# Regulating Cyber Incidents: A Review of Recent Reporting Requirements

Angelica Marotta[a] and Stuart Madnick[b]
*MIT Sloan School of Management, U.S.A.*

Keywords: Cybersecurity, Regulatory Compliance, Incident Reporting.

Abstract: In today's digital landscape, cyber incidents have become more frequent and sophisticated, posing significant threats to organizations and individuals. To mitigate these risks, governments and regulatory bodies worldwide have developed various incident reporting regulations for organizations to follow. However, the effectiveness of these regulations in handling cyber incidents remains a point of debate. This paper focused on examining current cyber incident reporting regulations and their characteristics, with the primary objective of identifying the regulatory factors that impact the effectiveness of these regulations. Key aspects under investigation included timing requirements, the clarity in defining cyber incidents, and the provision of explicit guidelines regarding the necessity and scope of reporting incidents. Finally, it provides insights into how regulatory requirements can be improved to better handle cyber incidents in today's rapidly evolving regulatory environment.

## 1 INTRODUCTION

The increased reliance on digital technologies and the rise of ransomware attacks made the start of the 2020s a particularly vulnerable period for cybersecurity. For example, in March 2021, the Health Service Executive (HSE) of Ireland was attacked using a particular type of ransomware called "Conti," which caused prolonged interruption of care provision in the nation's healthcare system and severely affected critical services, such as gynecology and maternity clinics as well as cancer and children's care (Ivanković et al., 2023). Other attacks, including the JBS Foods ransomware attack, the Kaseya supply-chain attack, and the Accellion data breach, highlighted the persistent and evolving nature of these threats and demonstrated the need to adequately regulate reporting mechanisms (Bunge, 2021; Merken, 2022; Whitney, 2021). In the past, most reporting requirements were based primarily on privacy issues, in particular, the disclosure of Personal Identifiable Information (PII). Thus, cyber-attacks that shut down factories and many forms of ransomware were not required to be reported if no PII was disclosed.

The need for cyber incident reporting regulations has become increasingly important as the frequency and severity of cyber-attacks continue to rise. Over the years, significant developments have been made in developing cyber incident reporting regulations, including establishing cybersecurity agencies and creating cyber threat intelligence sharing platforms. For instance, in the United States, the National Institute of Standards and Technology (NIST) has developed a comprehensive framework for improving critical infrastructure cybersecurity (Ross et al., 2021). The framework provides a set of standards, guidelines, and best practices to help organizations better manage and reduce cyber risks. Additionally, the Department of Homeland Security (DHS) has established the Cybersecurity and Infrastructure Security Agency (CISA), which serves as the nation's lead agency for cybersecurity (Cybersecurity and Infrastructure Security Agency, n.d.). CISA helps to coordinate the response to cyber incidents and provides guidance to organizations on how to improve their cybersecurity posture. Thus, agencies such as NIST and CISA play a critical role in developing and supporting regulatory efforts. For example, in 2021, President Biden issued Executive

[a] https://orcid.org/0000-0002-0021-1305
[b] https://orcid.org/0000-0001-9240-2573

Marotta, A. and Madnick, S.
Regulating Cyber Incidents: A Review of Recent Reporting Requirements.
DOI: 10.5220/0012086000003555
In *Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023)*, pages 410-416
ISBN: 978-989-758-666-8; ISSN: 2184-7711

Order on Improving the Nation's Cybersecurity (EO 14028), which outlines several important steps organizations and government agencies must take to protect themselves from cybersecurity threats (Executive Order on Improving the Nation's Cybersecurity, 2021). To further clarify the Order, the Office of Management and Budget (OMB) issued a memorandum in September 2022 specifying that agencies must adhere to the NIST Guidance (Boyens et al., 2013; Young, 2022). This guidance recommends that organizations have an incident response plan in place and ensure that employees are adequately trained to respond to cybersecurity threats.

Another regulation aimed at improving the nation's cybersecurity posture by strengthening incident reporting and response capabilities is the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which was signed into law in March 2022. CIRCIA requires critical infrastructure organizations to report any cyber incidents to CISA within a specified timeframe. Therefore, this highlights the crucial role that CISA plays in incident reporting and response.

