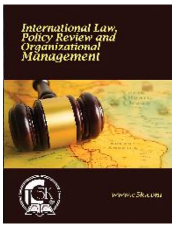
International Law Policy Review Organizational Management
"Volume 1, Issue 1, Year 2024"
website: https://www.c5k.com



Research Article

The Impact of the US on the Development of International Cybersecurity Law: Legal Challenges and Emerging Norms

Syeda Farjana Farabi[1,*], Abdullah Al Sakib[2], Md Faruque[3], Salma Akter[4]
[1]*Department of Business Administration, Westcliff University, Irvine, CA 92614, USA*
[2]*Department of Information Technology, Westcliff University , Irvine, CA 92614, USA*
[3]*Department of Law, University of Derby (London), Kedleston Road, Derby DE3 16B, UK*
[4]*Department of Law, Stamford University Bangladesh, 51 Siddeswari Road (Ramna), Dhaka-1217*
**Corresponding Author:* *s.farabi.184@westcliff.edu*

ARTICLE INFO

Article history:
03 Jul 2024 (Received)
23 Aug 2024 (Accepted)
30 Aug 2024 (Published Online)

Keywords:
Cyber security, Regulations, Policies, NIST Cyber Security Framework, HIPAA, GLBA, FISMA, CISA, CCPA, DOD CMMC, Cyber Threats, Data Compromises, Fraud, Trend Analysis, Public-Private Partnerships, Cyber Resilience.

ABSTRACT

The rise in cyber threats and assaults in the current digital era has made cyber security an essential field that poses major risks to individuals, organizations, and nations. Numerous national and international cyber security laws and regulations have been developed in response to these evolving challenges. The efficiency of the country's present cyber security laws and policies is evaluated in this article in light of the growing sophistication and frequency of cyber-attacks. The National Institute of Standards and Technology (NIST) Cyber security Framework and important laws like HIPAA, GLBA, FISMA, CISA, CCPA, and the DOD Cyber security Maturity Model Certification are highlighted in this comprehensive framework that was developed by the US government. The report examines how these restrictions affect various industries and looks at patterns in data on cybercrime from 2000 to 2022. The results emphasize the difficulties, achievements, and necessity of ongoing adaptation in the face of changing cyber threats.

DOI: https://doi.org/10.103/xxx @ 2024 International Law Policy Review Organizational Management (ILPROM), C5K Research Publication

1. Introduction

Given the rise in frequency and sophistication of cyber threats, cyber security in the US has emerged as a crucial and dynamic topic. It is comparable to data security, which deals with preventing data from being stolen or hacked (Nfuka et al., 2014). Due to its reliance on digital infrastructure for vital services, trade, and communication, the country is a prime target for cyber-attacks. Data breaches, ransomware attacks, and nation-state-sponsored cyber espionage are just a few of the many cyber threats that can affect individuals, government organizations, and private businesses. To improve the resilience of the country's cyberspace, the United States has created a comprehensive cyber security architecture that involves cooperation between the public and private sectors as well as academic institutions. The National Institute of Standards and Technology (NIST) Cyber Security Framework is a fundamental component of the U.S. cyber security policy. A set of best practices and principles for managing and strengthening an organization's cyber security posture are provided by this framework. It places a strong emphasis on incident response, ongoing monitoring, and risk management to improve overall cyber security resilience. Furthermore, some federal organizations, such as the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS), are essential to the protection of vital infrastructure and the investigation of cybercrimes. The costs of cybercrime include knowledge loss and damage, the cancelation of hacked data and systems, cash taken, and misplaced effectiveness, Theft of financial and personal resources misappropriation and information (Ahmad, 2020).

Founded in 2009, the U.S. Cyber Command is in charge of safeguarding the military's cyber capabilities and defending the country against serious cyber threats. Notwithstanding these initiatives, problems still exist, and the field of cyber security is always changing. Businesses in the private sector also contribute significantly to cyber security by making significant investments in staff and technology to protect their networks and data. The United States' strategy to cyber security must include ongoing cooperation between the public and commercial sectors, international cooperation, and a commitment to staying ahead of developing threats. To properly protect the country's digital infrastructure, lawmakers and cyber security experts need to be alert and flexible as threats continue to change. Using people's flaws to force labor

*Corresponding author: s.farabi.184@westcliff.edu (Syeda Farjana Farabi)

Cite: Syeda Farjana Farabi, Abdullah Al Sakib, Md Faruque, Salma Akter (2024). The Impact of the US on the Development of International Cybersecurity Law: Legal Challenges and Emerging Norms. *International Law Policy Review Organizational Management,* 1(1), pp. 23-32.

and obtain information is known as social engineering (Okereafor & Adebola, 2020). Cyber threats and attacks have increased concerningly in the United States, which is indicative of a worrying trend of an increase in cybercrime. The sophistication of cyber threats is rising along with technology, which presents serious obstacles to the nation's cyber security environment. An "Association of Computing Machinery" research emphasizes the rise in ransomware assaults, in which malevolent parties encrypt private information and demand payment to decrypt it. These assaults have caused disruptions and monetary losses by focusing on several industries, including essential infrastructure, finance, and healthcare. To counteract the ever-evolving strategies used by hackers, the study highlights the necessity of ongoing cyber security measure enhancement. Spammers frequently use phrases and keywords that incite panic and a sense of urgency while crafting their spam messages (Aldawood & Skinner, 2019).

