Science and Technology Publishing (SCI & TECH)
ISSN: 2632-1017
Vol. 8 Issue 2, February - 2024

Cybersecurity Laws and Regulations

Umadevi Nakkolla
Industrial Technology - School of Industrial Sciences and Technology
University Of Central Missouri, Warrensburg, Missouri, United States
Uxn49860@ucmo.edu

Joseph Long
Engineering Technology – School of Industrial Sciences and Technology
University of Central Missouri, Warrensburg
Missouri, United States
jdlong@ucmo.edu

Abstract-This article provides an overview of the current state of cyber security laws and regulations, addressing the developing responses to the increasing complexities of the digital realm. The document underscores significant global and local policies, with a focus on the significance of adherence, safeguarding data, and managing incidents to mitigate cyber threats. The paper underscores the essential requirement for adaptable legal structures to ensure the safety of individuals, businesses, and critical infrastructures in an increasingly interconnected world, as emphasized in the analysis.

Keywords—Cybersecurity Regulations, Cybersecurity Compliance, International Cybersecurity Treaties, Regulatory Frameworks, Online Privacy Laws.

I. Introduction

In today's rapidly changing digital landscape, cyber security has taken center stage as a critical concern. Governments worldwide have responded by enacting comprehensive cyber security laws and regulations, aimed at protecting individuals, organizations, and vital infrastructure from the escalating threat of cyberattacks. These legal frameworks are designed to ensure the security of sensitive information, mitigate risks, and foster a secure and resilient online ecosystem. By enforcing these laws, authorities seek to create a safer digital environment while holding cybercriminals accountable. This article explores the fundamental aspects of cyber security laws and regulations, analyzing their significance, impact, and the challenges they address in an interconnected society.

II. Legislation and Regulations

Cyber laws, also known as Internet laws, are rules that govern software, e-commerce, information security, and the digital transfer of data. The use of the internet poses various security and privacy risks, with sophisticated criminals employing advanced tactics for illegal

activities and potential fraud. To safeguard against such threats, the implementation of a cyber security policy is crucial. These policies and laws aim to protect individuals and businesses by holding criminals accountable for their harmful actions and subjecting them to appropriate penalties set by the federal government. Cyber laws primarily address three key areas: Fraud, Copyright, and Defamation [1].

III. Cyber Security Laws in India

India has four primary laws concerning Cybersecurity:

- Information Technology Act (2000): Enacted by the Indian parliament, the Information Technology Act aims to safeguard the e-governance, e-banking, and e-commerce sectors. Its scope has expanded to encompass all modern communication devices.

- Indian Penal Code (IPC) (1860): This cybercrime prevention act primarily addresses identity theft and other cyber frauds related to sensitive information theft.

- Companies Act (2013): Passed in 2013, the Companies Act ensures regulatory compliance, including e-discovery, cyber forensics, and cybersecurity diligence. It also outlines the responsibilities of corporate directors and executives in confirming cybersecurity commitments.

- NIST Compliance: The National Institute of Standards and Technology (NIST)-approved Cybersecurity Framework (NCFS) covers all the necessary principles, standards, and best practices to effectively address cybersecurity risks [1].

IV. Cyber Security Laws in the USA

A. Federal Government- There are three major federal cybersecurity regulations:

- Health Insurance Portability and Accountability Act (HIPAA) (1996): HIPAA, approved by the 104th United States Congress, aims to regulate and modernize the transmission of medical and healthcare information.

- Gramm-Leach-Bliley Act (1999): The Gramm-Leach-Bliley Act, passed by the 106th United States Congress, requires financial institutions, including those providing loans, financial advice, or insurance, to disclose their information-sharing policies to customers and safeguard sensitive data.

- Homeland Security Act (2002): The Homeland Security Act includes the Federal Information Security Management Act (FISMA), which underscores the importance of information security in achieving the economic and national security objectives of the United States.

B. State Government

- Notice of Security Breach Act (2003): The Notice of Security Breach Act requires companies handling sensitive customer data, such as names, credit card numbers, social security numbers, and medical records, to publicly disclose any security breaches that occur within their organization. This regulation encourages businesses to allocate a significant portion of their budget to establish a secure infrastructure, thereby avoiding potential damage to their reputation.