These developments have helped to enhance the effectiveness of cyber incident reporting regulations and ensure timely responses to cyber incidents. However, despite the recent regulations surrounding cyber incident reporting, organizations still struggle to implement these requirements effectively. For example, it is often difficult for organizations to collect accurate information on the nature, impacts, and frequency of attacks and report this information to the relevant regulatory authorities within the required reporting timeframe. Therefore, the effectiveness of these regulations depends on various factors, such as their timing requirements for reporting and their clarity in defining a cyber incident and what should be reported. This study seeks to examine recent cyber incident reporting regulations and their characteristics, with a focus on determining the regulatory factors that impact the effectiveness of cyber incident reporting rules. Finally, this study provides insights into how reporting regulatory efforts can be improved to better address the growing issue of handling cyber incidents in an effective manner.

## 2 RELATED LITERATURE REVIEW

Among the most significant regulatory developments in cybersecurity, incident reporting has been specified by several authors as a crucial regulatory element, requiring organizations to quickly report any security incidents and take necessary measures (Michalec et al., 2022; Silverajan & Vistiaho, 2019; Slonka, 2020). In particular, most experts agree that many cyber incidents involve a country's Critical National Infrastructure (CNI) (Gkioulos & Chowdhury, 2021; Maglaras et al., 2019). For example, the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) was one of the first incident reporting regulations specifically designed to ensure the security of critical infrastructure systems and protect sensitive data (Awati, 2022). Consequently, critical infrastructure protection has emerged in the literature as a pressing concern and a critical area to examine as part of the new regulatory landscape surrounding incident reporting (Slayton & Clark-Ginsberg, 2018).

However, some scholars argued that these regulations present several challenges (Madnick, 2022a; Silverajan & Vistiaho, 2019). For instance, one problem is that most countries' cybersecurity-related laws have focused on privacy rather than cybersecurity, leaving companies without the necessary tools and information to report incidents and counter cyber threats (Madnick, 2022b). One example of privacy-centered regulation is the General Data Protection Regulation (GDPR) (The European Parliament and the Council of the European Union, 2016). Marotta and Madnick (2021) argued that while progress has been made in improving cybersecurity through GDPR, organizations cannot assume that the requirements imposed by the legislation are enough to handle cybersecurity and effectively report any cyber incident. On the other hand, Andreasson and Fallen (2018) presented a different perspective on this topic, highlighting the importance of balancing security objectives with other regulatory goals, such as privacy, to achieve cyber resiliency.

Several authors also argued that organizations face the challenge of balancing reporting and confidentiality. For example, Johnson (2015) argued that revealing the details of a security incident can expose vulnerabilities or assets that can trigger further attacks. Therefore, this dilemma may hinder compliance with regulations and reporting incidents effectively. The author also stressed the importance of unifying cyber-reporting requirements and mechanisms to reduce the complexity of reporting to different industry regulators and entities, such as national infrastructure protection agencies, law enforcement, and Computer Emergency Response Teams (CERTs). Similarly, Parlour (2019) raised concerns about regulatory fragmentation and the need to determine the best cyber-incident framework to improve cyber resilience. Wolff (2016) supports this view, stating that regulators have distinct roles in promoting security reporting goals. For example, some incident reporting regulations are intended to protect consumers from cyber threats, while others aim to aid real-time detection and response. As a result, meeting reporting expectations can be a daunting task for organizations, as they are subject to varying requirements with respect to timing of reporting, the type of information that needs to be reported, and the parties to whom the reports must be submitted.

Having reviewed the major academic viewpoints on incident reporting regulations, it is important to explore how the resulting issues analyzed in the literature could have been beneficial in practical situations. By scrutinizing case studies of past incidents, we can identify the areas where incident reporting regulations could have effectively prevented or reduced such incidents' effects. In the following section, we will delve into some notable cyber-attacks where incident reporting regulations could have had a substantial impact.

# 3 POTENTIAL IMPACTS OF INCIDENT REPORTING REGULATIONS IN PAST INCIDENTS

Cyber incident reporting regulations have become increasingly important for organizations, as they provide numerous advantages. These regulations help organizations keep track of incidents and reduce future occurrences, inform policy decisions, identify potential risks, and incentivize organizations to take preventative or corrective measures. Additionally, incident reporting builds trust between organizations and their customers.

In the past, there have been cyber-related incidents where reporting could have helped to avoid or contain data breaches.

For example, we know that ransomware attacks continue to spread around the world. The National Vulnerability Database (NVD) contains a list of over 200,000 Common Vulnerabilities and Exposures (CVE) (NIST, n.d.-a, n.d.-b). Many of these CVEs could be used to initiate a ransomware attack. It would be an enormous effort for a company to try to resolve all of these CVEs. But, it turns out that only a very small subset of these CVEs are actually being exploited by ransomers (SOCRadar, 2022). By knowing these CVEs, companies can more efficiently focus their energy to defend themselves against these vulnerabilities. This would not be possible if the actual vulnerabilities being exploited by ransomware gangs was not reported.

