Harmonizing Cyber Incident Reporting: Challenges in Definitional Consistency

Abstract

Cyber incidents have become a significant global risk, with costly repercussions for organizations in various sectors. The establishment of comprehensive cybersecurity laws has led to the development of varying definitions for cyber incidents. However, despite the importance of understanding cyber incidents, defining them remains a complex task due to the evolving threat landscape. This paper provides an overview of the current state of cyber incident definitions, their consistency and inconsistency across various regulations, and their implications. Furthermore, it discusses the potential benefits of more nuanced and comprehensive approaches to defining cyber incidents.

Introduction

Cyber incidents are increasing, with cyber-attacks targeting organizations across diverse industries. Consequently, countries have been introducing comprehensive cybersecurity laws, mandating companies to identify and report cyber incidents (Madnick, 2022). Regulators have used different definitions with varying degrees of precision relating to what a cyber incident is. For example, some definitions focus on incidents that impact critical infrastructure (e.g., power grids, transportation systems, or financial institutions), which can pose substantial risks to public safety, national security, or economic stability (Slayton & Clark-Ginsberg, 2018). Other definitions, such as the US SEC, focus on whether the cyber incident had a "material impact." Comprehending and categorizing these incident definitions is an important step towards a standardized language for organizations and stakeholders and enabling swifter identification, response, and recovery from cyber incidents (Marotta & Madnick, 2021).

Therefore, with cybercrime projected to cost the global economy $10.5 trillion annually in the coming period, grasping the scope of cyber incidents and their effects is crucial for protecting networks and systems (Morgan, 2020). Diverse regulatory goals further complicate this task. This paper aims to offer a comprehensive overview of the current state of cyber incident definitions, assess their consistency across multiple regulations, and investigate the implications of their variances. Finally, this paper presents recommendations for developing improved definitions of cyber incidents and discusses the potential advantages of more detailed and nuanced approaches.

Literature Review: Addressing the Diverse and Evolving Nature of Cybersecurity Risks in Incident Definitions

The challenge of defining cyber incidents in cybersecurity has been a persistent issue in the field (Johnson, 2015; Strupczewski, 2021). Researchers, including Curti et al. (2021), have proposed various approaches to address this issue, including the development of taxonomies for cyber risks that consider factors such as impact, threat actors, vulnerabilities, and attack techniques. Others have advocated for more nuanced and specific definitions within legal and regulatory contexts, as Thaw (2013) suggests, while some, such as Craig et al. (2015), have highlighted the inadequacy of current cyber laws in effectively regulating "proactive cybersecurity." Kesan and Zhang (2020) emphasized the need for multifaceted definitions that consider various incident types and their consequences for effective response and risk management.

This complexity is further illustrated by the diverse range of threat types, each presenting unique regulatory challenges (Albladi & Weir, 2020; Ayala, 2016; Böhme & Schwartz, 2006; Bunge, 2021; Grobler et al., 2021; Srinivas et al., 2019). Insider threats, for instance, involve both human and technological factors, making it difficult to establish clear boundaries between negligence and malicious intent (Marotta & Madnick, 2022). Similarly, the distinction between viruses and worms can be blurry, posing challenges for regulations to effectively cover both types of threats (Kienzle & Elder, 2003). Other cyber threats present their own definitional challenges (Bailey et al., 2009). For example, the Federal Communications Commission (FCC)

has established guidelines for Internet Service Providers (ISPs) to detect and mitigate botnet[1] activities ("U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)," 2012). However, defining the point at which a device becomes part of a botnet may be unclear (van Eeten, 2017). Similarly, the US government has issued guidelines for organizations to follow to prevent and respond to ransomware[2] attacks, such as the "Ransomware Guide" published by CISA and MS-ISAC (CISA, 2020). However, defining ransomware incidents in regulations can be complex due to the changing attack vectors (e.g., phishing emails and drive-by downloads) (Kamil et al., 2022; Zimba, 2017). Furthermore, regulations mandating protective measures against malware such as rootkits, trojans, and spyware (Marotta & Madnick, 2021; Pierazzi et al., 2020), as well as password attacks (Slonka, 2020), encounter significant hurdles in their implementation. These difficulties arise primarily from the complexity of distinguishing between legitimate and malicious uses (Röpke & Holz, 2018) and identifying malicious intent (Grobler et al., 2021), which ultimately complicates the enforcement of effective cybersecurity policies.