- California Assembly Bill 1950 (2004): Enacted by the California State Legislature in 2004, this bill mandates businesses to maintain a reasonable level of cybersecurity and extend those security measures to their business partners to ensure an acceptable level of cybersecurity.

C. Proposed Regulation

The Consumer Data Security and Notification Act expands upon the Gramm-Leach-Bliley Act by requiring financial institutions to report any data breaches. The SPY Act (Securely Protect Yourself Against Cyber Trespass) was passed by the United States House of Representatives in 2005 but failed to pass in the Senate. It focused on addressing spyware and phishing frauds. The Cybersecurity Act of 2012, proposed in 2012, was not approved by the US Senate. It aimed to introduce anti-cybercrime legislation to enhance cybersecurity infrastructure and encourage businesses to adopt protective measures with incentives like liability protection. The Cybersecurity National Security Action Plan (CNAP), initiated by President Obama in 2016, aimed to raise public awareness about the increasing threat of cybercrime and educate individuals on how to strengthen and manage their digital security.

D. Other Government Efforts

The U.S. federal government has taken steps to enhance cybersecurity by increasing funding for research and collaborating with the private sector to establish appropriate standards and implement essential cyber laws. Additionally, the government has initiated various social media awareness campaigns to educate the public about the risks and threats of cybercrime [1].

After analyzing the Scope, Enforcement Mechanisms, and penalties of both countries the improvements required are:

V. Gaps and Areas for Improvement in India

- India could see improvements by strengthening the enforcement mechanisms for cybercrime laws, aiming for swift investigation and punishment of cyber offenses.

- Implementing more explicit and stringent penalties for cybercrime may discourage potential wrongdoers.

Regular updates to cybersecurity regulations are essential to address developing technology and cyber risks.

VI. Gaps and Areas for Improvement in the United States

- Having standardized and harmonized federal standards across states could enhance overall cybersecurity readiness and reaction.

- Enhanced collaboration between private industry and government entities can lead to the establishment of common standards and best practices.

Regulations should be regularly updated to address emerging cyber risks and technological advancements.

VII. International Cybersecurity Treaties and Agreements

President Biden and Prime Minister Modi have both restated their countries' commitment to an open, secure, inclusive, safe, interoperable, and reliable internet. They also pledged to continue their collaboration on various cybersecurity matters, including preventing and responding to cyber threats, advancing cybersecurity education and awareness, and working towards building resilient cyber infrastructure. The United States and India share a dedication to exchanging information on cyber threats and vulnerabilities and cooperating in investigating and managing cyber incidents [2].

Enforcing cybersecurity agreements between countries like the United States and India faces several obstacles due to the cross-border nature of cyber threats and the disparities in legal and regulatory frameworks. The key challenges are as follows:

- Jurisdictional Challenges: Determining jurisdiction in cyber incidents becomes complicated when attacks originate in one country but target systems in another, leading to jurisdictional issues in investigating and prosecuting cybercrimes.

- Legal and Regulatory Differences: The US and India have distinct legal and regulatory structures for addressing privacy and cybercrimes, making it difficult to work together and share information effectively.

- Cultural and Language Barriers: Different cultural values and language barriers may hinder effective communication and collaboration between the cybersecurity authorities of both countries during cyber incidents.

- Information Sharing Issues: Trust is crucial for sharing sensitive information about cyber threats and vulnerabilities, but concerns about data privacy and potential misuse of shared data can impede successful information exchange.

- Timing and Responsiveness: Prompt responses are crucial in managing cyber incidents, but coordination efforts might be delayed due to time zone variations or bureaucratic procedures.

- Differing Cybersecurity Priorities: Different cybersecurity objectives and focus areas in the US and India could impact the scope and effectiveness of their collaboration.

- Attribution Difficulties: Attributing cyberattacks to their true source can be challenging, as attackers often use sophisticated tactics to conceal their identity.

- Political Factors: Geopolitical and diplomatic considerations may influence country-to-country cybersecurity cooperation, especially if conflicts or disagreements exist over other issues.

- Lack of Cyber Law Harmonization: Differences in cyber laws and regulations between nations can hinder the implementation of agreements and coordinated responses to cyber incidents.