However, despite the introduction of more stringent regulations in the following years, many cyber incidents still remained unreported due to confidentiality issues and regulatory loopholes, which provided room for interpretation. The 2021 Colonial Pipeline attack highlighted this problem, as the company was not legally obligated to disclose the incident due to the lack of personal data being stolen (Madnick, 2022b). As a result, this attack served as a powerful wake-up call, highlighting the need to ensure that cyber incidents are adequately regulated. In response to this event, the Transportation Security Administration (TSA) quickly issued a mandate[1] requiring pipeline operators to publicly report any cyber incidents within 12 hours, conduct regular security assessments, and appoint a coordinator in the event of a breach (Uberti, 2022).

Cyber incidents such as those described above have provided important lessons about the significance of incident reporting in regulations. The first lesson learned is the importance of timing in reporting. For example, in the WannaCry ransomware attack, timely reporting could have been crucial in preventing cyber-attacks. It would have allowed for the rapid identification and patching of vulnerabilities, preventing attackers from exploiting them. Furthermore, it would have enabled authorities to take necessary steps to contain the damage caused by the attack and prevent similar incidents from occurring in the future.

The second lesson learned is the importance of defining a cyber incident in regulations. The Colonial Pipeline attack showed that a more precise understanding of what constitutes a cyber incident is necessary to ensure that incidents are reported accurately and uniformly, avoiding ambiguity and confusion. The lack of clear guidelines on the definition of a cyber incident allowed the company to

[1] The TSA issued two directives in 2021 concerning pipeline cybersecurity. In May 2021, the TSA issued the first directive (SD-01), and in July 2021, the second directive (SD-02) was issued, known as the "TSA Pipeline Security Directive 2021-02 Series". The second directive expired on July 26, 2022, after which the TSA issued a third directive, which came into effect on July 27, 2022 (Security Directive Pipeline-2021-02C, also referred to as “SD02C”) (Security Administration Transportation, 2021).

avoid reporting the incident, which could have led to a better response and prevented further damage. Therefore, accurately defining cyber incidents in regulations is crucial to ensure that companies take necessary steps to protect themselves and their customers' data, and report any breaches promptly. Finally, these attacks also emphasized the need for more stringent and accurate incident reporting regulations that offer clarity to organizations in understanding the importance of reporting incidents and what needs to be reported. These regulations play a key role in ensuring that organizations are aware of their responsibilities and helping them take necessary actions to mitigate risks.

After analyzing the potential role of incident reporting regulations in previous incidents, it is crucial to further investigate and scrutinize the resulting lessons learned. By comprehending the drawbacks and areas of improvement highlighted by past incidents, it can be possible to enhance readiness for future events and limit their consequences. In the following sections, we will examine these lessons learned and explore how related regulatory factors can be applied to create more effective incident reporting regulations in the future.

# 4 REGULATORY FACTORS INFLUENCING THE EFFICACY OF CYBER INCIDENT REPORTING REGULATIONS

Considering the observations derived from the literature review and the analysis of past incidents, the efficacy of cyber incident reporting regulations seems to be influenced by several factors, including timing requirements, the clarity in understanding of what constitutes a cyber incident, and the provision of clear guidelines on why it is necessary to report incidents and what to report. The next sections examine each of these factors in detail.

## 4.1 Reporting Timing

Reporting cyber-attacks has its advantages and disadvantages when it comes to timing requirements. On the one hand, regulations such as the Network and Information Security (NIS2) Directive provide a sense of urgency, requiring that organizations report incidents as soon as possible (Directive (EU) 2016/1148, 2022). Similarly, the GDPR also requires organizations to report data breaches to EU data protection authorities within 72 hours (Article 33) and notify affected parties "with undue delay" (Article 34) if the breach poses a high risk to individuals' rights and freedoms (The European Parliament and the Council of the European Union, 2016). In the US, another regulation with a short reporting window is the New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500). This comprehensive cybersecurity framework applies to banking, insurance, and financial services companies operating in the state of New York (New York Consolidated Laws, 2022). This regulation requires supervised entities to submit incident reports to the Department of Financial Services (DFS) within 72 hours of becoming aware of any data breaches, unauthorized access attempts, and other cybersecurity-related events[2]. This can be beneficial in mitigating the damage caused by the attack.