Furthermore, the United States is becoming increasingly concerned about nation-state-sponsored cyber espionage. Nation-states attempting to breach vital infrastructure and U.S. government networks are posing a persistent and sophisticated cyber threat, according to a thorough assessment published by the "Cyber Security and Infrastructure Security Agency (CISA)". The research emphasizes how crucial it is to strengthen information-sharing and cyber defenses to protect national security. The growing prevalence and intensity of cyber-attacks highlight the need for a comprehensive and cooperative strategy encompassing public and private sectors as well as academia to strengthen the country's cyber security posture. The other checks concerned illegal access to several additional websites, including several belonging to US colleges (Kabay, 2012). Cyber security laws and regulations are essential in protecting sensitive data and vital infrastructure in the United States against cyber threats such as malware, hacking, and data breaches. They create a structure that enables businesses to successfully safeguard their networks and systems. These legal actions guarantee that victims of cybercrime have legal recourse and also make businesses and individuals responsible for any cyber incidents. Cybersecurity standards are a set of procedures or technical techniques that assist enterprises in safeguarding their online environment (Collier et al., 2014). All things considered, these regulations establish a baseline for safeguarding private data and vital infrastructure against online attacks. It is crucial to understand that, depending on the situation, compliance with various rules and regulations may be situation-specific and industry-specific.

2. Literature review

2.1. NIST Cybersecurity Framework:

The Cybersecurity Framework was created by the National Institute of Standards and Technology (NIST) to give businesses best practices and standards for managing and enhancing cybersecurity risk management. Cybercrimes evolved from sporadic, one-person operations to a series of coordinated, highly complex crimes committed by a well-organized criminal business. Even if many of the crimes had occurred in earlier decades, their scope and frequency have not returned (White, 2013). Standards, policies, and procedures are all included in the framework to improve cyber security. NIST Cyber Security Framework 1.1, which was issued in April 2018, is the most recent version. A collection of best practices and standards called the National Institute of Standards and Technology (NIST) Cyber Security Framework is used in the US to assist firms in managing and enhancing their cyber security risk management procedures. The framework, which was created by NIST in response to Executive Order 13636, offers firms in a variety of industries a flexible and voluntary structure to improve their cyber security resilience. Five fundamental tasks form the basis of the framework: identify, protect, detect, respond, and recover. Organizations can utilize the framework to evaluate and improve their cyber security posture. Each function stands for important components of an all-encompassing cyber security program. According to Steve Morgan, the founder and chief editor of Cyber Security Ventures, the costs associated with cybercrime include reputational damage, embezzlement, fraud, theft of financial and personal information, disruption of regular business operations following an attack, forensic investigation, and the restoration and deletion of compromised data and systems (Ventures, 2017). The first function, "Identity," is concerned with creating an organizational framework, comprehending asset management, and defining risk management techniques to comprehend and manage cybersecurity issues. The "Protect" role entails putting safety measures in place to guarantee the provision of essential infrastructure services, such as training programs, access controls, and data protection protocols. While the "Respond" function describes what to do during a cyber security issue, the "Detect" function emphasizes ongoing monitoring and prompt identification of cyber security incidents. To guarantee the safeguarding of data and infrastructure within corporations, governments, and organizations, cybersecurity standards and frameworks are necessary (Srinivas et al., 2019).

An article from The Established for Critical Infrastructure Technology claims that Mirai created and built a botnet by abusing Internet of Things technology and production line default or hardcoded client names and passwords. The Mirai Botnet was deployed against Dyn, a provider of web infrastructure, in October 2016 (Advisers, 2018). The last function, "Recover," is creating and putting into practice plans for quickly restoring systems and services after a cyber security event. Businesses in the US are urged to evaluate and strengthen their cyber security posture under their risk management requirements and corporate goals by utilizing the NIST Cybersecurity Framework. Because of the framework's versatility, it can be used in a variety of industries and help create a more secure and resilient cyberspace. A comprehensive and flexible set of best practices and standards, the NIST Cyber Security Framework (CSF) is intended to help enterprises manage and improve their cyber security risk management procedures. The framework, created by the National Institute of Standards and Technology (NIST), offers a versatile method that businesses in a range of industries can utilize to improve their cyber security posture. The Core, Implementation Tiers, and Framework Profile make up the three main parts of the framework's structure.

Standards for the security of private patient health information are established by HIPAA. To maintain the privacy, accuracy, and accessibility of health information, covered organizations such as hospitals and health insurance providers must abide by HIPAA requirements. To protect the security and privacy of people's health information, the United States passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996. In addition to addressing the issues with electronic healthcare data transfer, HIPAA works to protect the integrity and security of sensitive patient data. Preventing or lessening cyber-attacks and lowering the danger of cyber threats is the primary goal of cyber security guidelines (Purser, 2014). The Privacy Rule and the Security Rule are the two main regulations that control how health information is protected among the several standards that make up the act. While the Security Rule concentrates on the security measures required to protect electronic PHI, the Privacy Rule sets guidelines for the use and disclosure of protected health information (PHI).