- Capacity and Resource Limitations: Unequal cybersecurity resources and skills in different countries may affect contributions in joint cybersecurity initiatives.

Despite these challenges, both the US and India are committed to collaborating on cybersecurity, and regular communication, trust-building measures, and priority alignment will be crucial in overcoming these obstacles. International agreements and standards promoting cross-border cooperation on cyber threats may also be necessary to strengthen the global cybersecurity ecosystem.

VIII. Privacy Laws and Data Protection Regulations

The California Consumer Privacy Act (CCPA) grants consumers more control over the personal information collected by businesses and provides guidelines for its implementation. This landmark law offers Californian consumers enhanced privacy protections, including the right to be informed about data collection, the option to delete personal data (with restrictions), the ability to opt out of data sharing or sales, and protection from unfair treatment when exercising CCPA rights.

Proposition 24, also known as the CPRA, was approved by California voters in 2020 and updated the CCPA with additional privacy provisions effective from January 1, 2023. Along with the rights mentioned earlier, customers gained new rights such as limiting the use of sensitive personal information and correcting inaccurate data held by businesses.

Businesses subject to the CCPA have several obligations, including responding to customer requests to exercise their rights and providing clear privacy notices. The CCPA applies to various businesses, including data brokers, ensuring a wide scope of privacy protection for California residents [3].

IX. Impact on Businesses

The CCPA and CPRA impose significant compliance requirements on companies dealing with the personal information of California residents. Companies must be transparent about their data collection practices, offer mechanisms for customers to exercise their rights, and maintain records of their data processing activities.

Data management and security are crucial for organizations to safeguard customer information and prevent unauthorized access or breaches. Failure to protect customer data may lead to severe fines and legal consequences. Businesses must implement procedures to handle customer requests regarding their personal information, including providing access, deletion, and honoring opt-out requests for data sharing or sales.

Handling sensitive personal information requires extra caution, and organizations must obtain explicit consent before processing such data. Companies selling or sharing personal information must be upfront about their practices and allow customers to opt out.

Non-compliance with the CCPA and CPRA may result in penalties and legal actions, with consumers having the right to sue companies for specific data breaches. The California Attorney General's Office oversees the enforcement of these regulations.

X. Impact on Individuals

In California, individuals have enhanced privacy rights, giving them more control over their personal information. They can be informed about the collection, usage, and sharing of their data. Customers have the right to access and control their personal information, including obtaining copies, correcting inaccuracies, or requesting deletion.

Individuals also have the option to opt out of having their data sold or shared with third parties for marketing or other purposes. Moreover, consumers are protected from discrimination based on their exercise of privacy rights, ensuring fair treatment in prices, goods, and services.

XI. Enforcement

The California Attorney General (AG) has the authority to enforce compliance with the CCPA and CPRA, and businesses found in violation may receive warnings, penalties, or legal action. Under the CCPA and CPRA, consumers have the right to sue companies in court if their non-encrypted and non-redacted personal information is exposed due to the

company's failure to implement reasonable security measures.

Non-compliance with the CCPA and CPRA can lead to civil fines and statutory damages for customers affected by data breaches. Both regulations aim to protect customers' privacy rights and hold businesses accountable for their data handling practices, promoting data protection, transparency, and consumer rights.

XII. Critical Infrastructure Protection

There are 16 sectors of critical infrastructure in the United States that are considered vital due to their significance to national security, economic stability, public health, and safety. Disruption or damage to any of these sectors could have severe and far-reaching consequences [4].

The National Cybersecurity Strategy, issued by the Biden-Harris Administration, aims to ensure that all Americans can benefit from a safe and secure digital environment. To achieve this, the strategy focuses on several key actions, including:

- Enhancing cybersecurity standards in critical industries to safeguard public safety and national security and streamlining compliance requirements.
- Promoting collaboration between the public and private sectors to protect critical infrastructure and essential services effectively.
- Securing and modernizing federal networks and updating incident response policies [4].

XIII. Government Surveillance Laws

While security measures aim to protect individuals from harm, privacy is crucial for safeguarding personal information and data. Balancing access to private information for security purposes with the right to privacy is essential to create a safer internet while respecting human rights.