Conversely, the California Consumer Privacy Act allows for a more generous 45-day period for reporting incidents, allowing organizations more time to analyze and report cyber-attacks. Another example of incident reporting regulation is the Critical Entities Resilience Directive (CER), designed to protect the availability, integrity, and confidentiality of critical infrastructure systems in the EU (Directive (EU) 2022/2557, 2023). The proposed Directive states that Member States must carry out regular risk assessments and have proactive measures to detect, report, and address cybersecurity incidents. However, reporting cyber-attacks has also prompted a regulatory concern about the different timing requirements for reporting a cybersecurity incident. Thus, determining which one to prioritize in case of conflicting deadlines can be challenging for organizations. Furthermore, it can be difficult to keep up with these regulations and comply with their deadlines, especially considering the varying types of incidents. For example, in March 2022, the US Securities and Exchange Commission (SEC), an agency of the federal government, issued a proposed rule[3], intending to improve and standardize cybersecurity risk management, strategy, governance, and incident reporting disclosure by public companies (The Securities and Exchange

[2] The NYDFS Cybersecurity Regulation mentions incident reporting in § 500.17 Notices to superintendent (a) Notice of cybersecurity event.

[3] The proposal is titled "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."

Commission, 2022). In particular, the SEC's requirement to report within four business days only applies if the attack is deemed "material." Determining whether an incident is "material" can be complex and time-consuming. Therefore, analyzing a cyber-attack can take weeks, and establishing materiality can be subjective. As a result, an incident that one company views as not material and, thus, is not reported, would not provide the useful information needed to prevent a similar attack on another company who would view it as very "material."

### 4.2 Definition of an Incident from a Security and Compliance Point of View

The digital landscape has changed considerably, making regulations often unsuitable for defining a cyber incident adequately. As a result, organizations face the challenge of determining which incidents qualify as cyber incidents and which do not. To address this issue, new or updated legislation was created to provide clearer definitions. For example, in 2020, the European Commission made a proposal to update the NIS Directive as part of the new EU Cybersecurity Strategy. As a result, the revised Directive (NISD2) provided a much more nuanced definition of a cyber incident than the one outlined in the previous version issued in 2016 (NISD) (Directive (EU) 2016/1148, 2022).

However, interpreting the regulations remains challenging, especially in determining if a cyber issue has the potential to become an incident. For example, according to one official definition provided by NIST, a cyber incident only requires an action that "imminently jeopardizes" a system or presents an "imminent threat" of violating a law (NIST, 2011). More specifically, a cyber incident is defined as an occurrence that:

(1) actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
(2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

This definition includes incidents that do not necessarily need to result in an actual security breach but could lead to one (Madnick, 2022a). An analogy to understand this issue is the aviation term "near miss" or "close call," which refers to the loss of safe separation between aircraft in flight (Thoroman et al., 2019). This particular circumstance can result in a mid-air collision in the worst-case scenario. A similar situation can occur in cybersecurity as well. Examples of such occurrences may include spear-phishing attacks targeting a particular organization or the discovery of evidence of a common vulnerability in a system. However, incidents such as failed login attempts or phishing email reporting may not necessarily qualify as cyber incidents. This lack of clarity surrounding cyber "near miss" leaves organizations navigating in a gray area as to what should count as a cybersecurity incident. Therefore, it is critical to have a clear and comprehensive definition of cyber incidents to ensure that organizations can identify and respond to them adequately.

### 4.3 Why Report Incidents and What to Report

The question of exactly why to report incidents and what to report is rarely answered with a single, definitive response. There are many different possible options, including the need to identify the type of attack that happened, the methods used, and the impact of the incident. Reporting incidents can help organizations get statistics and know what may be coming their way, thus improving their ability to prepare for future attacks. In this regard, several regulations on cyber incident reporting have been implemented in many countries to ensure that organizations report incidents that could significantly impact the public and share awareness of incident reporting. For example, in some countries, regulations require organizations to report any cyber incident, regardless of the severity. These regulations have been effective in making organizations understand why and what to report. The success of these regulations can be seen in the increased number of reported incidents, which has helped to improve the overall understanding of cyber threats. However, there are also concerns that regulations can be too prescriptive and that organizations may not report incidents that they consider minor, as they fear negative publicity or are not adequately trained. For example, only 288 out of roughly 200,000 vulnerabilities listed in the National Vulnerability Database (NVD) were exploited for ransomware attacks (Madnick, 2022b). To address these concerns, some regulations provide guidance on what should be reported and how to assess the impact of an incident, but there is still a need for further education and support to ensure that all organizations are reporting incidents effectively.