Beyond these specific threat types, the concept of "near misses" in cybersecurity introduces an additional layer of complication to regulatory frameworks. Often overlooked, these incidents refer to potentially severe situations that were narrowly averted (Thoroman et al., 2019). To address this issue, lessons can be drawn from other fields; for instance, the US Federal Aviation Administration's model for defining near misses in aviation[3] offers valuable insights into cybersecurity (Bair et al., 2017). Nevertheless, a significant challenge remains: standard cyber incident definitions frequently fail to address the consequences of disclosing potential threats (Bair et al., 2017). Consequently, this oversight may inadvertently discourage information sharing due to concerns about potential liability or other complications, thus hindering the overall effectiveness of cybersecurity efforts (Madnick, 2022).

Methodology

To examine the definitions of cyber incidents, this study employed a systematic methodology, focusing on agencies and regulations from the United States and Europe[4] (Joyce et al., 2017). In particular, our investigation relied on an extensive regulatory database that was assembled as part of this research. We collected and analyzed about 200 enacted or proposed regulations through systematic database searches, including LexisNexis and official government repositories. The database was structured using an 8-column format[5], capturing key aspects of each regulatory element, as shown in the simplified examples below (Table 1):

Table 1: Examples of Regulatory Elements.

[1] Botnets are collections of infected and remotely controlled devices.

[2] Ransomware is a type of malware that encrypts an organization's data, demanding a ransom payment for their release (Kamil et al., 2022)

[3] The definition of a Near Midair Collision is "an incident associated with the operation of an aircraft in which a possibility of a collision occurs as a result of proximity of less than 500 feet to another aircraft, or a report is received from a pilot or flight crew member stating that a collision hazard existed between two or more aircraft" (NMACS System Information, n.d.).

[4] The focus on the US and Europe was a deliberate decision made to facilitate an in-depth analysis of the strategic efforts undertaken by some of the foremost agencies in the development of cybersecurity frameworks and guidelines. This targeted approach allowed for a more meaningful examination of the nuances and complexities associated with the current regulatory landscape in these regions. Additionally, this focused methodology lays the groundwork for future investigations and comparative research across a variety of regions. By examining the regulatory efforts of these leading regions in detail, researchers can better understand the strengths and weaknesses of different cybersecurity policies and frameworks. This, in turn, may help inform the development of more effective and efficient strategies for addressing cyber incidents on a global scale.

[5] Key aspects of the database included: ID (unique identifier), Actors/Country (involved entities/regions), Type (regulatory classification), Case (regulatory name), Source (responsible authority), Date (key timeline), Explanation (purpose and/or provisions), and Category (regulatory domain to which the regulatory element pertains). Some of the categories identified in this study included Incident Reporting, Required Software Bill of Materials (SBOMs), Security by Design requirements, Ransomware, Data Governance, Supply Chain Security, Critical Infrastructure, and Information Exchange.

ID	Actors/ Country	Type	Case	Source	Date	Explanation	Category
01	USA	Act	Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)	Cybersecurity and Infrastructure Security Agency (CISA)	Signed: 2022	Establishes a unified reporting system for critical infrastructure incidents	Critical Infrastructure, Incident Reporting, Ransomware, Information Exchange
02	EU	Directive	Network and Information Security Directive (NIS2)	European Parliament & Council of Europe	Adopted: 2022 Effective: 2023	Strengthens cybersecurity requirements across EU member states	Critical Infrastructure, Incident Reporting, Information Exchange, SBOMs

To ensure the robustness of our findings, we also conducted interviews with various executives from diverse industries (e.g., insurance, IT software and services, etc.), all of whom had at least 10 years' experience in cybersecurity and regulatory compliance. These interviews served as a critical qualitative component, providing industry insights and validating key points derived from our regulatory analysis.

