social Informatics Journal
Business, Politics, Law, Environmental Sciences & Technology

Vol 8, No 4, 2022 Series

An In-depth Review of Cybersecurity Controls in Mitigating Legal and Risk-Related Challenges

Bayewu A[1], Patcharaporn Y[2], Folorunsho O.S[3], & Ojo T.P[4]
[1]Northumbria University, New Castle, NE1 8ST, UK
2Washington University of Science and Technology, Vienna, VA, 22182, USA
[3] Washington University of Science and Technology, Vienna, VA, 22182, USA
[4]University of Indianapolis, IN, 46227, USA
E-mails: [1]hadeola_oyeyipo@yahoo.com; [2]ami.yamcharoen@wust.edu; [3]olusolafatoye@gmail.com; [4]titilikesyou@gmail.com

ABSTRACT

Organizations are facing an increasingly wide variety of cyber threats, posing significant legal and risk related challenges within a connected Digital World. The purpose of this Review is to analyze, in detail, the effectiveness of cyber security controls and their role as mitigation tools for these challenges. This paper offers insight into best practices for organizations with a view to protecting sensitive information and ensuring compliance, through an examination of the link between cybersecurity, legal frameworks and risk factors. The review begins by looking at the current state of cybersecurity, which is characterized by complex legal and risk factors faced by organizations. It focuses on the regulatory framework, industrial standards and legal obligations in place for cyber security practices to be understood and taken into account by organizations. In addition, the paper reviews various cybersecurity control measures that organizations can put in place to deal with legal and risk factors. The Authority shall examine the technical controls, which are designed to ensure that unauthorized access and data leakages are not allowed, e.g., access controls, encryption and network monitoring systems. In addition, consideration is given to administrative controls to create a strong security culture within organizations, including safety policies, risk assessments and employee training programs.In summary, the review paper assesses the effectiveness of new technologies for strengthening cyber security controls. To identify and mitigate cyber threats, it examines the potential of machine learning, artificial intelligence, and behavioral analysis. These technologies have an important role to play in the proactive defense mechanisms, making it possible for organizations to respond swiftly to emerging risks.

Keywords: Cybersecurity Controls, Legal Compliance, Risk Mitigation, Information Security, Regulatory Frameworks, Threat Assessment, Incident Response, Risk Factors, Data Protection, Security Awareness.

Journal Reference Format:
Bayewu A., Patcharaporn Y., Folorunsho, O.S. & Ojo T.P. (2022): An In-depth Review of Cybersecurity Controls in Mitigating Legal and Risk-Related Challenges. Social Informatics, Business, Politics, L:aw, Environmental Sciences & Technology Journal. Vol. 8, No.4. Pp 1-10. www.isteams/socialinformaticsjournal. Article DOI No - dx.doi.org/10.22624/AIMS/SIJ/V8N4P1.

1. INTRODUCTION

Cybersecurity controls, which address legal and risk factors linked with data breaches and unauthorized access, play an important role in protecting organizations from cyber threats. The necessity of strong cybersecurity measures is becoming increasingly important as more and more people are relying on digital systems and networks. The background and significance of cyber security checks are described in this section, which highlights the importance of their implementation. The healthcare sector has been the target of threat actors, and many hospitals in this industry have lost revenues to cyber-attacks. The federal government has enforced Health Portability and Accountability Act (HIPAA) as the industry standard to ensure that organization can protect their infrastructure and the patient's protected health information. In healthcare, it was recorded that external threats are more significant than internal threats based on the information gathered from the incident history. This paper will prioritize the internal and external threats, and methods to reduce organizational cyber risk will be recommended.

The list of controls that will reduce risk and support compliance will be discussed. Today's ever changing threat landscape poses major challenges for organizations around the world. Cyber criminals are constantly developing new ways of exploiting vulnerabilities and gaining unauthorized access to sensitive information, (Smith et al., 2020) Cyber-attacks may result in severe financial and reputational damage, as well as legal consequences (Herath & Rao, 2019). To ensure the protection of IT assets and mitigate possible risks, organizations need to prioritize their cyber security controls. The legal landscape surrounding cybersecurity is multifaceted, with numerous regulatory frameworks and compliance requirements. In the healthcare sector organizations are required to comply with specific industry standards and regulations such as General Data Protection Regulation GDPR in the European Union or Health Insurance Portability and Accountability Act (HIPAA). There can be significant penalties and regulatory consequences for breaches of these regulations, as outlined by (Fuchs et al., 2020). Moreover, organizations are exposed to several risk factors such as insider threats, third party vulnerabilities and new technologies that create new security challenges (Erlin, 2021).