2.2. HIPAA (Health Insurance Portability and Accountability Act)

The HIPAA Security Rule provides a thorough framework for protecting electronic patient health information (ePHI). It requires the implementation of administrative, physical, and technical measures by covered entities, including health plans, clearinghouses, and healthcare providers, to guarantee the confidentiality, integrity, and availability of electronic patient health information. Measures including risk assessments, audit controls, encryption, and access controls are all part of the system. Adopting policies and procedures to protect ePHI from unauthorized access or disclosure, as well as conducting routine risk assessments to find and address possible vulnerabilities in their information systems, are requirements for covered companies. It is permissible for a nation or business to reject laws or guidelines released by other parties and to create their own exclusive guidelines or regional regulations (Bloor et al., 2009). Serious consequences, like as fines and legal action, may arise from breaking HIPAA regulations. In an increasingly digital and networked healthcare environment, the framework that HIPAA provides is crucial for fostering public confidence in the healthcare system and safeguarding individuals' private health information.

2.3. Gramm-Leach-Bliley Act (GLBA):

Financial institutions must protect the private financial information of their consumers under GLBA. It requires the creation and execution of information security programs and contains clauses regarding the security and confidentiality of nonpublic personal information. Using NIST SP 800-14 guarantees that businesses have information technology security solutions ready for cyber-attacks (Almuhammadi et al., 2017). The Financial Modernization Act of 1999, or the Gramm-Leach-Bliley Act (GLBA), is a significant piece of US legislation that aims to improve customer privacy and information security in the financial industry. The Glass-Steagall Act (GLBA), which was passed to abolish some of its provisions, established new regulations for financial institutions, including banks, credit unions, and securities firms, about safeguarding the nonpublic personal information (NPI) of their customers. The principal aim of the GLBA is to guarantee that financial institutions implement suitable measures to preserve the privacy and security of client data (U.S. Congress, 1999). Financial institutions must create, carry out, and maintain extensive information security programs under GLBA. To ensure the safety, privacy, and accuracy of consumer data, these programs need to have technical, administrative, and physical security measures in place. In addition, the Act requires financial institutions to give clients brief and understandable privacy warnings outlining the institution's information-sharing policies and offering them the choice to refuse to share their information with unaffiliated third parties. Serious fines and legal action may follow noncompliance with the GLBA. As essential components of IT governance, cyber security standards are reviewed to make sure a company is adhering to its cyber security strategy and policies (Baron et al., 2019). The Act seeks to provide customers control over how financial institutions use and share their personal financial information, emphasizing the significance of transparency in information-sharing processes.

2.4. Federal Information Security Modernization Act (FISMA):

One of the most important pieces of cyber security law in the US is the Federal Information Security Modernization Act (FISMA), which was passed in 2002. It requires government agencies to put security measures in place to protect their data and information systems. Ensuring the availability, confidentiality, and integrity of the data that government agencies gather, keep, and use is the main objective. Additionally, from January to December 2018, the number of phishing emails detected worldwide climbed by 250%. Attackers are being pushed to evade ever-more-effective anti-phishing technologies and procedures, which has led to an evolution of phishing assault methodologies (Khiralla & Network, 2020). Agencies must set up extensive information security plans per FISMA, which must include ongoing security testing, incident response planning, frequent risk assessments, and continuous control monitoring. Agencies must also notify the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB) about their compliance with the statute. The primary organization charged with developing security standards and guidance for federal agencies is identified by FISMA as the National Institute of Standards and Technology (NIST). "NIST Special Publication 800-53" from NIST offers a thorough framework outlining the security measures that federal agencies need to implement to comply with FISMA regulations. The 2017 Norton Cyber Security Insights Report demonstrates the increasing global trend of cyberattacks and the damages they cause (NORTON, 2017).

2.5. Cybersecurity Information Sharing Act (CISA):

Enacted by the US Congress in 2015, the (CISA) provides liability protections for private enterprises that exchange information with the government about cyber dangers. Cyber dangers result in significant trade barriers, privacy violations, corporate hazards, and financial losses (Sheehan et al., 2019). To protect vital infrastructure and national security from cyber-attacks, its main objective is to improve the sharing of cyber threat intelligence between the public and commercial sectors. Under CISA, private organizations can provide cyber threat intelligence to federal agencies, such as the Department of Homeland Security (DHS), and the government can exchange information with private organizations in return. CISA also contains provisions for voluntarily creating Information Sharing and Analysis Organizations (ISAOs). Information on cyber threats can be shared among members of these organizations more easily. To counter cyber dangers, companies that share information in good faith are protected from responsibility under the law. Nonetheless, detractors, including campaigners for civil rights and privacy, contend that CISA might not provide enough protection for private data and might be used by the government for monitoring purposes (Enterprise Engineering Solutions, 2023). Contrary to most references, all industrial Internet of Things (IIoT) attacks occur at the information transmission layer (Alshaibi et al., 2022).