The initial phase aimed to amass comprehensive information on cyber incident definitions (Fink, 2010). Following this phase, a comparative analysis of the definitions was conducted, identifying keywords, themes, similarities, limitations, and discrepancies among the various definitions provided by the agencies and regulations (Creswell, 2017; Creswell et al., 2007). The methodology employed a comparative approach to ensure an objective and consistent evaluation of the definitions (Gough et al., 2012; Kitchenham, 2004). The final stage involved synthesizing the findings from the data analysis to underscore the importance of harmonizing cybersecurity regulations and definitions and understanding of the current state of cyber incident definitions and their impact on the current efforts in addressing cyber threats.

Analysis: Agencies' and Regulations' Definitions of Cyber Incident

Several countries have agencies focused on cyber incident definitions and efficient regulatory protocols. In the US, there are industry-specific agencies such as the Securities and Exchange Commission (SEC), which oversees the financial sector, and regional bodies such as those found in individual US states like the California Office of Information Security (OIS) that address state-level cybersecurity concerns (Everett, 2003; The Securities and Exchange Commission, 2022). Additionally, in various parts of the world, there are specialized agencies, such as the Australian Cyber Security Centre (ACSC) and the National Cyber Security Centre (NCSC) in the United Kingdom (Australian Cyber Security Centre (ACSC), 2022; National Cyber Security Centre (NCSC), 2021). In this paper, we examined some of the most prominent cybersecurity agencies from the United States and Europe: NIST (National Institute of Standards and Technology), CISA (Cybersecurity and Infrastructure Security Agency), and ENISA (European Union Agency for Cybersecurity).

In this paper, we have specifically focused on the definitions provided by each agency, examining their respective contribution to formulating cyber incident definitions and their influence on the cybersecurity regulatory landscape. A summary of each agency's definition can be found in Table 2.

Table 2: Agencies' definitions.

Regulation	Definition of Cyber Incident
NIST	"An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." (NIST, n.d.)
CISA	"Report incidents as defined by NIST Special Publication 800-61 Rev 2, to include attempts to gain unauthorized access to a system or its data, unwanted disruption or denial of service, or abuse or misuse of a system or data in violation of policy" (CISA, n.d.)
ENISA	"an event [G.11] that has been assessed as having an actual or potentially adverse effect on the security or performance of a system" (ENISA, n.d.)

Approaches to Defining Cyber Incidents: NIST, CISA, and ENISA Perspectives

NIST provided several definitions of a cyber incident (or cyber event); for this study, we examined the definition referred to as "computer security incident," which captures the aspects impacted during a cyber event. The focus on confidentiality, integrity, and availability (often called the CIA triad) highlights the importance of safeguarding information assets. Furthermore, NIST acknowledges both actual and potential threats, potentially emphasizing the need for identifying and addressing "close calls" before they escalate into full-fledged incidents (NIST, 2011). However, although this definition is among the few that suggest the potential inclusion of "cyber near misses," the lack of further details about the impacts of sharing data on potential threats might inadvertently hinder the disclosure of near-miss information. As a result, cautious legal practices may suggest treating "imminent threats" as subjects for investigation or litigation. This approach could then discourage the sharing of information that reveals the existence of possible risks. NIST's expertise was instrumental to build a resilient and secure digital infrastructure, a cornerstone of the US cyber defense strategy under the Biden administration (Ross et al., 2021; The White House, 2023).

CISA's definition is influenced by NIST, with reference to NIST's Special Publication 800-61 Rev 2. In addition, it includes attempts to gain unauthorized access, unwanted disruption or denial of service, and abuse or misuse of a system or data in violation of policy.

Finally, the definition of a cyber incident provided by ENISA covers a broad range of events, emphasizing the importance of both security and performance in a system. However, the term "adverse" within the definition could have both advantages and disadvantages. Moreover, it does not explicitly mention the potential consequences, such as financial loss or reputational damage, which could limit its applicability in certain contexts.

While all three definitions address the negative impact of cyber incidents on information systems, NIST and CISA provide a more comprehensive view by including policy violations; ENISA's definition is succinct and centered on the adverse effects on security or performance.