To protect its digital assets, maintain the trust of stakeholders and to guarantee business continuity it is important for organizations to implement effective cybersecurity controls. By employing a combination of technical and administrative controls, organizations can mitigate the risks associated with cyber threats and maintain compliance with legal obligations (Kshetri, 2020). Furthermore, cybersecurity controls help establish a proactive defense posture, enabling organizations to detect and respond to incidents in a timely manner (Wang et al., 2021). This review report shall provide an in-depth analysis of the effectiveness of cyber security controls and their contribution to dealing with legal and regulatory risk factors. Organizations have considerable challenges to protect their Digital Assets and ensure that they comply, considering a growing incidence of cyber threats and an evolving regulatory environment. The paper aims at informing organizations wishing to enhance their cybersecurity posture on the importance of cyber security controls, examine their effectiveness and provide useful information for them.

2. LITERATURE REVIEW

Cyber threats are serious problems for organizations operating in a digital environment, which affect their operations, reputation and profitability. An overview of the different organizations dealing with cyber threats and their potential impact is given in this section (Kure, H. I. et al, 2018). A wide range of malicious activities targeting organizations' digital assets are covered by cyber threats. The types of cyber threats that most frequently occur are malware, phishing attacks, ransomware, distributed denial of service: (DDoS) attack, insider and threat (Kshetri, N., 2020). The threats take advantage of weaknesses in the systems, networks and people's behavior to seek unauthorized access, steal personal data, disrupt operations or cause loss of revenue. Cyber security threats can have a very serious and widespread impact on organizations. Financial losses are an immediate consequence of a cyber-attack as they can lead to tangible costs, like ransom payments, incident response efforts and system repairs. Moreover, organizations may suffer reputational damage, leading to a loss of customer trust and loyalty (Cavelty, 2020).

Another significant impact of cyber threats is the disruption of operations. DDoS attacks can overload computer systems and render them inaccessible, as well as disrupt business operations. (Cherdantseva et al., 2016). In addition, the cyber-attacks can destroy critical data that would result in an operational interruption until payment or recovery of ransoms (Herath & Rao 2019). Moreover, the potential theft of sensitive information may lead to serious consequences that include identity thefts, fraud and infringements on trade secrets. This can result in financial harm to individuals and organizations alike (Cavelty, 2020).

2.1Legal and Risk Factors Associated with Cybersecurity

As organizations are forced to navigate the ever-changing landscape of legislation, regulations and possible threats, cyber security is intertwined with legislative and risk factors. An overview of the regulatory and risk factors associated with cybersecurity is included in this section to highlight the challenges that organizations are facing when it comes to keeping up with security practices and avoiding possible risks.

2.1.1 Legal Factors

Organizations are covered by a legal framework that imposes various responsibilities and obligations on them in relation to cyber security. Data protection and privacy laws, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, govern the collection, storage, and processing of personal data (Hildebrandt & Galetta, 2019). Failure to comply with these laws may entail significant legal and financial consequences, including regulatory penalties, judicial actions or reputational damage.

In addition, the role of industry specific regulations in defining cyber security requirements is also played. For instance, healthcare organizations must adhere to the Health Insurance Portability and Accountability Act (HIPAA), which safeguards patient information (Custers, 2019). Financial institutions must comply with regulations such as the Payment Card Industry Data Security Standard (PCI DSS) to protect customer financial data (Borodin & Bailey, 2019). Non-compliance with these regulations can lead to penalties and loss of trust among stakeholders.

2.1.2 Risks Factors

There are various risk factors to be faced by organizations that influence their cybersecurity posture. There is a significant risk of insider threats arising from employees or trusted individuals with authorized access (D'Arcy et al., 2019). Malicious insiders can intentionally misuse data or systems, while unintentional errors or negligence by well-meaning employees can inadvertently lead to security breaches (Safa et al., 2020).

The cybersecurity landscape is also contributed by the risks posed by external parties. Businesses have often depended on vendors, suppliers and service providers who may be given access to confidential information. Failure to properly vet and manage these third-party relationships can introduce vulnerabilities and increase the risk of data breaches (Kshetri, 2020).

As organizations embrace innovations like cloud computing, the Internet of Things, or IoT and AI, emerging technologies represent a further risk factor. These technologies introduce new attack surfaces and potential vulnerabilities that cybercriminals can exploit (Wang et al., 2021). In the assessment and mitigation of risks related to such technologies, organizations need to remain alert.

2.2Regulatory Frameworks and Compliance Requirements

In shaping their cybersecurity practice and ensuring compliance of organizations with legal obligations, regulatory frameworks and requirements play an important role. An overview of the regulatory environment and requirements related to cyber security are set out in this section, which stresses the difficulties faced by organizations with respect to meeting these obligations.

