Advancing Healthcare Security: Developing a Composite Set of Cybersecurity Requirements for the Healthcare Industry

Yamcharoen P[1], Folorunsho O.S[2], Bayewu A[3] & Fatoye O.E[4]
[1] Washington University of Science and Technology, Vienna, VA, 22182, USA
[2] Washington University of Science and Technology, Vienna, VA, 22182, USA
3Northumbria University, New Castle, NE1 8ST, UK
[4]Lead City University Ibadan, Oyo State, Nigeria
E-mails: [1]ami.yamcharoen@wust.edu; [2]olusolafatoye@gmail.com; [3]omowunmisesekinatf@yahoo.com
[4]olusolafatoy@gmail.com

ABSTRACT

The need for a strong security measure to ensure that patients' data and health environments are protected has been highlighted by rapid digitization of healthcare systems, as well as an increased reliance on connected technologies. This review focuses on developing a common set of cybersecurity requirements designed specifically for health organizations, which is aimed at addressing the specific cyber challenges facing the healthcare sector. The review shall start by analyzing current cybersecurity requirements in the fields of health, which will include appropriate standards, frameworks, regulations and guidelines. The paper highlights the need to consolidate and create a coherent framework with an analysis of the present situation, as well as identifying gaps and weaknesses in approaches currently being pursued. Emphasis is placed on the integration and harmonization of existing requirements while addressing healthcare specific concerns, in order to establish a common set of cybersecurity requirements. The aim of such a approach would be to bridge the gaps in different standard and guidelines, ensuring that healthcare organizations are provided with a coherent and useful framework for improving their cybersecurity posture. The methodology and approach for the development of a common set of security requirements have been outlined in this report, highlighting the importance of stakeholder engagement within the healthcare sector. In order to highlight the need to adapt and scale up cybersecurity measures, key elements and the structure of the proposed framework are presented. Finally, the review presents challenges and future directions including adapting rapidly to healthcare technology developments, balancing security and functionality in clinical settings as well as promoting cooperation and sharing of knowledge within the health sector.

Keywords: Healthcare security, Cybersecurity requirements, Composite framework, Patient data protection, Healthcare industry, Digitization, Interconnected technologies

CISDI JournalReferenceFormat
Yamcharoen P., Folorunsho O.S., Bayewu, A. & Fatoye O.E. (2023): Advancing Healthcare Security: Developing a Composite Set of Cybersecurity Requirements for the Healthcare Industry. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 14 No 1, Pp 9-.20. DOI: dx.doi.org/10.22624/AIMS/CISDI/V14N1P2. Availableonlineathttps://www.isteams.net/cisdijournal

1. INTRODUCTION

Due to technological progress and growing demand for efficient, accessible health care services, the healthcare sector has been undergoing an important transformation of its Digitalization over these past years. In order to improve patient care, streamline processes and achieve better outcomes, the integration of Digital solutions has created a revolution in healthcare delivery.

Digital transformation includes a wide range of aspects, e.g., EHRs, telehealth, remote monitoring, mobile health applications and data analysis (World Health Organization, 2021), Widespread use of electronic health records is an important driver for this transformation. Electronic health records, or eEHRs, provide healthcare professionals with the capacity to retain, access and transmit patient information in an electronic form instead of a paper record. In addition to improving the efficiency of patient care, reducing medical mistakes, and coordinating healthcare between different providers, use of EHRs has been shown to improve coordination in health care (Office of the National Coordinator for Health Information Technology. n.d.).

In the past years, particularly with a worldwide COVID 19 pandemic, telemedicine has been gaining considerable attention as another key component of Digital Transformation. Telehealth refers to the use of telecommunications technology so that health services can be delivered remotely, making it easier for patients to receive care at home. In addition to improving access to care and the patient's convenience, it also allowed healthcare providers to offer virtual consultations, remote monitoring and telemedicine services (American Telemedicine Association. n.d.). In the digital transformation of healthcare, the proliferation of mobile health applications has also played an important role. These applications are a means of providing patients with the opportunity to monitor their health condition, manage symptoms and access appropriate medical information. Individuals are empowered to take an active role in the management of their health, to promote patient involvement and to take care of themselves, thanks to mobile health applications (Ventola, C. L., 2014).

Data Analytics and Big Data have become an important tool for healthcare, which enables the extraction of useful information from a large volume of health data. The process of discovering patterns, trends and predicted models for the purpose of influencing clinical decision making, disease surveillance, population health management is facilitated by advances in analytic techniques (Topol, E. J., 2019). There is great potential to improve outcomes for patients and healthcare delivery through a digital transformation of health care. But, in particular as regards cyber safety and data protection, it also introduces new challenges. Cyber threats and data breaches are primary targets of healthcare organizations due to the growing connectivity of health systems and a large amount of sensitive patient information being generated. Therefore, to safeguard patient data, healthcare environments and trust in the digital health ecosystem it is necessary to implement strong cybersecurity measures with an integrated set of cyber security requirements which are specific for the medical sector.