Technology companies should develop solutions that effectively secure user data while implementing suitable security measures. Users, on the other hand, have a responsibility to protect their privacy by understanding how their data is collected, used, and shared, and taking necessary actions accordingly [5].

XIV. Examples of current government monitoring techniques include:

- Video Surveillance: Modern security cameras offer higher image quality and extensive storage capabilities. Governments commonly use traffic cameras and can access footage from private company security cameras.
- GPS Tracking: With the increasing use of smartphones and advancements in satellite technology, governments can track the location and activities of their citizens.
- Internet Activity Monitoring: Governments have the capability to monitor individuals' online behavior, including their communications, visited websites, and used programs or services.
- Algorithms and Artificial Intelligence: Governments utilize computer algorithms and artificial intelligence to identify behavioral patterns, gather information about individuals, and even predict their future actions. These tools can analyze online content, images, and biometric data such as faces, voices, gaits, fingerprints, and DNA [6].

XV. Incident Response and Reporting Requirements

A data breach occurs when there is a security incident that compromises the confidentiality, accessibility, or integrity of data under your business or organization's responsibility. If such a breach occurs and poses a risk to someone's rights and freedoms, you must notify the supervisory authority promptly, within 72 hours of becoming aware of the breach. If your company or organization is a data processor, you must inform the data controller about the breach.

All affected individuals must be notified if the data breach poses a high risk to their rights and freedoms unless adequate technological and organizational safeguards are in place to mitigate the risk. To prevent potential data breaches, it is essential for your organization to implement the necessary technical and organizational safeguards [7].

XVI. Cybercrime Laws and Challenges in Prosecuting Cybercriminals

Cybersecurity regulation in the United States is managed through a combination of federal and state laws. The Federal Trade Commission (FTC) is responsible for enforcing federal cybersecurity laws and regulations. Additionally, the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) play significant roles in cybersecurity regulation [8].

Investigating and prosecuting cybercrime is particularly challenging due to the global nature of cyber threats. Cybercriminals may operate from one jurisdiction but use infrastructure in another to target businesses or individuals in different countries, employing sophisticated techniques to amplify their criminal activities and evade law enforcement. Since cybercrime is a global problem, it requires a collaborative approach and close cooperation with other governments to find effective solutions [9].

XVII. Cybersecurity Standards and Frameworks

A cybersecurity framework provides a universal language and standardized set of guidelines for security leaders in various nations and businesses to communicate and assess their security postures, as well as those of their vendors. Having a framework simplifies the process of defining the activities and

procedures necessary for analyzing, managing, and mitigating cybersecurity risks within an organization. Some common cybersecurity frameworks include NIST Cybersecurity Framework, SOC2, NERC-CIP, HIPAA, GDPR, FISMA, ISO 27001, and ISO 27002 [10].

XVIII. Emerging Technologies and Regulations

The emergence of Industry 5.0, focusing on smart factories utilizing IoT, blockchain, and AI, presents cybersecurity challenges. Researchers propose solutions like blockchain-based intrusion detection systems (IDS) and access control to secure Industry 5.0 from DDoS, scanning, and data injection attacks.

Applying machine learning to IDS is suggested to monitor network activity and detect anomalies, reducing intrusion risks. For IoT privacy in the Internet of Vehicles (IoV), blockchain's data accuracy is valued, but privacy concerns remain, addressed by methods like ring signatures and pseudonym approaches. Various security mechanisms are required for different applications in Long-Range Wide-Area Networks (LoRaWAN). Researchers propose algorithms for LoRaWAN models. In the Industrial Internet of Things (IIoT), a novel method combining the Viterbi algorithm and indirect trust is suggested, maintaining transparency with blockchain.

Blockchain is recommended for EHR access control, presenting the Biometric-Based Electronic Health Record (BBEHR) system. A model using feature extraction and machine learning differentiates hazardous and benign communication. A blockchain-based system for continuous vehicle monitoring is proposed, and camera sensor networks use the cooperative relay tracking with prediction (CRP) method to enhance target tracking. These articles provide insights into blockchain and AI-based cybersecurity techniques for Industry 5.0 [11].

XIX. Compliance and Auditing

A cybersecurity compliance audit is conducted by a third-party agency to assess the presence of appropriate security systems and ensure adherence to regulatory requirements. Preparing for an external audit involves conducting a comprehensive internal audit.