2.2.1 Regulatory Frameworks

Various frameworks for managing cyber security practices have been put in place by governments and regulators all over the world. One prominent example is the General Data Protection Regulation (GDPR) implemented by the European Union. The General Data Protection Regulation lays down strict requirements for organizations that process personal data, including the implementation of appropriate technical and organizational measures to protect personal data (Fuchs, C., et al., 2020). Non-compliance with the GDPR can result in significant financial penalties and reputational damage.

In the United States, regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) impose cybersecurity and privacy requirements on healthcare and financial institutions, respectively (Hoffman, 2020). The purpose of these Regulations is to ensure that sensitive information and personal data are protected.

2.2.2 Compliance Requirements

Adequate compliance with the legal frameworks requires fulfilling specific cybersecurity requirements and demonstrating respect for best practices. Organizations shall carry out comprehensive safety controls, conduct risk assessments, develop incident response plans and regularly train their staff on security awareness (NIST 2020), Regular security audits and inspections, which are intended to guarantee continuous fulfilment of the requirements, may also be involved in compliance.

Compliance requirements are also contributed by industry specific standards and frameworks. For example, the Payment Card Industry Data Security Standard (PCI DSS) applies to organizations that handle credit card information and mandates specific security controls to protect cardholder data (PCI Security Standards Council, 2020). Compliance with these industry standards is essential to ensure that organizations operating in the regulated sectors fulfil their obligations.

2.2.3 Challenges and Implications

The challenge for organizations is to comply with the regulatory framework and meet its compliance requirements. Compliance has become a continuous and hard process due to the complexity of legal frameworks, variations in regional regulations as well as evolving security landscape (Fuchs et al. 2020). It is vital that organizations allocate resources in order to be able to keep up with regulatory changes, invest in cyber security technologies and personnel as well as make regular evaluations of their compliance.

Failure to fulfil regulatory requirements can result in severe consequences. In addition to financial penalties and judicial consequences, organizations are at risk of damage to their reputations, loss of trust in clients or decreased market competitiveness (Custers, 2019). In the case where organizations have to inform affected persons and regulatory authorities about security incidents, failure to comply with compliance requirements can also result in a breach of notification obligations.

3. REVIEW PROCESS

3.1 Reducing Cyber Risk from Internal and External Threats

The security team must prioritize the five insider threats: careless workers, insider agents, feckless third parties, disgruntled employees, and malicious insiders. Employees bypassing security and privacy measures will violate the PHI and pose legal implications for the organization. When employees break acceptable use policies, leave sensitive PHI in plain sight of onlookers, or install unapproved applications onto company devices, they leave their network vulnerable to infiltration. Through negligence, the employee might be violating HIPAA security and privacy rule if the security team does not have a monitoring system that tracks the employee's activities (Perakslis, 2014). The security team will reinforce guidelines from the point of hire to prevent the employee from compromising the patient data and exposing the organization to risk. New hires must comply with the cybersecurity guideline and sign the non-disclosure agreement (Coronado & Wong, 2014).

The insider agent can be by a third-party contractor, the employee either full-time or part-time. From third-party contractors to permanent staff, the Inside Agent could be anyone. The security team needs to devise a means to track the activities of all entities accessing the organization's resources by implementing a security monitoring system at the security operation center to monitor inflow and outflow traffic. The security team will enforce the HIPAA security rule to restrict file access to only authorized users or implement user activity monitoring to send alerts when suspicious activity is detected. This will help the security team to reduce the risk from Inside Agents (Mohammed, 2017).
The security team must investigate contractors, vendors, and third parties that will provide services and supply IT equipment to the organization. The third party will compromise security through harmful access, negligence, and improper use of resources.

The security team will investigate the hardware and solutions before purchase. It is important to buy equipment and solutions from industry-approved and verified vendors to protect the organization's network and prevent the potential risk of cyber-attacks. The security team will implement a network monitoring system to monitor the activities of the third-party, contractors, and vendors. Managers and supervisors should always look for signs that an employee is about to quit. Before they retire or transition to another job, the security team will restrict employee access to protect patient-protected health information. The security team will initiate a role level access control to monitor the activity of the employee in real-time, and they will be restricted from downloading the unauthorized application on their computer or downloading non-business-related organization files on their computer to prevent them from leaving a back door that can be exploited to compromise data. The disgruntled employee can turn into an insider agent, and they may potentially leak protected health information.