The Role of Agencies' Definitions in US Cybersecurity Regulations

These definitions play a critical role in shaping cybersecurity regulations. For instance, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) aims to establish a unified reporting system for critical infrastructure incidents (CISA, 2022). Similarly, the New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500) sets baseline standards for financial institutions (NYDFS Proposes Amendments to Cybersecurity Regulation | Insights | Holland & Knight, n.d.). Furthermore, the Health Insurance Portability and Accountability Act (HIPAA) and NIST are related in the context of safeguarding sensitive health information. To help organizations comply with HIPAA's security requirements, NIST has published a set of guidelines (Bowen et al., 2008). The Federal Information Security Modernization Act of 2014 (FISMA) is influenced by NIST's definition and work on cyber incident handling and refers to events that can compromise the security of an information system or the information it contains, including violations or threats of violation of security policies, procedures, and acceptable use policies. In addition, NIST provided a comprehensive framework (NIST Risk Management Framework) for implementing an effective risk management program that meets FISMA requirements (CSRC, 2020).

The definitions of the regulations mentioned in this section are summarized in Table 3.

Table 3: Some Cybersecurity Regulations in the USA

Regulation	Definition of Cyber Incident
The Cyber Incident Reporting for Critical	An incident[6] that "actually" jeopardizes an information system, or the information contained on such a system. A threat of imminent harm to an information system, therefore, is not covered (CISA, 2022)

[6] This definition represents a simplified interpretation of the definition presented in the Act for reasons of clarity. In particular, CIRCIA refers to the existing definition of an "incident" from 6 U.S.C. § 659(a), which refers to a section of the United States Code that deals with the National Cybersecurity and Communications Integration Center (NCCIC) (6 USC 659: National Cybersecurity and Communications Integration Center, 2015). More specifically, this section defines "cyber incident" as follows: "the term "incident" means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system". However, CIRCIA also excludes any incident

Infrastructure Act (CIRCIA)	
NYDFS Cybersecurity Regulation	"Cybersecurity Event means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System." (NYDFS Proposes Amendments to Cybersecurity Regulation | Insights | Holland & Knight, n.d.)
HIPAA Security Rule	A "Security Incident" is defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations in an information system[7]." (Office for Civil Rights (OCR), 2013)
The Federal Information Security Modernization Act (FISMA)	An "incident" is "an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." (Federal Information Security Modernization Act of 2014, 2014)

The Role of Agencies' Definitions in EU Cybersecurity Regulations

In Europe, ENISA served as a driving force behind numerous EU regulations. A prime example is the NIS2 Directive (EU 2022/2555), which aims to advance cybersecurity throughout the EU (Directive (EU) 2016/1148, 2022; Wolff, 2016). The GDPR relies on ENISA's expertise to address cyber incidents. Similarly, the ePrivacy Directive benefits from ENISA's guidance for securing electronic communications and user privacy. Finally, the NIS2 Directive and the revised Payment Services Directive (PSD2) also leverage ENISA's definitions for improved cybersecurity posture and protecting sensitive payment information, respectively. It is worth noting that NIS2 is one of the few pieces of legislation incorporating the term "near miss." The inclusion of this definition reflects the European Commission's commitment to strengthen the cybersecurity posture of EU member states (Vandezande, 2024).

The definitions of the regulations mentioned in this section are summarized in Table 4.

Table 4: Cybersecurity Regulations in Europe

Regulation	Definition of Cyber Incident
General Data Protection Regulation (GDPR)	"A 'personal data breach' means a breach[8] of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (The European Parliament and the Council of the European Union, 2016)
ePrivacy Directive	""personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.'" (Directive 2009/136/EC of the European Parliament and of the Council, 2009)
Cybersecurity Act[9]/ Directive on Security of Network and Information	"(5) 'near miss' means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented

that "imminently, but not actually" jeopardizes information or information systems. Thus, near-miss events that do not result in actual harm or compromise seem to be excluded from this definition of a "cyber incident."

[7] This definition is broader than the one related to "breach" under HIPAA, which specifically involves the unauthorized acquisition, access, use, or disclosure of protected health information (PHI).

[8] The GDPR definition of a personal data breach specifically focuses on instances where personal data has been compromised due to security lapses. This includes scenarios involving accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data. While the definition does not explicitly mention attempted breaches, it is important to note that it primarily covers instances where an actual breach has occurred.

[9] The EU Cybersecurity Act cites Article 4(7) of Directive (EU) 2016/1148, also known as the "NIS Directive," for the definition of a cyber incident. However, the NIS 2 Directive (Directive EU 2022/2555) came into effect on January 16, 2023, and officially replaced the original NIS Directive, which was repealed on October 18, 2024. Given the updated regulatory framework, the NIS 2 Directive should now be referenced for the definition of a cyber incident. It is important to highlight the significance of incorporating the NIS definition into the Cybersecurity Act, as it strengthens the legal framework and fosters a unified approach to addressing cybersecurity threats across the European Union.