# 5 CONCLUSION

Cyber incident reporting regulations have become increasingly important in today's digital landscape due to the rise of cyber threats and the need to timely intervene to counter them. However, the impact of these regulations requires significant changes throughout the organization, which are not just limited to the actions undertaken by security leaders, such as CISOs and CIOs. Top management and the Board must be fully aware of the scope of these regulations and review the related compliance procedures accordingly. Additionally, employees must be trained to understand current policies and processes. Particularly attention must also be devoted to understanding new concepts introduced in new regulations, such those concerning "materiality." The definition of materiality may play a critical role in determining which incidents should be reported; it can help organizations determine the significance or impact an incident could have on their operations, reputation, or financial stability. However, current regulations incorporating this concept may include vague requirements and guidance. Thus, organizations struggle to determine which incidents should be reported, leading to issues, such as underreporting or overreporting of incidents. As a consequence, underreporting incidents can result in regulators being unaware of potential threats, while overreporting incidents can lead to a waste of resources. It is, therefore, essential for regulators to enhance current regulatory initiatives and learn from the positive features of regulations, such as Security Directive Pipeline-2021-02C and Critical Entities Resilience Directive (CERD). For example, by incorporating clearer timelines for reporting incidents and expanding the definition of reportable incidents, regulators can ensure that organizations are aware of potential incidents that could adversely affect their business and customers. However, recently, there have been some notable improvements in the field of incident reporting. For instance, the Biden-Harris Administration unveiled a new National Cybersecurity Strategy on March 2, 2023, which aims to protect the United States' critical digital infrastructure (The White House, 2023). This strategy was developed in response to several cyber threats that posed a significant risk to public services in recent years. In particular, "Strategic Objective 1.4" under this strategy focuses on updating the Federal Incident Response Plans and Processes, which also includes enhancing the CIRCIA. More specifically, according to this objective, the Act will require all critical entities to report cyber incidents to the CISA "within hours." Thus, these timely notifications will enable faster incident response at the Federal level. The road to overcoming incident reporting challenges is still long. However, it is essential to advise regulators, either directly or through industry associations, to help improve regulations continually. Thus, organizations and regulators must work together to increase the quality and quantity of cyber-attack reporting and discuss regulatory issues through collaboration and feedback.

# REFERENCES

Executive Order on Improving the Nation's Cybersecurity, The White House 1 (2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Andreasson, A., & Fallen, N. (2018). External cybersecurity incident reporting for resilience. *Lecture Notes in Business Information Processing*, *330*, 3–17. https://doi.org/10.1007/978-3-319-99951-7_1

Awati, R. (2022, March). *What is NERC CIP (critical infrastructure protection)?* TechTarget. https://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection

Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2013). Supply Chain Risk Management Practices for Federal Information Systems and Organizations. *NIST Special Publication 800-161*, 1–282. https://doi.org/10.6028/NIST.SP.800-161R1-DRAFT2

Bunge, J. (2021). *JBS Paid $11 Million to Resolve Ransomware Attack*. Wall Street Journal. https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781

Cybersecurity and Infrastructure Security Agency. (n.d.). *CISA Cybersecurity Advisory Committee | CISA*. Retrieved March 15, 2023, from https://www.cisa.gov/resources-tools/groups/cisa-cybersecurity-advisory-committee

Directive (EU) 2016/1148. (2022, December). *NIS 2 Directive*. Official Journal of the European Union. https://www.nis-2-directive.com/

Directive (EU) 2022/2557. (2023, January 16). *The Critical Entities Resilience Directive (CER)*. Official Journal of the European Union as Directive. https://www.critical-entities-resilience-directive.com/

Gkioulos, V., & Chowdhury, N. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

Ivanković, D., Jansen, T., Barbazza, E., Fernandes, Ó. B., Klazinga, N., & Kringos, D. (2023). Status of the health information system in Ireland and its fitness to support health system performance assessment: a multimethod assessment based on stakeholder involvement. *Health Research Policy and Systems*, *21*(1), 1–12. https://doi.org/10.1186/S12961-022-00931-1/FIGURES/4

Johnson, C. W. (2015). Contrasting Approaches to Incident Reporting in the Development of Safety and Security--Critical Software. *Safecomp*, 19. http://www.dcs.gla.ac.uk/~johnson

Madnick, S. (2022a). *Why Companies Need to Start Sharing More Information About Cyberattacks*. https://www.wsj.com/