Internal malicious insiders are one of the most dangerous threats to detect. Unlike the Inside actors, they usually act on their incentives rather than those of an external party. They can leverage their ownership to access private information for financial or personal gain. Moreover, because they are already inside the network, they have no roadblocks preventing them from abusing secure data. The employee would leak a patient's personally identifiable information for profit, making it easy for patients to be vulnerable to financial fraud (Li et al., 2021).As challenging as it can be to detect the employee acting as a malicious insider, the security team can adopt countermeasures to protect patient data. The security team with the information technology team will regulate and control access to patient and organization-sensitive data.

The five external cybersecurity threats that must be prioritized are ransomware threats, cloud vulnerabilities and misconfigurations, web application attacks, bad-bot traffic, and increased phishing volumes (Lee, 2021).The ransomware attack has been one of the major cyber threats to the healthcare sector since the global pandemic. Cyber attackers have uncovered that healthcare organizations' lifesaving, delivering vital treatments were extorted using ransomware to attack their victims in infrastructure. The adoption and expansion of modern digital technology to create a seamless environment for doctor-patient interaction have created a lot of gaps that the threat actors leverage to lunch their attacks. The security team at hospitals must ensure that risk assessment and networking testing are conducted timely to prevent the likelihood of an attack (Humayun et al., 2021).

In healthcare, patients' data have been compromised due to vulnerabilities in the misconfigurations of cloud services. The geometric growth in adopting cloud services in healthcare has transformed the business operation due to the increased demand for remote telehealth services. Healthcare should use multi-vendor cloud services to host most of their databases, and the security team must collaborate with the cloud service provider to ensure the misconfiguration that can lead to the vulnerability of the solution is eradicated (Gunes et al., 2021). Healthcare lacked the required technology to manage their web application, and the threat actors are exploiting the weakness to attack healthcare infrastructure. The security team must implement controls that enable better visibility into third-party applications and API connections to protect their infrastructure and cybersecurity space. With the appropriate control in place, the security team will have visibility and detect who is accessing the organization's resources at a point in time (Genge et al., 2015).

Bot traffic is a challenge for healthcare because it is difficult to traffic malicious traffic in real-time due to the increase in traffic. Patients accessing the healthcare website activities were interrupted because of the level of traffic flow to the organization's network. At some point, the volume of traffic flow caused a downtime that prevented the patient from accessing their portal or contacting their provider. The threat actors leverage the high-volume traffic to scrap web content, track account creation, take over an account, and perpetrate different types of fraud. The threat actors use credential stuffing and password cracking to hack into patient web portals. The security team must ensure that networks are segmented to track traffic flow from one point to another on the organizational network. The network segmentation will help reduce risk and track malicious activities in real-time (Cybersecurity, 2018). The security team must enforce cybersecurity awareness across the organization to familiarize the employees and contractors with different phishing patterns adopted by the threat actors to target the healthcare infrastructure.

3.2 Cyber Risk Reduction Using Critical Security Controls

The security team will develop a critical security control to protect the organization's infrastructure and secure protected health information. Table 1 below summarizes the critical security control needed to protect the healthcare’s evolving cybersecurity landscape.

Table 1: Summary Of Critical Security Control Needed To Protect The Healthcare’s Evolving Cybersecurity Landscape

Control Name	Why the control is critical
Inventory and control of enterprise assets	Will prevent external attackers are constantly monitoring healthcare cyber space from targeting healthcare enterprise solutions like the on-premises and cloud-based databases.
Inventory and control of software assets	The security team will review the organization's software inventory to identify any enterprise assets running software that is not required for business purposes. Any default software that comes with an enterprise solution must be uninstalled because of potential security risks, providing no benefit to the enterprise.
Data protection	Hospital might lose enterprise control over sensitive or protected patients, which might impact the organization's business operation. The security team must implement a robust data management solution to prevent the loss of data because of espionage or theft. It is required and HIPAA standards that patient data must be encrypted when shared internally or with external covered entities.