2.6. California Consumer Privacy Act (CCPA):

The CCPA requires firms to use appropriate security measures to protect the personal information of their customers, even though its primary concern is privacy. California people now have more control over the personal information that companies hold on them thanks to the historic California Consumer Privacy Act (CCPA). The CCPA, which was passed in 2018 and went into effect on January 1, 2020, gives customers more control by giving them the right to know what personal information is gathered, sold, or released by companies. To identify malicious nodes in the Internet of Things network, the authors demonstrated a fog layer-based DDoS threat identification technique (Gaurav et al., 2021). Covered organizations must notify customers about their data practices and comply with requests for access, erasure, or opt-out of their personal information being sold. These businesses include those with annual gross revenues above $25 million or those that handle the personal information of at least 50,000 California consumers. A thorough framework for privacy protection is introduced by the CCPA, which encourages accountability and openness in the gathering and use of personal data. Businesses must update their privacy policies, let customers know about their rights, and set up procedures so they may use those rights. Furthermore, companies must strictly adhere to the law's requirements and put appropriate security measures in place to protect customer information. Hemphill and Longstreet have also concentrated on data breaches in the US retail sector, taking into account the Payment Card Industry Data Security Standard, or PCI DSS (Hemphill & Longstreet, 2016). In addition to having a big impact on companies that operate in California, the CCPA also has a big impact on the privacy landscape in the US and shapes conversations about possible federal privacy legislation.

2.7. DOD Cybersecurity Maturity Model Certification (CMMC)

The CMMC was implemented by the Department of Defense (DOD) to improve the security of Controlled Unclassified Information (CUI) in the defense industrial base. This standard's primary goal is to guarantee that cyber security issues are taken into account when designing road vehicles and that they are safeguarded against various cyber-attacks (Macher et al., 2020).To take part in DOD contracts, suppliers and contractors must adhere to strict cyber security requirements. To improve cyber security procedures inside the defense industrial base (DIB), the United States Department of Defense (DOD) Cyber security Maturity Model Certification (CMMC) is a comprehensive framework. CMMC is a five-level maturity model that was introduced to address concerns about the security of sensitive information in the supply chain. The levels range from basic cyber hygiene to advanced capabilities. It also addresses important information security topics that must be taken into account when establishing policies for businesses and government agencies (Schmitz et al., 2021). Every level expands on the one before it, covering particular areas and skills that are essential to cyber security. Notably, CMMC ensures a more stringent and uniform evaluation method by replacing self-assessment with third-party certification. By the middle of the 2020s, the DOD intends to progressively include CMMC standards in new contracts, placing a strong emphasis on working with stakeholders and industry experts to adapt to changing cyber threats. As a result, federal agencies in both the United States and Canada will accept a product if it satisfies FIPS 140-2 standards (Boboň, 2021). Potential implementation costs for DIB organizations, particularly smaller businesses, present a challenge, as does the constant requirement for updates to keep up with the ever-changing cyber security threat landscape. Fig. 1 of a research released in April 2017 by American cyber security company Symantec states that phishing attacks occurred in the United States more than in any other country in 2016. On Symantec's list, it is ranked highest. It ranked second in the last year of 2015 with 18.89% of threats identified globally, although that number has since increased to 23.96%.

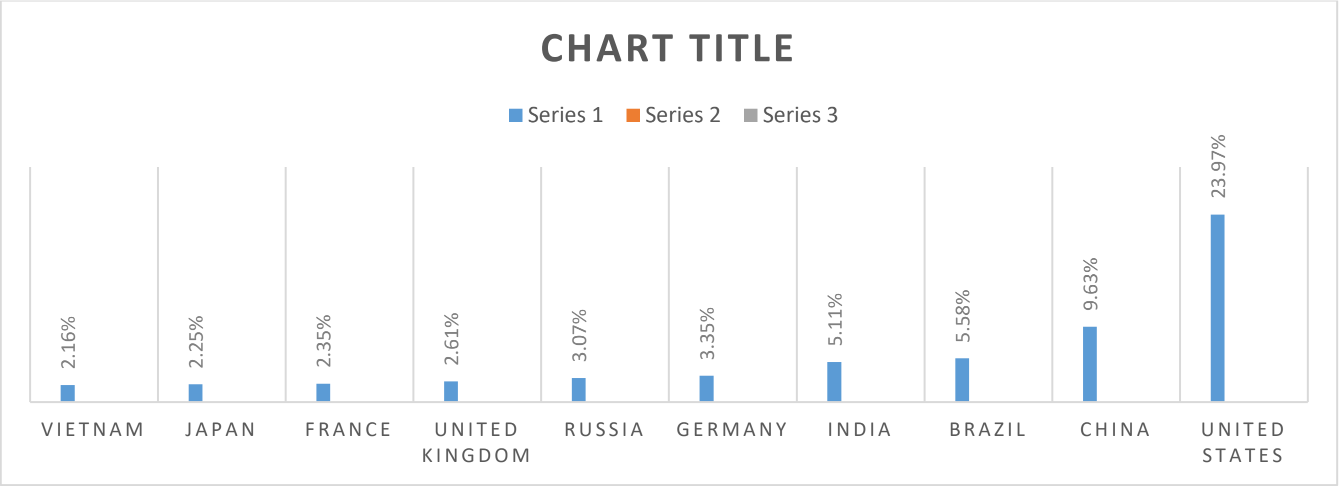


Fig. 1. The 10 countries that were the source of the most cybercrime in 2016.