Madnick, S. (2022b, August 29). *New Cybersecurity Regulations Are Coming. Here's How to Prepare*. https://hbr.org/2022/08/new-cybersecurity-regulations-are-coming-heres-how-to-prepare

Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., & Janicke, H. (2019). Cyber Security: From Regulations and Policies to Practice. *Springer Proceedings in Business and Economics*, 763–770. https://doi.org/10.1007/978-3-030-12453-3_88

Marotta, A., & Madnick, S. (2021). A Framework for Investigating GDPR Compliance Through the Lens of Security. In Jamal Bentahar, I. Awan, M. Younas, & T.-M. Grønli (Eds.), *Mobile Web and Intelligent Information Systems* (pp. 16–31). Springer, Cham. https://doi.org/10.1007/978-3-030-83164-6_2

Merken, S. (2022). *Accellion reaches $8.1 mln settlement to resolve data breach litigation | Reuters*. Reuters. https://www.reuters.com/legal/litigation/accellion-reaches-81-mln-settlement-resolve-data-breach-litigation-2022-01-13/

Michalec, O., Milyaeva, S., & Rashid, A. (2022). When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures? *Big Data and Society*, *9*(1). https://doi.org/10.1177/20539517221108369

New York Consolidated Laws. (2022). Part 500 Cybersecurity Requirements for Financial Services Companies. In *Westlaw*. https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)

NIST. (n.d.-a). *CVEs and the NVD Process*. Retrieved May 3, 2023, from https://nvd.nist.gov/general/cve-process

NIST. (n.d.-b). *National Vulnerability Database - NVD Dashboard*. Retrieved May 3, 2023, from https://nvd.nist.gov/general/nvd-dashboard

NIST. (2011). *Computer Security Incident*. CSRC. https://doi.org/10.1007/springerreference_10815

Parlour, R. (2019). EU Cybersecurity Policy in the Financial Sector. *Journal of Financial Crime*, *26*(3), 666–668. https://doi.org/10.1108/JFC-07-2018-0073/FULL/PDF

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & Mcquaid, R. (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. *National Institute of Standards and Technology*, *2*(NIST Special Publication 800-160), 310. https://doi.org/10.6028/NIST.SP.800-160v2r1

Security Administration Transportation. (2021). *Security Directiver Pipeline 2021-02C (SD02C)*. https://www.cisa.gov/shields-up.

Silverajan, B., & Vistiaho, P. (2019). Enabling cybersecurity incident reporting and coordinated handling for maritime sector. *Proceedings - 2019 14th Asia Joint Conference on Information Security, AsiaJCIS 2019*, 88–95. https://doi.org/10.1109/AsiaJCIS.2019.000-1

Slayton, R., & Clark-Ginsberg, A. (2018). Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. *Regulation and Governance*, *12*(1), 115–130. https://doi.org/10.1111/rego.12168

Slonka, K. J. (2020). Managing Cyber Security Compliance Across Business Sectors. *Issues In Information Systems*, *21*(1), 22–29. https://doi.org/10.48009/1_iis_2020_22-29

SOCRadar. (2022). *Top Critical Vulnerabilities Used by Ransomware Groups -SOCRadar*. SOCRadar.Io. https://socradar.io/top-critical-vulnerabilities-used-by-ransomware-groups/

The European Parliament and the Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. In *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ES

The Securities and Exchange Commission. (2022). *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*. https://www.sec.gov/news/press-release/2022-39

The White House. (2023). National Cybersecurity Startegy. *U.S. Government Printing Office (GPO)*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Thoroman, B., Goode, N., Salmon, P., & Wooley, M. (2019). What went right? An analysis of the protective factors in aviation near misses. *Ergonomics*, *62*(2), 192–203. https://doi.org/10.1080/00140139.2018.1472804

Uberti, D. (2022). *TSA Eases Pipeline Cybersecurity Rules Issued After Colonial Hack*. Wall Street Journal. https://www.wsj.com/articles/tsa-eases-pipeline-cybersecurity-rules-issued-after-colonial-hack-11656511031

Whitney, L. (2021). *Kaseya supply chain attack impacts more than 1,000 companies | TechRepublic*. TechRepublic. https://www.techrepublic.com/article/kaseya-supply-chain-attack-impacts-more-than-1000-companies/

Wolff, J. (2016). Models for Cybersecurity Incident Information Sharing and Reporting Policies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2587398

Young, S. D. (2022). MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES. *The White House*. https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf.