ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Compliance Considerations in Cyber Incident Response

Haritha Madhava Reddy

USA

ABSTRACT

As cyber threats become more frequent and sophisticated, organizations must prioritize both proactive prevention and efficient incident response strategies. Compliance plays a pivotal role in strengthening an organization's capacity to manage security breaches, safeguard sensitive data, and fulfill legal responsibilities. Moreover, the evolving nature of cyber threats, coupled with shifting regulations, highlights the need for organizations to continuously adapt. As such, key areas of focus include comprehensive risk assessment, building effective response teams, navigating regulatory frameworks, and leveraging advanced technologies. Ethical considerations, such as protecting privacy and ensuring transparent communication, are integral to maintaining a compliant and effective response. Ultimately, embedding compliance into incident response is not just a legal necessity but is strategically imperative for preserving organizational integrity, fostering stakeholder trust, and ensuring long-term resilience in a rapidly evolving digital environment.

***Corresponding author**

Haritha Madhava Reddy, USA.

Received: January 03, 2022; **Accepted:** January 14, 2022; **Published:** January 20, 2022

Keywords: Cyber Incident Response, Compliance, Data Protection, Regulatory Frameworks, Cybersecurity, Incident Response Plan, Data Breach, Risk Assessment, Legal Obligations, Ethical Considerations, GDPR, HIPAA, PCI DSS, Privacy

Introduction

Cyber incident response is an integral key to an organization's cybersecurity strategy. With cyber threats growing in complexity and frequency, it's no longer enough for organizations to simply focus on preventing incidents; they must also be well-prepared to respond effectively when incidents occur. An incident response plan that integrates compliance considerations serves as a powerful tool for quickly identifying, containing, mitigating, and recovering from security incidents [1]. At the same time, it helps organizations demonstrate their commitment to regulatory authorities and stakeholders, ensuring that they meet the standards required in their industry.

Furthermore, a thorough risk assessment forms the foundation of any incident response plan. It involves identifying potential threats, vulnerabilities, and their impact on both the organization and its compliance posture [2]. By aligning their incident response strategies with specific compliance requirements—whether it's GDPR, HIPAA, or PCI DSS, for example—organizations can ensure they address all necessary legal, regulatory, and industry obligations in their response efforts.

As such, an effective incident response requires a well-rounded team with expertise in various areas, including cybersecurity, legal, communications, and business operations. Importantly, members of this team must be trained in compliance-related issues, which ensures that during an incident, all necessary legal and regulatory duties are upheld, reducing the likelihood of non-compliance penalties.

Understanding the Regulatory Landscape

The regulatory environment for cybersecurity is increasingly complex and varies between industry, geographic region, and the type of data involved. As organizations face a diverse range of cyber threats, they must ensure that their incident response plans are not only effective but also fully compliant with applicable laws and regulations. Each regulatory framework sets specific requirements for how organizations should handle security incidents, including breach detection, containment, reporting, and recovery. Understanding these requirements is essential for avoiding legal repercussions, minimizing financial losses, and maintaining customer trust.

The GDPR, which came into effect in May 2018, is one of the most stringent data protection laws, applying to any organization that handles the personal data of individuals in the European Union (EU), regardless of where the organization is based [3]. One of the key mandates of GDPR is prompt notification of data breaches. Organizations must report certain types of breaches to the relevant authority within 72 hours of becoming aware of the incident, or unless the breach is unlikely to result in a risk to the rights and freedoms of individuals [4]. Failing to meet this strict timeline or mismanaging the response can lead to severe penalties. GDPR allows fines of up to €20 million or 4% of annual global turnover, whichever of the two is higher for the situation [5]. In addition to financial penalties, non-compliance can result in reputational damage, especially if organizations fail to notify affected individuals promptly. This notification must include details about the nature of the breach, consequences, and the measures being taken to mitigate the risks.

Next is the Health Insurance Portability and Accountability Act (HIPAA), or more specifically the HIPAA Security Rule, which sets forth requirements for protecting Protected Health Information

(PHI), primarily in the healthcare sector in the United States [6]. When a breach involving PHI occurs, covered entities and their business associates must follow a set of strict protocols to ensure compliance. HIPAA requires organizations to notify the U.S. Department of Health and Human Services (HHS), affected individuals, and, in some cases, the media, depending on the scale of the breach. The notification process for breaches under HIPAA must occur within 60 days of discovering the breach, but organizations are encouraged to notify as soon as possible [7]. The content of the notification must include a description of what happened, the types of information involved, the steps affected individuals should take, and what the organization is doing to investigate, mitigate harm, and prevent future breaches. In the case of non-compliance, civil penalties can range from $100 to $50,000 per violation, with a maximum annual penalty of $1,500,000 for repeated violations [8]. Additionally, organizations can face criminal charges if the breach involves intentional misuse of PHI. Thus, compliance with HIPAA during incident response is crucial for avoiding both financial penalties and legal action.