Systems 2 (NIS Directive2)	from materialising or that did not materialise; (6) 'incident'[10] means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems; (7) 'large-scale cybersecurity incident' means an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States;" (DIRECTIVE (EU) 2022/2555 (NIS 2 Directive), 2022)
Payment Services Directive (PSD2)[11]	"Operational or security incident" is "A singular event or a series of linked events unplanned by the payment service provider which has or will likely have an adverse impact on the integrity, availability, confidentiality and/or authenticity of payment-related services." (European Central Bank, 2018; Final Report Revised Guidelines on Major Incident Reporting under PSD2 FINAL REPORT ON THE REVISED GUIDELINES ON MAJOR INCIDENT REPORTING UNDER PSD2 2, 2021)

The influential definitions provided by those agencies play a crucial role in aligning various regulations with a common understanding of cyber incidents.

Comparative Analysis

Agencies' and regulations' definitions highlight specific keywords that can impact the comprehension of the cyber incident concept. A comparative table below (Table 5) showcases the inclusion of these terms across the regulations described in the previous sections:

Table 5: Comparative table

Keyword/ Theme	CIRCIA	NYDFS	HIPAA	FISMA	GD PR	ePrivacy	Cybersecurity Act / NIS Directive2	PSD 2
Incident	✓		✓	✓			✓	✓
Event		✓					✓	✓
Breach					✓	✓		
Occurrence				✓				
Unauthorized Access/ Disclosure		✓	✓		✓	✓	✓	
Disruption		✓					✓	
Misuse/Use		✓	✓					
Modification/Alteration			✓	✓				✓
Destruction				✓	✓	✓		
Integrity				✓			✓	✓
Confidentiality				✓			✓	✓
Availability				✓			✓	✓
Authenticity							✓	✓
Materialization							✓	
Security Policies				✓				
Violation				✓				
Interference			✓					
Imminent Threat/Near misses/ Attempt	✓[12]	✓	✓	✓			✓	
(Security of) Information Systems	✓	✓	✓	✓			✓	
Personal and Payment Data/ Electronic Communication Data	✓	✓	✓	✓	✓	✓	✓	✓

[10] Based on the definitions provided in the NIS 2 Directive, it can be inferred that the term "incident" in point (6) does not include "near misses" as described in point (5). While both terms refer to events that could compromise data or services, "near misses" are those that were successfully prevented from materializing or that did not materialize. On the other hand, this definition states that an "incident" specifically denotes an event that has compromised the data or services. Thus, in this case, the distinction between the two terms likely implies that the definition of an "incident" does not encompass "near misses."

[11] This definition can be found under the EBA Revised Guidelines on major incident reporting under PSD2

[12] Mentioned but not explicitly covered.

Services							✓	✓

The table above shows several similarities and discrepancies, highlighting the diverse perspectives on the subject matter.

Similarities: Various regulations and guidelines employ common themes and keywords that reflect the global efforts to manage cybersecurity risks. For instance, the NYDFS, GDPR, ePrivacy Directive, and NIS2 all stress the significance of safeguarding unauthorized access to personal and healthcare information. Other regulations like FISMA focus on reducing alterations and damage resulting from cybersecurity incidents. Another prevalent theme found in regulations such as FISMA, NIS2, and PSD2 is the emphasis on the CIA Triad[13], requiring organizations to establish controls that protect the integrity, confidentiality, and availability of information. Furthermore, personal data and information systems are identified as two primary assets in the definitions of these regulations. Commonality across regulations is also reflected in organizational practices, as one cybersecurity engineer at a large insurance company noted in an interview: "*If we have a breach, we have to notify the consumers who might be affected. That's pretty a standard requirement across regulations, like CCPA and GDPR, for example. It's up to our team to figure out what we can report and how to do it.*" This statement highlights the shared emphasis on breach notification and consumer protection across various regulatory frameworks.

