INTERNATIONAL SEVEN JOURNAL
OF MULTIDISCIPLINARY
ISSN: 2764-9547

Navigating cybersecurity challenges: Legal implications and organizational strategies

10.56238/isevmjv2n1-012
Recebimento dos originais: 01/12/2023
Aceitação para publicação: 02/07/2023

Jammylly Fonseca Silva

ABSTRACT

The increasing frequency and sophistication of cybersecurity incidents—such as data breaches, ransomware attacks, and system violations—highlight significant legal and organizational challenges. Despite rising investments in cybersecurity, these incidents continue to evolve, presenting complex issues for both corporations and regulators. Traditional legal frameworks, primarily focused on financial damages, fail to address non-financial harms like emotional and psychological impacts on consumers. Studies by Teichmann and Wittmann (2022) and Kilovaty (2021) reveal gaps in current cybersecurity laws, emphasizing the need to incorporate psychological damages and enhance corporate liability standards. Research by Frank, Grenier, and Pyzoha (2021) demonstrates the increasing litigation risks for boards of directors following cybersecurity incidents. Their findings suggest that prior cyberattacks raise the likelihood of being held liable, though implementing frameworks like the American Institute of Certified Public Accountants' (AICPA) risk management guidelines can mitigate these risks. Additionally, Eijkelenboom and Nieuwesteeg (2020) analyze the disclosure of cybersecurity information in Dutch annual reports, finding a lack of transparency despite legal requirements. Their study underscores the need for better self-regulation or potential legal mandates to improve cybersecurity reporting. Falowo et al. (2022) examine the impact of digital interconnectedness on cybersecurity risks, noting that malware and phishing attacks are prevalent. Their research highlights the importance of organizational preparedness and adherence to frameworks such as the National Institute of Standards and Technology (NIST) guidelines for effective incident response. Sen (2018) identifies ongoing technical, economic, legal, and behavioral challenges that hinder effective cybersecurity, advocating for new strategies to overcome these barriers. Overall, enhancing cybersecurity resilience requires a comprehensive approach, integrating improved legal frameworks, organizational transparency, and proactive risk management.

Keywords: Cybersecurity Incidents, Legal Responsibility, Psychological Harms, Regulatory Frameworks, Incident Response.

INTRODUCTION

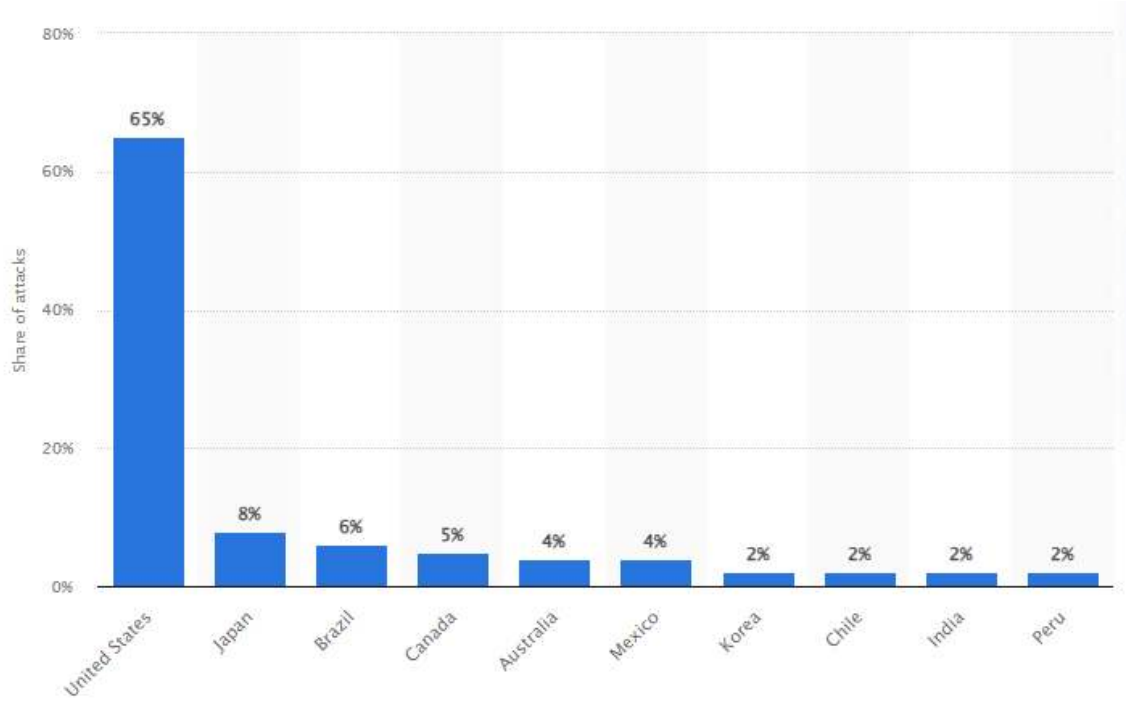
Cybersecurity incidents, including data breaches, ransomware attacks, and violations of cyber-physical systems, are becoming more frequent and sophisticated, raising significant concerns about their legal repercussions. As digital threats continuously evolve, the legal responsibilities of organizations involved in such incidents have become both critical and complex. Data protection laws, such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the US, impose specific obligations on

companies regarding personal data protection and notification. Non-compliance can lead to substantial financial penalties and damage to reputation.

Beyond data protection regulations, civil liability laws also play a crucial role. Organizations may face legal action for negligence if they fail to implement adequate security measures to safeguard their clients' and partners' information. Liability for damages to third parties, including customers and suppliers, may involve financial compensation for losses due to security breaches. Additionally, legislation is evolving to address the growing complexity of cybercrimes. New laws on cybercrime and cyberterrorism are being enacted to tackle severe attacks and their ramifications, while responsibilities for technology service providers and software developers are being reassessed, especially regarding system vulnerabilities exploited by attackers.