Another crucial regulatory framework, namely the Payment Card Industry Data Security Standard (PCI DSS) applies to organizations that handle payment card data. It establishes comprehensive requirements for safeguarding credit card information, with specific guidelines for incident response. When a breach involves payment card information, the PCI DSS mandates that organizations immediately contain the breach, prevent further data exposure, and notify relevant stakeholders, including payment card issuers and acquiring banks. PCI DSS requires organizations to have an established incident response plan that includes procedures for responding to a breach, analyzing the cause, and mitigating future risks [9]. Breaches involving payment card data often trigger mandatory forensic investigations by qualified security assessors (QSAs), who ensure that the organization has complied with PCI DSS standards [10]. Failure to meet these requirements can result in fines ranging from $5,000 to $100,000 per month [11]. Additionally, organizations may face increased transaction fees, reputational damage, and loss of the ability to process credit card payments altogether. This makes adherence to PCI DSS an essential component of any incident response strategy for organizations dealing with payment card data.

In addition to GDPR, HIPAA, and PCI DSS, other regulatory frameworks also impose strict requirements on how organizations should handle cyber incidents: Sarbanes-Oxley Act (SOX), which applies to publicly traded companies in the U.S. and mandates the protection of financial data and disclosure of cybersecurity risks to stakeholders; Cybersecurity Maturity Model Certification (CMMC) targets defense contractors in the United States and requiring them to meet specific cybersecurity standards to protect sensitive defense-related information; NIS Directive (EU Network and Information Security Directive), which requires essential service operators and digital service providers in the EU to notify national authorities of significant cyber incidents; California Consumer Privacy Act (CCPA), which imposes obligations on businesses to disclose data breaches and providing consumers with the right to sue for damages resulting from unauthorized access to their personal information [12-14]. There is an abundance more regulatory procedures that can be found between different countries and within our own, however, regardless of the compliance standard of interest, it can be certain that non-compliance with these regulatory frameworks during a cyber incident response can lead to a range of serious consequences. Such consequences result in significant Financial Penalties in the form of fines that can reach millions of dollars, with some regulations, such as GDPR, allowing fines based on a percentage of global revenue, making the financial impact potentially catastrophic. Similarly, failing to meet the notification requirements can erode customer trust, especially when sensitive data is involved; a delayed or improper response can result in significant reputational harm, which may take years to recover from. Organizations may face lawsuits, either from regulators or individuals affected by the breach, especially if there is evidence of negligence or a failure to protect sensitive information. In general, it can also be understood that investigations, fines, and other legal challenges can consume valuable resources, causing further disruption to business operations at a time when the organization is already dealing with the consequences of the breach.

Key Components of a Compliant Incident Response Plan

To ensure an effective compliant incident response plan, there are a couple of key components that should be emphasized. First, continuous monitoring of networks and systems to quickly detect anomalies and potential security incidents, along with regular compliance control reviews to ensure alignment with regulations. Once an incident is detected, swift action is required to contain it and prevent further damage, while complying with relevant legal frameworks that may specify steps for containment. Thereafter, the process of restoring systems and data must adhere to compliance requirements, particularly around data integrity and confidentiality. Finally, after an incident is resolved, conducting a post-mortem analysis is essential to identify areas for improvement [15]. This review should also evaluate how well compliance obligations were met during the response process.

Legal Considerations

Legal teams play an essential role in ensuring compliance throughout the incident response process. They help organizations navigate the complex landscape of breach notification laws, document compliance with regulations, and manage communication with affected parties, clients, and regulators. Laws like GDPR require prompt notification of breaches, and legal teams ensure that proper communication channels and timelines are followed. Similarly, documenting and reporting, such as with incident documentation must be thorough, accurate, and comply with legal and contractual requirements. Another consideration regarding incident response is to ensure that a clear communication protocol should be established, and implementing legal teams are involved at the appropriate stages of incident response.