Differences: Navigating regulatory frameworks also entails handling an inherent fragmentation, which is worsened by inconsistent terminology related to cyber incidents. Most regulations classify incidents as either "incidents" or "events," although both terms are slightly different meanings. An "incident" typically refers to an unplanned disruption affecting an organization's cyber infrastructure or information. A cyber incident does not always equate to a successful breach. In many cases, it refers to an "attempted breach," where malicious actors try to infiltrate a system or network but are ultimately unsuccessful. This distinction is crucial because it highlights the importance of proactive security measures and continuous monitoring to detect and thwart potential threats, including near misses. Conversely, an "event" is a broader term, encompassing any observable activity within a system. In addition, other regulations employ alternative expressions, such as "breach" and "occurrence." A "breach" denotes unauthorized access to or disclosure of sensitive data, while an "occurrence" is a more general concept, describing any event or situation that happens, regardless of whether it has a positive or negative impact. Moreover, regulations often overlook critical security terms in their definitions, including "authenticity," "materialization," and "imminent threats/near misses," which are included in some regulations. Finally, mentioning imminent threats and near misses, as seen in FISMA and NIS2, can help organizations proactively manage risks and enhance their security posture. In addition, both the NYDFS and the HIPAA Security Rule recognize the importance of addressing not only successful cyber incidents but also attempted ones. By including the term "attempt" or "attempted" in their definitions of a "Cybersecurity Event" and a "Security Incident," respectively, these regulations implicitly acknowledge the significance of "near misses" in the cybersecurity landscape. Regulations not mentioning these categories of incidents may not adequately prepare organizations for future incidents. The challenges posed by these varying definitions and requirements are also highlighted by a GRC program manager at an American software company who stated: "*Incident management, incident reporting, risk management - we deal with all these different things that they [regulations] ask for in slightly different ways. But really, the evidence we're providing to show that these controls are operating effectively is the same evidence we're using again and again.*" This observation underscores the operational inefficiencies created by the lack of standardization across regulatory frameworks, despite the underlying security principles remaining consistent.

Conclusions

Our analysis reveals significant variations in cyber incident definitions across regulations, leading to potential confusion and compliance challenges for organizations. These findings highlight the need for a unified approach to enhance global cybersecurity efforts. Developing a comprehensive and universally accepted definition of cyber incidents is essential. For example, it's crucial to create a unified terminology

[13] The CIA Triad, which stands for Confidentiality, Integrity, and Availability, serves as a guiding principle for information security. Confidentiality ensures that data is accessible only to authorized individuals. Integrity guarantees that the data remains accurate and unaltered, while availability confirms that authorized users can access the data when needed.

across regulations, ensuring clear definitions for terms like "incident," "event," "breach," and "occurrence." A standardized definition should also extend the CIA Triad (confidentiality, integrity, availability) and incorporate principles like authenticity. Additionally, industry-specific cybersecurity requirements, particularly for sectors, such as finance and healthcare, must be included, reflecting their unique regulatory needs. Focusing on shared themes such as unauthorized access, integrity, confidentiality, and availability can further form the basis for global collaboration in tackling cybersecurity issues. A position paper by the World Economic Forum's Systems of Cyber Resilience: Electricity initiative stresses the need for standardized approaches in this context (World Economic Forum, 2023). Future research should focus on developing a comprehensive framework that balances sector-specific needs with universal applicability, while evaluating the effectiveness of harmonized guidelines on incident reporting and response. This framework should also consider the impact of emerging threats, such as AI-driven attacks, on shaping incident definitions and explore ways to bridge regulatory gaps.

References

6 USC 659: National cybersecurity and communications integration center, United States Code 1 (2015). https://uscode.house.gov/view.xhtml?req=(title:6 section:659 edition:prelim)

Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1), 1–19. https://doi.org/10.1186/s42400-020-00047-5

Australian Cyber Security Centre (ACSC). (2022). *Who we are*. Cyber.Gov.Au. https://www.cyber.gov.au/about-us/about-acsc/who-we-are

Ayala, L. (2016). Cybersecurity for Hospitals and Healthcare Facilities. *Cybersecurity for Hospitals and Healthcare Facilities*. https://doi.org/10.1007/978-1-4842-2155-6