Control Name	Why the control is critical
Secure configuration of enterprise assets and software.	The security team must implement a strong configuration at the initial state, and the configuration must be maintained to prevent the degrading of the software security as new patches and versions are available. If there is a change in the operational requirements, the software configuration can be tweaked to support the new requirements.
Access control management	The security team must implement multi-factor authentication across the organization for administrators and others. MFA should be universal for all privileged or administrator accounts. The MFA will be linked to the user's phone number or email address to protect hospital infrastructure and user credentials from getting into the hands of unauthorized users.
Continuous vulnerability management	The security team must have timely information about the threats within the industry and the pattern of attacks adopted by the threat actors. It is important to devise a means to track the latest patches, software updates, security advisories, and threat patterns within the cyberspace industry. The security team must identify the vulnerabilities within the healthcare system before the threat actors do. The vulnerability monitoring should be automated to ensure the organization's infrastructure is fully secured.
Audit Log Management	The security team will log records of incidents immediately after an attack is detected, and it is essential to have a database where incident records will be stored for analysis. The security team will analyze the logs to understand the attack's impact. The security can determine the resource that has been assessed if the retention logs are correctly stored and timely.
Malware defenses	The security team must implement malware defenses suitable for the changing in the cybersecurity landscape of the organization via rapid update and timely integration that will work with incident response and network vulnerability management. The security team will deploy the defense system at every entry point on the network to detect malicious activities and malicious code lunch by threat actors.

4. CONCLUSION

The security team at hospitals should prioritize the five insider threats: careless workers, insider agents, feckless third parties, disgruntled employees, and malicious insiders. Employees bypassing security and privacy measures will violate the PHI and pose legal implications for the organization. Through negligence, the employee might be violating HIPAA security and privacy rule if the security team does not have a monitoring system that tracks the employee's activities. The five external cybersecurity threats that must be prioritized are ransomware threats, cloud vulnerabilities and misconfigurations, web application attacks, bad-bot traffic, and increased phishing volumes. Patient data have been compromised due to vulnerabilities in the misconfigurations of cloud services. Hospital lacked the required technology to manage its web application, and the threat actors are exploiting the weakness to attack hospitals' infrastructure. The security team must implement controls that enable better visibility into third-party applications and API connections to protect their infrastructure and cybersecurity space. The security team should develop a critical security control to protect the organization's infrastructure and secure protected health information. Table 1 summarizes the critical security control needed to protect the healthcare evolving cybersecurity landscape.

REFERENCE

1. Borodin, A., & Bailey, M. (2019). Addressing the Cybersecurity Challenges of the Financial Sector. IEEE Security & Privacy, 17(3), 69-75.
2. Cavelty, M. D. (2020). Cybersecurity Threats and Their Implications for Public Security. Journal of Strategic Security, 13(1), 45-62.
3. Cherdantseva, Y., et al. (2016). Analysis of the Impact of DDoS Attacks on Business Performance. Computers & Security, 56, 110-125.
4. Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. Biomedical instrumentation & technology, 48(s1), 26-30.
5. Custers, B. (2019). Data Protection and the Internet of Things: The Application of the EU General Data Protection Regulation to the IoT. Computer Law & Security Review, 35(2), 105-123.
6. Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP, 4162018.
7. D'Arcy, J., et al. (2019). Examining Insider Threat Detection and Risk Mitigation in Cybersecurity: A Review and Directions for Future Research. Journal of Organizational Computing and Electronic Commerce, 29(3), 185-208.
8. Fuchs, C., et al. (2020). Cybersecurity Regulations: Europe as a Cautionary Tale. Journal of Cybersecurity, 6(1), 1-8.
9. Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures. International Journal of Critical Infrastructure Protection, 10, 3-17.
10. Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cybersecurity risk assessment for seaports: A case study of a container port. Computers & Security, 103, 102196.
11. Herath, T., & Rao, H. R. (2019). Cybersecurity Breach Disclosure: The Role of IT Governance, Board Composition, and Firm Characteristics. Journal of Information Technology, 34(1), 48-62.

12. Hildebrandt, M., & Galetta, A. (2019). European Data Protection Law: The General Data Protection Regulation. Oxford University Press.
13. Hoffman, A. J. (2020). Security Breach and the Erosion of U.S. Public Trust in the Internet. Journal of Cybersecurity, 6(1), 1-9.
14. Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. Egyptian Informatics Journal, 22(1), 105-117.
15. Kshetri, N. (2020). The Institutional Complexity of Regulatory Compliance in Cybersecurity. Regulation & Governance, 14(1), 89-110.
16. Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences, 8(6), 898.
17. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659-671.
18. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security.
19. Emerging trends and recent developments. Energy Reports, 7, 8176-8186.
20. Mohammed, D. (2017). US healthcare industry: Cybersecurity regulatory and compliance
21. issues. Journal of Research in Business, Economics and Management, 9(5), 1771-1776.
22. Perakslis, E. D. (2014). Cybersecurity in health care. N Engl J Med, 371(5), 395-397.
23. Smith, A. D., et al. (2020). Current and Emerging Threats in Cybersecurity: A Research Framework. Computers & Security, 91, 101738.
24. Wang, Q., et al. (2021). Cyber Threat Intelligence and Analytics: A Review. Journal of IInformation Privacy and Security, 17(1), 1-19.