Effective management of cybersecurity incidents requires a proactive approach, including robust security measures, regular audits, and well-trained incident response teams. A swift and effective response, along with compliance with legal obligations for notification and communication, is crucial to mitigating legal consequences and maintaining organizational integrity.

Figure 1: Countries with the biggest share of prevented cyber attacks worldwide from September to November 2022. Source: Statista.



Teichmann and Wittmann (2022) delve into the evolving threat of cybercrime and its implications for corporate liability. Their study emphasizes that companies cannot rely on luck or naive assumptions to avoid cyberattacks. Instead, they must be aware of the liability risks associated with data breaches and privacy concerns, which are increasingly governed by emerging cybersecurity regulations. The authors stress the importance of proactive measures and highlight a significant gap in the literature regarding data security and liability regulations.

Katkova et al. (2020) focus on the legal responsibilities within cybersecurity, specifically examining the Ukrainian Law "On the Main Principles of Cybersecurity Provision in Ukraine" from October 5, 2017. This law encompasses responsibility for breaches in national security, electronic communications, and information security involving cyberspace. The study categorizes legal responsibilities into administrative, criminal, and civil domains and identifies a gap in the regulation of robotic liability.

Falowo et al. (2022) investigate the rise in digital interconnectedness and the increasing reliance on the internet for managing information, analyzing 803 significant cybersecurity incidents reported over the past decade. They find that malware and phishing techniques were responsible for a large portion of these incidents. The study emphasizes the need for organizational preparedness and recommends adopting the National Institute of Standards and Technology (NIST) incident response framework or similar guidelines for effective response.

Frank, Grenier, and Pyzoha (2021) explore the trend of increased lawsuits against boards of directors following cybersecurity incidents. Their research finds that directors are more likely to be held liable if a company has experienced a previous cyberattack. However, implementing the American Institute of Certified Public Accountants (AICPA) cybersecurity risk management framework can reduce this liability risk, particularly when external assurance is obtained.

Eijkelenboom and Nieuwesteeg (2020) examine the disclosure of cybersecurity information in Dutch annual reports from a financial law and economics perspective. Despite the absence of strict legal requirements, they find that a significant percentage of Dutch companies disclosed cybersecurity-related information in their 2018 reports. However, detailed disclosures were limited, potentially compromising stakeholder protection.

Kilovaty (2021) critiques cybersecurity law for focusing solely on financial harms from data breaches while neglecting the emotional and psychological impacts on consumers. The study argues for a new framework to address these non-financial harms, recommending a revision of the concept of "personal information" and the inclusion of additional protected information categories.

Sen (2018) analyzes the rising trend of cybersecurity incidents despite increased investments in security. The study identifies technical, economic, legal, and behavioral challenges that impede effective cybersecurity and highlights the limitations of recent initiatives by various stakeholders. The research underscores the need for innovative strategies and solutions to overcome these persistent barriers and enhance cybersecurity protection.

In conclusion, the increasing frequency and sophistication of cybersecurity incidents underscore the urgent need for comprehensive legal and organizational strategies to address their multifaceted challenges. The evolving landscape of digital threats and the expanding scope of regulatory frameworks highlight the critical importance of robust cybersecurity measures and proactive risk management. While current legislation, such as data protection laws and civil liability statutes, provides a foundation for addressing financial harms and negligence, there remains a significant gap in recognizing and addressing non-financial damages, such as emotional and psychological impacts.

Studies by Teichmann and Wittmann (2022) and Kilovaty (2021) reveal the necessity for a broader perspective on corporate liability and the inclusion of psychological harms within cybersecurity law. Similarly, research by Frank, Grenier, and Pyzoha (2021) demonstrates the increasing litigation risks for corporate boards, emphasizing the need for adherence to frameworks like the AICPA guidelines to mitigate liability. Furthermore, Eijkelenboom and Nieuwesteeg (2020) and Falowo et al. (2022) highlight the importance of transparency and organizational preparedness in managing cybersecurity risks effectively.

The legal landscape must continue to evolve, addressing both financial and non-financial damages and incorporating advancements in cyber threat management. As cyber threats become more sophisticated, companies must not only comply with existing regulations but also adopt proactive measures to protect stakeholders and enhance overall cybersecurity resilience. By integrating these findings and recommendations, organizations and policymakers can better navigate the complexities of cybersecurity, ultimately improving protection and response to digital threats.

REFERENCES

1. Eijkelenboom, E., & Nieuwesteeg, B. (2020). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law & Security Review, 40*, 105513. https://doi.org/10.2139/ssrn.3667418

2. Falowo, O., Popoola, S., Riep, J., Adewopo, V., & Koch, J. (2022). Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents. *IEEE Access, 10*, 134038-134051. https://doi.org/10.1109/ACCESS.2022.3231847

3. Frank, M., Grenier, J., & Pyzoha, J. (2021). Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework. *Journal of Accounting and Public Policy*, 106860. https://doi.org/10.1016/J.JACCPUBPOL.2021.106860

4. Katkova, T., Stiebieliev, A., Chmykhun, S., & Mkrtchan, M. (2020). Provision of cybersecurity in Ukraine: Issues of legal responsibility. https://doi.org/10.1007/978-3-030-37618-5_22

5. Kilovaty, I. (2021). Psychological data breach harms. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3785734

6. Sen, R. (2018). Challenges to cybersecurity: Current state of affairs. *Communications of the Association for Information Systems, 43*, 2. https://doi.org/10.17705/1CAIS.04302

7. Teichmann, F., & Wittmann, C. (2022). When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. *Journal of Financial Crime*. https://doi.org/10.1108/jfc-04-2022-0093