An internal audit enables a thorough examination of all cybersecurity risks faced by the company. It facilitates an evaluation of existing defenses, assessing the effectiveness of policies, practices, and technologies in countering current threats.

The benefits of an internal audit of cybersecurity compliance are numerous. It allows the organization to gauge its progress in terms of data security. Through this self-evaluation, vulnerabilities can be identified and addressed proactively, reducing the likelihood of attackers exploiting weaknesses through breaches [12].

The level of an organization's safety is heavily influenced by the quality of its cybersecurity and data protection measures, as cyber incidents and data leaks can have severe impacts. It is essential for businesses to ensure their staff receives the best Ethical Hacking certification or follows cybersecurity guidelines. Compliance with cybersecurity regulations is crucial for several reasons, including:

- Avoiding Regulatory Penalties: Failure to comply with security laws can lead to significant fines and penalties for organizations. By implementing regulation-based cybersecurity planning, the likelihood of security breaches can be reduced.
- System of Risk Management: Cybersecurity compliance enables data protection, activity monitoring, network infrastructure safety, and security policies for authorization. These security regulations provide a set of guidelines for gathering, managing, storing, and sharing sensitive data, contributing to an effective risk management system [13].

XX. Digital Rights and Civil Liberties

Cybersecurity and privacy are closely intertwined, with privacy laws significantly impacting cybersecurity measures. These regulations emphasize the need for secure handling of customer information to prevent data leaks and breaches, and they require prompt notification in case of any data breaches.

The protection of information assets and ensuring confidentiality, integrity, and availability of data and systems are crucial aspects of cybersecurity and information security. Companies in regulated industries are legally obligated to maintain data and system performance, and compliance involves actions like breach reporting, implementing cybersecurity safeguards, and providing consumers with information and choices.

Organizations often deal with private information from consumers, customers, clients, and employees, which is covered by privacy laws. Compliance with these laws involves respecting consumer rights, breach notification, and implementing appropriate cybersecurity measures to protect personal data [14].

Data privacy is a key focus, particularly concerning the collection, storage, usage, and sharing of consumer data. Businesses must adhere to privacy laws, which grant consumers specific rights. Cybersecurity is vital in safeguarding against online threats such as identity theft and data breaches, providing protection for both organizations and individuals. Strong cybersecurity procedures are necessary for securing data and ensuring the safety of customers [15].

XXI. Cyber Security Education and Workforce Development

Despite the critical importance of cybersecurity for the security and prosperity of the United States, there is a significant shortage of cybersecurity

professionals. Efforts are being made to address this shortage by increasing the supply of skilled cybersecurity talent. However, one of the main challenges is the lack of qualified teachers who can deliver comprehensive cybersecurity instruction in high schools.

To enhance cybersecurity education in career and technical education (CTE), the U.S. Department of Education is working with other federal agencies on two initiatives: the Presidential Award for Cybersecurity Education and CTE CyberNet. These programs aim to create pathways from secondary education to postsecondary study and cybersecurity careers. The goal is to bridge the skills gap and meet the nation's demand for cybersecurity experts by supporting and recognizing CTE instructors who can effectively educate students for careers in cybersecurity [16].

XXII. Case Briefs

A. SHEIN fined US$1.9mn over data breach affecting 39 million customers:

The state of New York recently imposed a fine of $1.9 million on Zoetop Business Company, the parent firm of popular fashion brands SHEIN and ROMWE, for its failure to report a data breach that affected 39 million customers.

The data breach occurred in July 2018 when an unauthorized third party gained access to SHEIN's payment systems. After being alerted by the payment processor about potential intrusion and card data theft, SHEIN conducted an investigation and discovered that the personal and identifying information of 39 million customers had been compromised. This included email addresses, hashed account passwords, names, city/province information, and other data. Unfortunately, due to encryption flaws, the attackers were able to extract complete password credentials from the victims. The breach also impacted ROMWE, with the login information of approximately 7.3 million accounts stolen and later found for sale on the dark web in 2020.

An investigation by the New York Attorney General's office revealed various shortcomings in Zoetop's response to the incident. The company failed to prompt the 39 million affected individuals to change their account passwords. Instead, they only informed 6.4 million customers who had previously placed orders with SHEIN to reset their passwords. Furthermore, Zoetop changed the passwords for the affected ROMWE accounts without notifying the users of the data breach.