3. Methodology

Updates to the regulatory measures addressing critical infrastructure vulnerabilities have mostly languished until President Obama's 2013 State of the Union Address and Executive Order 13636. For example, the Obama Administration proposed a comprehensive cyber security law in 2011 to strengthen protection for vital infrastructure. Sections of the Proposal from the Administration The Cyber Security Act of 2012 would have assigned a new National Cyber Security Counselor the responsibility of identifying critical cyber infrastructure, conducting sector-by-sector cyber risk assessments, and establishing a voluntary, outcome-based cyber security program for critical infrastructure in collaboration with private sector owners and operators.139 Nevertheless, the bill ran into resistance from the business community and was not approved by the Senate. As of May 2014, legislation based on the recommendations made by the House of Representatives Cyber Security Task Force has not yet been passed. "No comprehensive cyber security legislation has been enacted since 2002," although cyber-attacks have become more sophisticated and frequent during the past ten years. The Obama Administration took administrative action in response to this congressional impasse.

3.1. Breakdown of the NIST Cybersecurity Framework:

The Cyber Security Framework employs a risk-based methodology to help organizations identify, stop, and deal with cyber threats. The Cyber Security Framework "relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience," as opposed to creating new risk management procedures and cyber security standards. This approach enables the Framework to "scale across borders, acknowledge the global nature of cyber security risks, and evolve with technological advances and business requirements." The Cyber Security Framework gives organizations a "common language" to assess their cyber security posture, identify their desired cyber security state, rank areas for improvement, gauge their progress toward that state, and set up adequate channels of communication with internal and external stakeholders regarding cyber security risk. The Framework Core, which "provides a set of activities to achieve specific cyber security outcomes, and references examples of guidance to achieve those outcomes," is presented first in the Cyber Security Framework. The Framework Core is an organizational map of industry-recognized cybersecurity practices that are useful in managing cybersecurity risk; it is neither an entire list nor a checklist, but it does offer uniform vocabulary that helps organizations comprehend the effects of good cybersecurity practices. The Framework Core is divided into four sections that help map relevant cyber security standards, guidelines, and best practices: Functions, Categories, Subcategories, and Informative References which shows in Table 1.

Table 1: Four sections that help map relevant cybersecurity

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy	ID.AM-1: Physical devices and systems within the organization are inventoried	• CCS CSC 1 •COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 •ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8

The Core starts by outlining crucial cyber security operations "at their highest level," or Functions. By categorizing procedures into these crucial areas, the Framework's five Functions—Identify, Protect, Detect, Respond, and Recover—are meant to help a company articulate its approach to managing cyber security risk. "Groups of cyber security outcomes, closely tied to programmatic needs and particular activities," or "categories of cyber security outcomes," are contained inside each Function and are more specific subsets of the overarching practices. Every Category supports an organization's methodology for delineating the principal Functions that underpin the Cyber Security Framework.

4. Result and discussion

Financial losses attributable to cyber risks have increased significantly and steadily over the period studied, according to a trend analysis of the "Cost of Cyber Crimes" (Fig. 2) dataset covering the years 2007 to 2022. From $239.10 million in 2007 to an astounding $10,300.00 million in 2022, the data clearly shows an increase. This increasing trend suggests that the financial impact of cybercrimes on different companies has increased significantly, which is alarming. The years starting in 2010 are noteworthy because there was a noticeable increase in expenditures. This increase in cyber threats points to a significant turning point in the field and indicates that cyber-attacks are becoming more potent and aggressive. The dataset's largest financial toll is represented by the year 2022, which stands out as a peak.

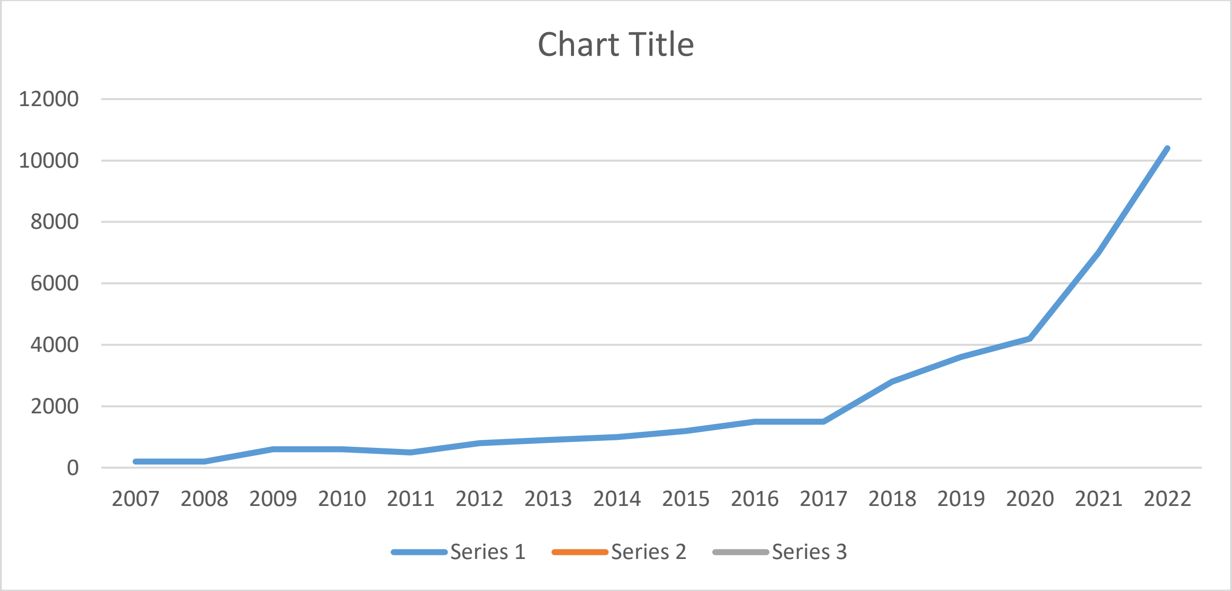


Fig. 2. Cost of Cyber Crimes (Oluomachi et al., 2024).

Although the breakdown of the data from year to year shows varied degrees of increase, certain years had more significant spikes than others, which could indicate changes in the tactics or intensity of cyber-attacks during particular times. This detailed research makes it possible to comprehend the trends at a finer level, which makes it easier to focus on cyber security efforts. Strong cyber security measures are desperately needed, as seen by the ongoing rise in cybercrime expenses.

The "Data Compromises" (Fig. 3) dataset's trend analysis from 2005 to 2022 reveals intriguing trends in the frequency of reported incidents. The information shows a steady rise in data breaches, with a notable spike from 157 cases in 2005 to 662 in 2010. The number of incidents fluctuated in the ensuing years, peaking in 2021 at 1862 occurrences. It is crucial to take into account the absence of 2022 data while examining the trend. Data breaches have steadily increased since 2015, which may indicate that cyber-attacks are becoming more sophisticated and have more attention. The year 2021 stands out in the statistics as the one with the most recorded data invasions. This highlights the growing spectrum of possible threats and the need for stronger cybersecurity defenses to protect sensitive information.

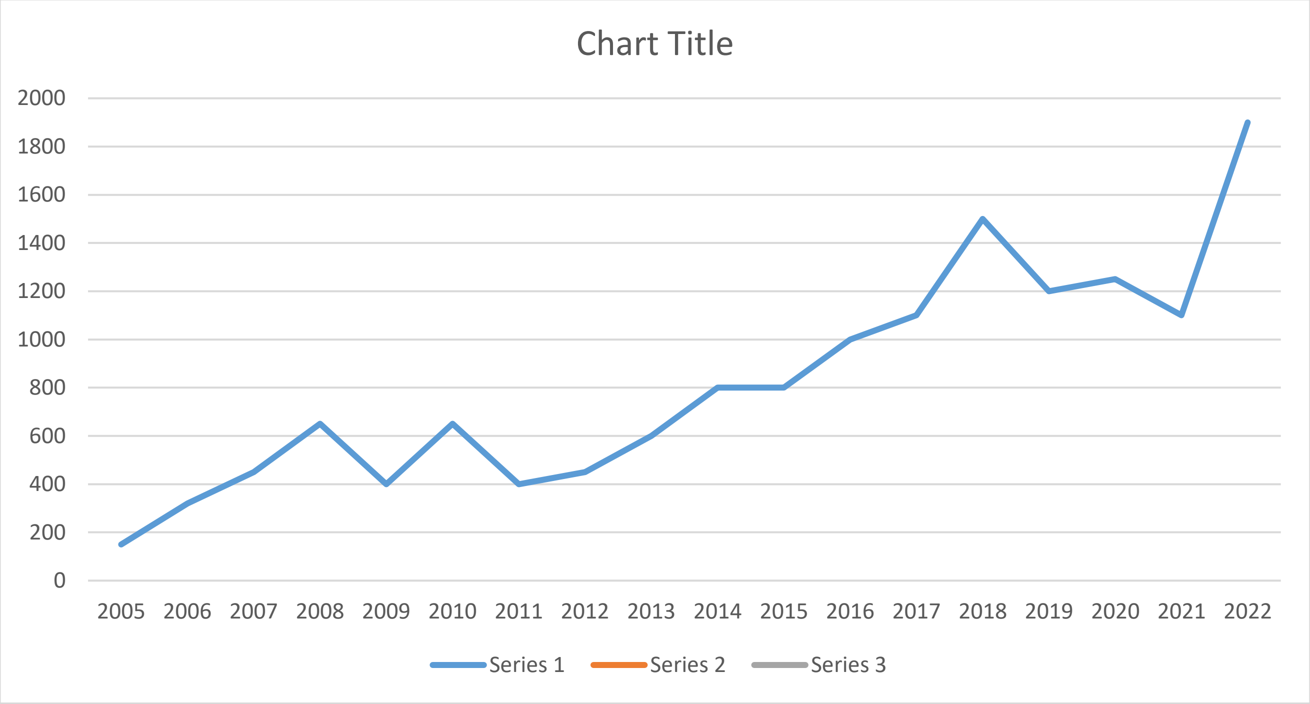


Fig. 3. Data Compromises.

Analyzing the year-over-year variations provides important information about potential changes in cyber-attack strategies. Differences in the number of data breaches in some years could indicate changes in the targets or tactics used by cybercriminals. To appropriately modify their security protocols, cybersecurity experts and organizations should closely monitor these patterns.