Bailey, M., Cooke, E., Jahanian, F., Xu, Y., & Karir, M. (2009). Al survey of botnet technology and defenses. *Proceedings - Cybersecurity Applications and Technology Conference for Homeland Security, CATCH 2009*, 299–304. https://doi.org/10.1109/CATCH.2009.40

Bair, J., Bellovin, S. M., Manley, A., Reid, B., & Shostack, A. (2017). That Was Close: Reward Reporting of Cybersecurity near Misses. *Colorado Technology Law Journal*, *16*. https://heinonline.org/HOL/Page?handle=hein.journals/jtelhtel16&id=353&div=22&collection=journals

Böhme, R., & Schwartz, G. (2006). Models and Measures for Correlation in Cyber-Insurance. *2006 Workshop on the Economics of Information Security (WEIS)*, *June 2006*, 1–26. https://www.semanticscholar.org/paper/24af7e7832277628c9fa108e31c31d75d3c494bc

Bowen, P., Johnson, A., Hash, J., Smith, C. D., & Steinberg, D. I. (2008). An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule. *NIST Special Publication*, *800*(October), 800–866. https://doi.org/10.6028/NIST.SP.800-66r1

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

CISA. (n.d.). *Report to CISA | CISA*. Cisa.Gov. Retrieved April 24, 2023, from https://www.cisa.gov/report

CISA. (2020). *CISA MS-ISAC Ransomware Guide*. https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware Guide_S508C.pdf

CISA. (2022). *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) | CISA*. https://www.cisa.gov/circia

Federal Information Security Modernization Act of 2014, 1 (2014) (testimony of US Congress). https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

Craig, A. N., Shackelford, S. J., & Hiller, J. S. (2015). Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis. *American Business Law Journal*, *52*(4), 721–787. https://doi.org/10.1111/ablj.12055

Creswell, J. W. (2017). Second Edition Qualitative Inquiry & Choosing Among Five Approaches Research Design. In *SAGE Publications*. https://www.researchgate.net/publication/342229325

Creswell, J. W., Hanson, W. E., Clark Plano, V. L., & Morales, A. (2007). Qualitative Research Designs: Selection and Implementation. *The Counseling Psychologist*, *35*(2), 236–264. https://doi.org/10.1177/0011000006287390

CSRC. (2020). *NIST Risk Management Framework | CSRC*. Nist.Gov. https://csrc.nist.gov/projects/risk-management/fisma-background%0Ahttps://csrc.nist.gov/Projects/risk-management

Curti, F., Gerlach, J., Kazinnik, S., Lee, M., & Mihov, A. (2021). Cyber Risk Definition and Classification for Financial Risk Management. *Federal Reserve Bank of Richmond*. https://advisenltd.com/

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

DIRECTIVE (EU) 2022/2555 (NIS 2 Directive), (2022).

Directive 2009/136/EC of the European Parliament and of the Council, (2009). https://edps.europa.eu/sites/default/files/publication/dir_2009_136_en.pdf

ENISA. (n.d.). *Glossary — Risk Management*. Retrieved April 24, 2023, from https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary

European Central Bank. (2018). *The revised Payment Services Directive (PSD2) and the transition to stronger payments security*. MIP OnLine. https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html

Everett, C. (2003). New Californian security law could pose problems for Europe. In *Computer Fraud and Security* (Vol. 2003, Issue 8, pp. 1–2). Elsevier BV. https://doi.org/10.1016/S1361-3723(03)08001-1

Final Report Revised Guidelines on major incident reporting under PSD2 FINAL REPORT ON THE REVISED GUIDELINES ON MAJOR INCIDENT REPORTING UNDER PSD2 2. (2021).

Gough, D., Thomas, J., & Oliver, S. (2012). Clarifying differences between review designs and methods. *Systematic Reviews*, *1*(1), 1–9. https://doi.org/10.1186/2046-4053-1-28

Grobler, M., Chamikara, M. A. P., Abbott, J., Jeong, J. J., Nepal, S., & Paris, C. (2021). The importance of social identity on password formulations. *Personal and Ubiquitous Computing*, *25*(5), 813–827. https://doi.org/10.1007/s00779-020-01477-1

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

Joyce, A. L., Evans, N., Tanzman, E. A., & Israeli, D. (2017). International cyber incident repository system: Information sharing on a global scale. *2016 IEEE International Conference on Cyber Conflict, CyCon U.S. 2016*. https://doi.org/10.1109/CYCONUS.2016.7836618