In addition, Zoetop issued a misleading press release on the SHEIN website's FAQ section, downplaying the severity of the breach. The press release denied evidence of credit card data theft, despite being informed otherwise, and falsely claimed that only 6.4 million customers were affected when the actual number was 39 million.

The investigation also found that Zoetop failed to provide the forensic investigator with access to the compromised systems and essential details about their data security practices. The company also neglected critical security measures, such as file integrity monitoring, log file analysis, audit trail retention, and quarterly network vulnerability scans. Additionally, they did not comply with PCI DSS requirements for protecting stored credit card data.

As a result of these failures, Zoetop faced significant fines from the state of New York for its negligence in protecting customer data and properly reporting the breach. This incident highlights the importance of robust cybersecurity protocols and transparent communication with consumers in the face of online threats [17].

B. Microsoft Azure Services Vulnerable To SSRF:

On January 17, 2023, Orca Security discovered four vulnerabilities in Microsoft Azure services that made them susceptible to server-side request forgery (SSRF) attacks. The affected services included Azure Functions, Azure Digital Twins, Azure Machine Learning, and Azure API Management. Microsoft promptly addressed and resolved the vulnerabilities, categorizing three of them as "Important" in severity and one as "Low." If left unpatched, these flaws could have allowed unauthorized access to internal resources, such as tokens, hostnames, security groups, MAC addresses, and user data. Fortunately, Microsoft's swift response mitigated the potential impact of these vulnerabilities and prevented significant harm.

- Response and Impact: According to Orca researcher Lidor Ben Shitrit, if left unaddressed, these SSRF vulnerabilities could have led to unauthorized access to internal resources and potential remote code execution. Microsoft's swift action helped mitigate the risks, underscoring the importance of robust authentication measures to prevent unauthorized access. An ongoing investigation is exploring possible connections to other security incidents.

- Preventive Measures: To enhance cloud infrastructure security and reduce SSRF risks, crucial steps include continuous monitoring, implementing the principle of least privilege, adopting network segmentation, and leveraging built-in security features provided by cloud providers like Microsoft Azure.

By adopting a comprehensive approach to cloud security, organizations can effectively protect themselves against SSRF attacks and other cyber threats [18].

C. Microsoft Exchange was used to hack diplomats long before the 2021 cyber attack

Researchers from Re-Security, a Los Angeles-based cybersecurity firm, stumbled upon a significant amount of stolen data while investigating the hack of an Italian retailer. The stolen data, totaling five gigabytes, was acquired by hacking into on-premises Microsoft Exchange servers of foreign ministries and energy companies over a span of three and a half years. The stolen information included data from eight energy corporations in the Middle East, Asia, and Eastern Europe, as well as correspondence from six foreign governments.

These attacks, not previously disclosed, occurred between January and March of the same year, preceding a highly publicized compromise of Microsoft Exchange servers. The 2021 attack, attributed to the Chinese state-sponsored group Hafnium, impacted around 60,000 individuals worldwide with malware. Although Resecurity cannot definitively ascertain if the same group was behind the earlier attacks, the stolen documents contained information that would be of interest to the Chinese government. Other cybersecurity experts warned that multiple countries might have been interested in the sensitive data related to Middle Eastern diplomacy and influential energy companies.

For years, hackers have exploited vulnerabilities in Microsoft's on-premises email systems to gain access to sensitive information from both public and private sector organizations. The Chinese government denied any involvement in these attacks and emphasized its opposition to online intrusion or attacks. Microsoft acknowledged that email systems are frequently targeted by nation-state actors seeking sensitive information, and they continuously collaborate with security partners to identify and address vulnerabilities.

The stolen data included diplomatic cables, critical network information, usernames, passwords, and confidential customer data. Re-security researchers found documents from foreign ministries and routine business activities, such as personnel changes, news summaries, autograph requests, and invitations to diplomatic conferences. Some affected countries acknowledged the cyberattacks but claimed no negative consequences, while others did not respond to inquiries.