As such, to ensure continuous improvement and adaptation, we must require organizations to regularly update their incident response plans. Tabletop exercises, real-world simulations, and staying informed on new regulations are key practices for ensuring both the incident response team and the plan itself are up to date [16]. Continuous improvement helps organizations remain resilient, agile, and compliant in the face of new challenges. Beyond legal compliance, ethical issues must also be addressed during cyber incident response. These include maintaining the privacy and confidentiality of sensitive information, ensuring transparency with stakeholders, and providing timely and accurate notifications to affected parties [17]. Ethical decision-making during an incident can significantly affect an organization's reputation and the trust it holds with clients and customers.

Technological Tools for Compliance

During the incident response process, there are several technological tools that can be used to support the compliancy process. First,

automated incident response tools that ensure that all steps in the response process are followed systematically and in line with compliance requirements. Similarly, Data Loss Prevention (DLP) solution systems help organizations prevent data breaches and swiftly identify and respond to incidents [18]. Another tool, known as Security Information and Event Management (SIEM) Systems, help provide real-time analysis of security events, aiding in detection and compliance monitoring [19].

Industry Specific Compliance Considerations

Different industries face unique compliance challenges when it comes to cybersecurity and incident response. Each sector handles specific types of sensitive data and operates under distinct regulatory frameworks that impose tailored requirements for managing and responding to cyber incidents. As a result, organizations must adapt their incident response plans to meet the specific legal, operational, and security needs of their respective industries.

The financial services sector is highly regulated due to the sensitivity of the data it handles and the critical role it plays in the global economy. Financial institutions must comply with various regulations that govern data protection, cybersecurity practices, and incident response. One of the key regulations in this regard is the Gramm-Leach-Bliley Act (GLBA), which requires financial institutions to protect consumers' personal financial information [20]. The act mandates that institutions implement a written information security plan, which includes procedures for detecting, responding to, and recovering from security breaches. Under GLBA, financial institutions must notify customers when a breach occurs that compromises the confidentiality of their personal information. The notification process must adhere to strict timelines and reporting requirements. Moreover, the GLBA Safeguards Rule requires institutions to continuously evaluate and update their information security programs, ensuring that incident response procedures evolve alongside emerging threats. Next is the Sarbanes-Oxley Act (SOX). Although SOX primarily focuses on financial reporting, it has important cybersecurity implications, particularly for publicly traded companies. SOX requires that companies implement internal controls to ensure the accuracy of financial reporting, which includes protecting against cyber threats that could impact financial data [21]. Furthermore, SOX mandates that companies disclose material cybersecurity risks and incidents to shareholders. Therefore, financial institutions must have robust incident detection and reporting mechanisms in place to identify and report incidents that could impact their financial integrity or reputation. Failure to do so could result in legal consequences and penalties from the Securities and Exchange Commission (SEC) [22]. For financial institutions that handle payment card data, the Payment Card Industry Data Security Standard (PCI DSS) also plays a critical role in shaping incident response protocols. PCI DSS compliance is essential to protect payment card information, ensure the integrity of payment systems, and prevent fraudulent activity [23]. Financial services organizations that fail to comply with these regulatory frameworks during a cybersecurity incident can face significant fines, sanctions, and reputational damage. The high stakes involved make it essential for financial institutions to maintain comprehensive incident response plans that align with regulatory requirements, support effective communication with stakeholders, and mitigate potential financial and legal liabilities.

The healthcare industry is another highly regulated sector due to the sensitive nature of the data it handles, primarily protected health information (PHI) [24]. Healthcare organizations must comply with stringent regulations that ensure the confidentiality, integrity, and availability of patient data. The key regulation governing incident response in healthcare is the Health Insurance Portability and Accountability Act (HIPAA). HIPAA sets out specific requirements for healthcare organizations regarding the protection of PHI, especially in the event of a cyber incident. The HIPAA Security Rule requires covered entities and their business associates to implement policies and procedures to address cybersecurity incidents and ensure the ongoing protection of patient data [25]. When a breach involving PHI occurs, covered entities must notify the affected individuals, the Department of Health and Human Services (HHS), and, in some cases, the media. The timeline for notification is within 60 days of discovering the breach, but it is encouraged to notify as soon as possible [26]. Healthcare organizations must ensure that their incident response plan includes detailed procedures for identifying breaches, containing them, and ensuring compliance with HIPAA's reporting requirements. The HIPAA Breach Notification Rule further outlines how covered entities and business associates must respond to security breaches involving PHI. Risk assessments must be conducted to determine whether PHI was compromised and whether notification is required. This rule ensures that all potential threats are addressed promptly and that patients and regulators are informed of breaches affecting PHI. Healthcare organizations that fail to comply with HIPAA during a breach response face substantial civil and criminal penalties. These penalties range from $100 to $50,000 per violation, with a maximum annual penalty of $1.5 million [27]. In addition to financial penalties, non-compliance can severely damage the organization's reputation and result in loss of patient trust. Given the sensitivity of healthcare data and the high penalties for non-compliance, healthcare organizations must ensure their incident response plans are thorough, regularly tested, and aligned with HIPAA's requirements. Training staff to understand and comply with these regulations is also critical to ensure effective incident management.

