cybersecurity with cyberinsurance markets and better risk assessment. *Minn. L. Rev.*, *102*, 191.
10. Khan, S. K., Shiwakoti, N., & Stasinopoulos, P. (2022). A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. *Accident Analysis & Prevention*, *165*, 106515.
11. Kim, L. (2017). Cybersecurity awareness: Protecting data and patients. *Nursing2022*, *47*(6), 65-67.
12. Koch, D. D. (2016). Is the HIPAA security rule enough to protect electronic personal health
13. information (PHI) in the cyber age. *Journal of Health Care Finance*, *43*(3).
14. Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and Issues: In Cybercrimes, cybercriminals and their policing, in crime, law and social change. *Crime, law and social change*, *67*, 3-20.
15. Matrix IFS. (n.d.). *NY DFS 500 cyber security regulation readiness checklist*.
16. Nazarro, C., White, M., & Setterlund, E. (2017). The Evolving Landscape of Data Privacy and Cyber Security in the Financial Services Industry. *Emory Corporate Governance and Accountability Review*, *4*(2), 369.
17. Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. *Computers & Security*, *74*, 371-383.
18. Poehlmann, N., Caramancion, K. M., Tatar, I., Li, Y., Barati, M., & Merz, T. (2021). The organizational cybersecurity success factors: an exhaustive literature review. *Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20*, 377-395.
19. Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.
20. Sangani, N. (2017). Cybersecurity and its impact on the financial services industry. *NY Business Law Journal*, 48.

21. Satariano, A., & Goldstein, M. (2017). Equifax says cyberattack may have affected 143 millioin the U.S. The New York Times. Retrieved from https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html
22. Subramania, S., & Wyatt, M. (2022). *Cybersecurity for critical infrastructure protection: A growing, highly visible threat calls for state leadership*. Deloitte.
23. Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of
24. cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. *JOIV: International Journal on Informatics Visualization*, *4*(4), 225-230.
25. Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, *23*(4), 1836-1846.
26. Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of article 2(4). *Yale J. Int'l L.*, *36*, 421.