4.1. Amount of Losses of Cyberattacks last twelve years (2010-2021), U.S.A.:

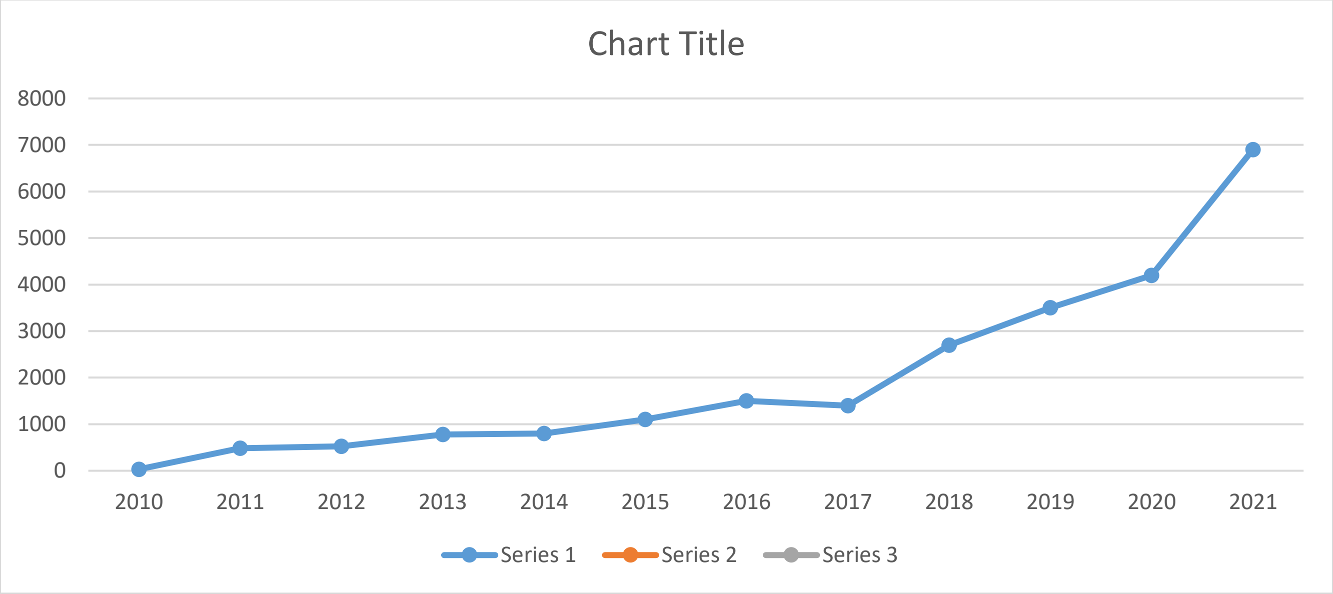


Fig. 4. Amount of Losses of Cyberattacks last twelve years (2010-2021), U.S.A.

We obtain information from the Federal Bureau of Investigation (FBI) and the Federal Trade Commission (FTC). The Consumer Sentinel Network Data Book was released by the Federal Trade Commission. the public data that was supplied. The databook is primarily concerned with financial losses, identity theft, fraud, and other consumer issues. Federal legislation is enforced by the Federal Bureau of Investigation (F.B.I.). It looks into a range of illegal activities, such as cybercrime, cyberterrorism, white-collar crimes, public corruption, abuses of civil rights, and other serious offenses. The FBI and FTC are federal agencies.

We make an Excel table once the data has been gathered. The table consists of 13 rows and 2 columns. The reporting years are shown in the first column, while the number of losses (in millions of dollars) is listed in the second. Every year, the figure is different. We obtain the total number for the applicable year by applying the summing formula. In order to create a 2D line chart, we collect and compute the data. We used the information in Fig. 4 to generate a 2D line chart. The amount of losses from cyber-attacks over the last 12 years, from 2010 to 2021, is displayed in a 2D line graph. The year is displayed on the X-axis, while the Y-axis displays the total number of losses due to cyber-attacks. The cost increased by 21.53% in 2011, 45.48% in 2012, and 29.13% in 2021. Fig. 2 provides more information.

Table 2 demonstrates the significant variation in the claimed cost of cybercrime, with an average cost of $2,013.94 billion in billions of US dollars and a standard deviation of $2,720.96 billion. Cybercrime has a minimum cost of $207.39 billion and a maximum cost of $10,300 billion. With a standard deviation of 478.17 instances, the average value of data compromise is 853.39 instances. There are 157 cases of data compromise at the minimum and 1,862 instances at the greatest figure. The mean fraudulent value is $1,553,312.87 billion, with a $598,004.75, standard deviation. The degree of dispersion in reported fraud amounts is shown in the variation of $598,004.75; this suggests heterogeneity in the financial impact of fraud episodes.