Kamil, S., Siti Norul, H. S. A., Firdaus, A., & Usman, O. L. (2022). The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges. *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*. https://doi.org/10.1109/ICBATS54253.2022.9759000

Kesan, J. P., & Zhang, L. (2020). Analysis of Cyber Incident Categories Based on Losses. *ACM Transactions on Management Information Systems*, *11*(4). https://doi.org/10.1145/3418288

Kienzle, D. M., & Elder, M. C. (2003). Recent worms: A survey and trends. *WORM'03 - Proceedings of the 2003 ACM Workshop on Rapid Malcode*, 1–10.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews, Version 1.0. In *Empirical Software Engineering* (Vol. 33, Issue 2004).

Madnick, S. (2022, 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

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

Marotta, A., & Madnick, S. (2022). Cybersecurity As a Unifying Factor for Privacy, Compliance and Trust: the Haga Hospital Case. *Issues In Information Systems*, *23*(1), 102–116. https://doi.org/10.48009/1_iis_2022_108

Morgan, S. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Cybersecurity Ventures. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

National Cyber Security Centre (NCSC). (2021). *What we do*. Www.Ncsc.Gov.Uk. https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

NIST. (n.d.). *Cyber risk - Glossary | CSRC*. Nist.Gov. Retrieved February 2, 2022, from https://csrc.nist.gov/glossary/term/cyber_risk

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

NMACS System Information. (n.d.). Federal Aviation Administration. Retrieved May 3, 2023, from https://www.asias.faa.gov/apex/f?p=100:35:::NO::P35_REGION_VAR:1

NYDFS Proposes Amendments to Cybersecurity Regulation | Insights | Holland & Knight. (n.d.). Retrieved February 23, 2023, from https://www.hklaw.com/en/insights/publications/2022/11/nydfs-proposes-amendments-to-cybersecurity-regulation

Office for Civil Rights (OCR). (2013). *2002-What does the Security Rule require a covered entity to do to comply with the Security Incidents Procedures standard*. HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/faq/2002/what-does-the-security-rule-require-a-covered-entity-to-do-to-comply/index.html

Pierazzi, F., Mezzour, G., Han, Q., Colajanni, M., & Subrahmanian, V. S. (2020). A Data-driven Characterization of Modern Android Spyware. *ACM Transactions on Management Information Systems*, *11*(1). https://doi.org/10.1145/3382158

Röpke, C., & Holz, T. (2018). Preventing malicious SDN applications from hiding adverse network manipulations. *SecSoN 2018 - Proceedings of the 2018 Workshop on Security in Softwarized Networks: Prospects and Challenges, Part of SIGCOMM 2018*, *18*, 40–45. https://doi.org/10.1145/3229616.3229620

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

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

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188.

https://doi.org/10.1016/j.future.2018.09.063
Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/j.ssci.2020.105143
Thaw, D. (2013). The Efficacy of Cybersecurity Regulation. *Georgia State University Law Review*, *30*. https://heinonline.org/HOL/Page?handle=hein.journals/gslr30&id=301&div=23&collection=journals
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 (General Data Protection Regulation - GDPR). 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 Strategy. *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
U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs). (2012). In *CSRIC III WG7 Final Report*.
van Eeten, M. (2017). Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. *Digital Policy, Regulation and Governance* , *19*(6), 429–448. https://doi.org/10.1108/DPRG-05-2017-0029
Wolff, J. (2016). Models for Cybersecurity Incident Information Sharing and Reporting Policies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2587398
World Economic Forum. (2023). *Facilitating Global Interoperability of Cyber Regulations in the Electricity Sector [Position Paper]*. https://www3.weforum.org/docs/WEF_Facilitating_Global_Interoperability_Cyber_Regulations_2023.pdf
Zimba, A. (2017). Malware-Free Intrusion: A Novel Approach to Ransomware Infection Vectors. *International Journal of Computer Science and Information Security*, *15*(2), 317–325. https://search.proquest.com/docview/1879494467?accountid=15977%5Cnhttp://su3pq4eq3l.search.serialssolution.com?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQ%3Acriminaljusticeperiodicals&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.ge