The hackers primarily targeted state-owned utilities, research centers, and energy firms in regions spanning Eastern Europe to Southeast Asia. The compromised data, which included sensitive administrative information, proprietary data, user lists, internal network permissions, and password details, allowed hackers to expand their presence within victim networks. Among the affected organizations were Doosan Fuel Cell Co., the State Oil Company of Azerbaijan Republic (SOCAR), Sharjah National Lube Oil Corp. in the United Arab Emirates, the National Electric Power Company of Jordan, and the Institute for Nuclear Research in Romania, among others.

The 2021 attack targeted zero-day vulnerabilities in the Microsoft Exchange email system and impacted tens of thousands of individuals worldwide. After the initial compromise, both attacks followed similar patterns, using web shells to access each server's internal login page and Mimikatz, an open-source password-stealing program, to capture passwords. Cybersecurity experts noted that these techniques have become signature tactics for government-affiliated hacking groups, including some associated with the Chinese government [19].

REFERENCES

[1] Narasimman, P. (2023, July 13). *Cyber security laws and regulations of 2023*. KnowledgeHut. https://www.knowledgehut.com/blog/security/cyber-security-laws

[2] The United States Government. (2023, June 22). *Joint statement from the United States and India*. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/06/22/joint-statement-from-the-united-states-and-india/

[3] Bonta, R. (2023, May 10). *California Consumer Privacy Act (CCPA)*. State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa

[4] Cybersecurity & Infrastructure Security Agency. (n.d.). *Critical Infrastructure Sectors*. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[5] Bessadi, N. (2023, April 20). *How can we balance security and privacy in the Digital World?* Diplo. https://www.diplomacy.edu/blog/how-can-we-balance-security-and-privacy-in-the-digital-world/

[6] Kitazawa, E. (2022, December 2). Government Surveillance: Examples of Global Monitoring. https://www.shortform.com/blog/government-surveillance-examples/

[7] *What is a data breach and what do we have to do in case of a data breach?* European Commission. (n.d.). https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en

[8] Brands, M. (2023, November 13). *Cybersecurity laws and legislation (2023)*. ConnectWise. https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation#

[9] Demers, C, J. (2023, July 17). *The Cybersecurity program*. Central District of California.

https://www.justice.gov/usao-cdca/outreach/cybersecurity-program

[10] Cisternelli, E. (2023, March 31). 7 cybersecurity frameworks that help reduce cyber risk. https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk

[11] Ferrag, A, M., Maglaras, L., & Benbouzid, M. (2023, May 11). Blockchain and Artificial Intelligence as Enablers of Cyber Security in the Era of IoT and IIoT Applications. https://www.mdpi.com/2224-2708/12/3/40

[12] Yacono, L. (2022, November 17). *Cybersecurity Compliance Audit: 6 steps to be compliant*. Cimcor. https://www.cimcor.com/blog/cybersecurity-compliance-audit#2-evaluate-existing-policies

[13] Sharma, K. (2023, July 13). Cybersecurity compliance: Frameworks, Benefits, Requirements. https://www.knowledgehut.com/blog/security/cyber-security-compliance

[14] Bandler, J. (2022, September 20). U.S. Privacy and Cybersecurity lows- an overview. https://resources.infosecinstitute.com/topic/u-s-privacy-and-cybersecurity-laws-an-overview/

[15] KnowledgeHut. (2023, July 13). Importance of cybersecurity: Need and Benefits. https://www.knowledgehut.com/blog/security/importance-of-cyber-security

[16] PCRN. (n.d.). Cybersecurity Education. Perkins Collaborative Resource Network. https://cte.ed.gov/initiatives/cybersecurity

[17] Powell, O. (October 14, 2022). SHEIN fined US$1.9mn over a data breach affecting 39 million customers. https://www.cshub.com/attacks/news/shein-fined-us19mn-over-data-breach-affecting-39-million-customers

[18] Gasic, D. (Jan 22, 2023). Microsoft Azure Services Vulnerable To SSRF. https://purplesec.us/security-insights/microsoft-azure-ssrf-vulnerabilities/

[19] Mehrotra, K. & Bloomberg. (August 4, 2021). Microsoft Exchange was used to hack diplomats long before the 2021 cyber attack. *Fortune.* https://fortune.com/2021/08/04/microsoft-exchange-cyber-attack-diplomats-china/