The retail sector, in contrast, faces unique cybersecurity challenges due to its reliance on electronic payment systems and the large volumes of personal and financial data it processes. One of the most important regulatory frameworks for retailers is the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS requires retailers to have an incident response plan that includes specific procedures for responding to data breaches involving payment card information. This plan must address how the breach will be contained, how stakeholders (such as card issuers and acquiring banks) will be notified, and how forensic investigations will be conducted to determine the cause of the breach. After a breach, organizations may be required to undergo a forensic investigation conducted by a Qualified Security Assessor (QSA) or an Approved Scanning Vendor (ASV) to assess how the breach occurred and whether PCI DSS compliance failures contributed to the breach [28]. The results of the investigation must be reported to the relevant stakeholders, and any compliance failures must be remediated. Retailers that fail to comply with PCI DSS face significant penalties from card issuers and acquiring banks, including fines of $5,000 to $100,000 per month until compliance is restored. In addition to fines, non-compliant retailers may face increased transaction fees, lawsuits, and loss of the ability to process credit card payments, which can have a devastating impact on their business [29].

Other industries, such as Manufacturing and Industrial Sectors, face compliance requirements related to operational technology (OT) and industrial control systems (ICS). Cybersecurity

incidents involving critical infrastructure, such as energy grids or water supply systems, may be subject to NERC-CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) standards or sector-specific regulations that mandate timely incident reporting and response. In the U.S., contractors working with the Department of Defense (DoD) must comply with the Cybersecurity Maturity Model Certification (CMMC). This framework requires defense contractors to meet specific levels of cybersecurity maturity, including robust incident response protocols to protect controlled unclassified information (CUI) [30].

Conclusion

Compliance considerations in cyber incident response are multi-dimensional, requiring organizations to navigate a complex web of regulatory, ethical, and technological challenges. With the ever-evolving nature of cyber threats and the increasing complexity of regulatory frameworks, maintaining compliance has become not just a legal obligation but also a strategic imperative for organizations. Ensuring that compliance is integrated into every aspect of the incident response process—from risk assessment to post-incident analysis—enables organizations to manage security breaches effectively while fulfilling their legal, regulatory, and ethical duties.

The dynamic nature of both cyber threats and compliance requirements means that organizations must adopt a proactive and adaptive approach to incident response. This includes staying up to date with evolving regulations such as GDPR, HIPAA, and PCI DSS, and continuously refining their response strategies to meet emerging risks. Organizations that embed compliance into their incident response framework are better equipped to handle the increasing scrutiny from regulators, clients, and other stakeholders. Additionally, they can avoid significant financial penalties and legal consequences that often accompany non-compliance in the wake of a data breach.

In today's complex digital landscape, where data breaches can cause far-reaching consequences beyond immediate financial loss, the ability to navigate compliance requirements and respond swiftly to incidents is crucial for long-term success. By integrating both compliance and effectiveness into incident response, organizations are not only protecting themselves from legal repercussions but also solidifying their position as responsible stewards of data, fostering greater resilience, and paving the way for continued growth and trust in the digital economy.