Table 2. Summary Statistics of Variables

Variables	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
Cost of Cyber Crimes (US'M)	207.39	10300.00	2013.94	2720.96
Data Compromises	157.00	1862.00	853.39	478.171
Fraud (USD)	820072.00	2789161.00	1553312.87	598004.75

Source: Author's Computation (2024) Using Stata 14

5. Conclusion and future work

In conclusion, it is critical to comprehend cyber security laws and regulations in the digital age of the internet's interconnectedness, which offers both significant advantages and risks. People, corporations, and nations face challenges as a result of the constantly changing nature and breadth of cyber risks. The evolution of cyber security laws over time reflects a growing recognition of the significance of protecting digital assets, personal information, and critical infrastructure. From the earliest days of addressing unauthorized access to the current era of stringent data protection legislation, these regulations have played a crucial role in shaping our digital environment. Principles such as data protection, breach notification, risk management, and responsibility form the foundation of cyber security regulations. The "Cost of Cybercrimes" varies widely, indicating a substantial financial impact on US-based businesses. Significant variation in reported costs was found, highlighting the heterogeneous nature of cyber threats. It is important to understand that certain occurrences have far larger consequences than others, highlighting how serious some cyber-attacks may be. This study suggests that the current state of cyber security necessitates a regulatory framework that is diverse and addresses a range of threats. The findings underscore the complex and dynamic nature of cyber security challenges faced by American enterprises. The effectiveness of current cyber security laws can be evaluated by their ability to respond to the ever-evolving threat landscape, address a wide range of cyber threats, and reduce the financial and operational fallout from cyber-attacks. To maintain the strength and adaptability of present rules in the face of the rapidly changing cybersecurity landscape, policymakers need to continuously evaluate and enhance them.

References

Advisers, U. C. E. J. W., Government Report. (2018). The cost of malicious cyber activity to the us Economy.

Ahmad, T. J. A. a. S. (2020). Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity.

Aldawood, H., & Skinner, G. J. I. J. o. C. A. (2019). A taxonomy for social engineering attacks via personal devices. *975*(2019), 8887.

Almuhammadi, S., Alsaleh, M. J. C. S., & Technology, I. (2017). Information security maturity model for NIST cyber security framework. *7*(3), 51-62.

Alshaibi, A., Al-Ani, M., Al-Azzawi, A., Konev, A., & Shelupanov, A. J. D. (2022). The comparison of cybersecurity datasets. *7*(2), 22.

Baron, J., Contreras, J. L., Husovec, M., Larouche, P., & Thumm, N. J. J. S. f. P. R., EUR. (2019). Making the rules: The governance of standard development organizations and their policies on intellectual property rights. *29655*.

Bloor, M., Sampson, H. J. W., employment, & society. (2009). Regulatory enforcement of labour standards in an outsourcing globalized industry: the case of the shipping industry. *23*(4), 711-726.

Boboň, S. J. M. U. B., Czech Republic. (2021). Analysis of NIST FIPS 140-2 Security Certificates.

Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. J. C. (2014). Cybersecurity standards: Managing risk and creating resilience. *47*(9), 70-76.

Gaurav, A., Gupta, B. B., Hsu, C.-H., Yamaguchi, S., & Chui, K. T. (2021). Fog layer-based DDoS attack detection approach for internet-of-things (IoTs) devices. 2021 IEEE international conference on consumer electronics (ICCE),

Hemphill, T. A., & Longstreet, P. J. T. i. S. (2016). Financial data breaches in the US retail economy: Restoring confidence in information technology security standards. *44*, 30-38.

Kabay, M. J. C. s. h. (2012). History of computer crime. 2.1-2.41.

Khiralla, F. A. M. J. I. J. o. C. S., & Network. (2020). Statistics of cybercrime from 2016 to the first half of 2020. *9*(5), 252-261.

Macher, G., Schmittner, C., Veledar, O., & Brenner, E. (2020). ISO/SAE DIS 21434 automotive cybersecurity standard-in a nutshell. Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops: DECSoS 2020, DepDevOps 2020, USDAI 2020, and WAISE 2020, Lisbon, Portugal, September 15, 2020, Proceedings 39,

Nfuka, E., Sanga, C., & Mshangi, M. J. I. J. o. I. S. S. (2014). The rapid growth of cybercrimes affecting information systems in the global: is this a myth or reality in Tanzania? , *3*(2), 182-199.

NORTON, B. S. (2017). Norton Cyber Securitu Insights Report Global results.

Okereafor, K., & Adebola, O. (2020). Tackling the cybersecurity impacts of the corona virus outbreak as a challenge to internet safety.

Oluomachi, E., Ahmed, A., Ahmed, W., & Samson, E. J. a. p. a. (2024). Assessing The Effectiveness Of Current Cybersecurity Regulations And Policies In The US.

Purser, S. (2014). Standards for cyber security. In *Best practices in computer network defense: incident detection and response* (pp. 97-106). IOS Press.

Schmitz, C., Schmid, M., Harborth, D., Pape, S. J. C., & Security. (2021). Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. *108*, 102306.

Sheehan, B., Murphy, F., Mullins, M., Ryan, C. J. T. r. p. A. p., & practice. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *124*, 523-536.

Srinivas, J., Das, A. K., & Kumar, N. J. F. g. c. s. (2019). Government regulations in cyber security: Framework, standards and recommendations. *92*, 178-188.

Ventures, C. J. H. G. (2017). Cybersecurity jobs report. *1*.

White, K. (2013). The rise of cybercrime 1970 through 2010. A tour of the conditions that gave rise to cybercrime and the crimes themselves. In: ed.