References

1. Pureti N (2021) Incident Response Planning: Preparing for the Worst in Cybersecurity. Revista de Inteligencia Artificial en Medicina 12: 32-50.
2. Torres A (2014) Incident response: How to fight back. SANS Institute InfoSec Reading Room https://csbweb01.uncw.edu/people/cummingsj/classes/mis534/articles/ch3_ir_sanssurvey.pdf.
3. Voigt P, Von dem Bussche A (2017) The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing 10.
4. Krystlik J (2017) With GDPR, preparation is everything. Computer Fraud & Security 2017: 5-8.
5. Wolff J, Atallah N (2021) Early GDPR penalties: Analysis of implementation and fines through May 2020. Journal of Information Policy 11: 63-103.
6. Moore W, Frye S (2019) Review of HIPAA, part 1: history, protected health information, and privacy and security rules. Journal of nuclear medicine technology 47: 269-272.
7. Redhead CS (2015) HIPAA privacy, security, enforcement and breach notification standards https://sgp.fas.org/crs/misc/R43991.pdf.
8. Stevens GM (2008) Enforcement of the HIPAA privacy and security rules. Library of Congress, Congressional Research Service https://digital.library.unt.edu/ark:/67531/metadc463388/.
9. Morse EA, Raval V (2008) PCI DSS: Payment card industry data security standards in context. Computer Law & Security Review 24: 540-554.
10. Rees J (2012) Tackling the PCI DSS challenges. Computer Fraud & Security 2012: 15-17.
11. Shaw A (2009) Data breach: from notification to prevention using PCI DSS. Colum. JL & Soc Probs 43: 517.
12. Burnett S (2021) Cybersecurity Maturity Model Certification (CMMC) Compliance for DoD Contractors. Old Dominion University https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1045&context=covacci-undergraduateresearch.
13. Markopoulou D, Papakonstantinou V, De Hert P (2019) The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review 35: 105336.
14. Goldman E (2020). An introduction to the california consumer privacy act (ccpa). Santa Clara Univ. Legal Studies Research Paper https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013.
15. Mitropoulos S, Patsos D, Douligeris C (2006) On Incident Handling and Response: A state-of-the-art approach. Computers & Security 25: 351-370.
16. Angafor GN, Yevseyeva I, He Y (2020) Game-based learning: A review of tabletop exercises for cybersecurity incident response training. Security and privacy 3: e126.
17. Lin HS, Dam KW, Owens WA (2009) Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities. National Academies Press https://nap.nationalacademies.org/catalog/12651/technology-policy-law-and-ethics-regarding-us-acquisition-and-use-of-cyberattack-capabilities.
18. Takebayashi T, Tsuda H, Hasebe T, Masuoka R (2010) Data loss prevention technologies. Fujitsu Scientific and Technical Journal 46: 47-55.
19. Vielberth M (2021) Security information and event management (SIEM). In Encyclopedia of Cryptography, Security and Privacy (pp. 1-3). Berlin, Heidelberg: Springer Berlin Heidelberg https://www.researchgate.net/publication/349807309_Security_Information_and_Event_Management_SIEM.
20. Cuaresma JC (2002) The gramm-leach-bliley act. Berkeley Tech LJ, 17, 497.
21. Act SO (2002). Sarbanes-oxley act. Washington DC https://sarbanes-oxley-act.com/.
22. Rosenfeld D (2019) Civil penalties against public companies in SEC enforcement actions: An empirical analysis. U Pa J Bus L 22: 135.
23. Ataya G (2010) PCI DSS audit and compliance. Information security technical report 15: 138-144.
24. Moore W, Frye S (2019) Review of HIPAA, part 1: history, protected health information, and privacy and security rules. Journal of nuclear medicine technology 47: 269-272.
25. Edemekong PF, Annamaraju P, Haydel MJ (2018) Health insurance portability and accountability act.
26. Redhead CS (2015) HIPAA privacy, security, enforcement and breach notification standards https://crsreports.congress.

gov/product/pdf/R/R43991.

27. Gonzalez E (2014) Complying with HIPAA: Avoid financial penalties by following these steps. Long-Term Living 63: 16-19.
28. Rahaman S, Wang G, Yao D (2019) Security certification in payment card industry: Testbeds, measurements, and recommendations. Proceedings of the 2019 ACM SIGSAC conference on computer and communications security 481-498.
29. Mahmud SY, Acharya A, Andow B, Enck W, Reaves B (2020) Cardpliance:{PCI}{DSS} Compliance of Android Applications. In 29th USENIX Security Symposium (USENIX Security 20) 1517-1533.
30. Ross R, Viscuso P, Guissanie G, Dempsey K, Riddle M (2015) Protecting controlled unclassified information in nonfederal information systems and organizations. US Department of Commerce, National Institute of Standards and Technology https://www.nist.gov/publications/protecting-controlled-unclassified-information-nonfederal-systems-and-organizations.