1.1Problem Statement

There are many benefits and advances in the digital transformation of health care. However, it also exposed the healthcare sector to a number of serious cybersecurity problems. Health care organizations are especially vulnerable to cyber-attacks and breaches because of the sensitivity of patients' data and connected nature of healthcare systems. The following problem statement highlights the key cybersecurity challenges faced by the healthcare industry: Increasing cyber threats: Ransomware, phishing attempts and data theft are all becoming increasingly common in the healthcare sector. These risks are likely to lead to unlawful access, theft or manipulation of patients' personal data which may jeopardize their health and affect the reputations of healthcare organizations. Complexity of healthcare systems: healthcare systems are complex, involving a number of interconnected devices, networks and applications. Such complexity makes it possible for hackers to exploit these vulnerabilities. In addition, compatibility concerns and security gaps that increase the risk of cyber-attacks are commonly caused by legacy systems and their integration with new technologies. Lack of cybersecurity awareness and training: Information on cyber security is frequently lacking from healthcare professionals, administrators or members of staff. Human errors such as falling victim to phishing attacks or accidentally giving out sensitive information could be caused by this knowledge gap, compromising the security of healthcare systems.

Inadequate Cybersecurity Measures: Many healthcare organizations struggle to implement robust cybersecurity measures due to budget constraints, limited resources, and competing priorities. This could result in vulnerabilities not being addressed, which will lead to weaknesses being exploited by cybercriminals and endangering the security of healthcare systems. Regulatory Compliance Challenges: For instance, the Health Insurance Portability and Accountability Act in the United States requires healthcare organizations to comply with different laws and standards relating to data protection and privacy. In order to comply with these requirements, healthcare organizations are facing a significant challenge in the management of cybersecurity risks. The protection of patient data, maintaining the trust of individuals seeking health care services and ensuring continuity of healthcare operations are essential to address these cybersecurity challenges. By setting up a general framework which guides healthcare organizations in the implementation of effective cybersecurity measures and risks mitigation, it is possible to help mitigate these challenges by developing a broad set of cyber security requirements specially designed for this sector.

1.3Objectives of the review

The objective of the study is as follows:

1. To identify and analyze the existing cybersecurity requirements, standards, frameworks, regulations, and guidelines applicable to the healthcare industry.
2. To evaluate the gaps, limitations, and incoherence between current approaches to cyber security in healthcare.
3. To propose the development of a composite set of cybersecurity requirements specifically tailored for healthcare organizations.
4. To highlight the benefits and advantages of a joint approach to cybersecurity in healthcare, e.g., enhanced data protection for patients, better compliance with regulations as well as effective allocation of resources.
5. To outline the methodology and approach for developing the composite set of cybersecurity requirements, considering stakeholder engagement and industry collaboration.

2. LITERATURE REVIEW

The medical sector has a huge volume of sensitive patient data, which makes it an important target for cyber threats. Various cybersecurity requirements, standards, frameworks, regulations and guidelines have been established with the aim of mitigating these risks. An overview of the current healthcare cyber security requirements will be provided in this section, showing the critical sources that organizations need to take into account. One of the primary regulations governing healthcare data security is the Health Insurance Portability and Accountability Act (HIPAA) in the United States. HIPAA includes a Security Rule setting out the administrative, physical and technical safeguards to protect electronic protected health information (ePHI) (U.S. Department of Health & Human Services, 2018).

Additionally, the National Institute of Standards and Technology (NIST) provides guidelines specifically for the healthcare sector. NIST Special Publication 800-66, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," offers detailed guidance on implementing the security requirements outlined in HIPAA (National Institute of Standards and Technology, 2008). A set of critical security checks known as CIS controls for efficient cyber defense has been developed by the Internet Security Centre. These controls are designed to address common cyber threats and offer specific recommendations for the healthcare industry (Center for Internet Security, n.d.). In addition, ISO/IEC 27001 and 27002, which form the framework for establishing an Information Management System with Security Controls, are also being developed by the International Organization of Standardization. These standards can be applied to healthcare organizations to ensure the confidentiality, integrity, and availability of patient data (International Organization for Standardization, 2013; International Organization for Standardization, 2015).

Healthcare organizations may also refer to the Federal Information Security Modernization Act (FISMA) and its associated guidelines from the National Institute of Standards and Technology (NIST) for comprehensive cybersecurity requirements and risk management practices (U.S. Government Publishing Office, 2014).

2.1Relevant Standards and Frameworks

Compliance with appropriate standards and frameworks which provide guidelines for best practices, control of risks and compliance is needed to ensure a robust cybersecurity in the healthcare sector. Some of the most important cybersecurity standards and frameworks that apply to health care are discussed in this section.

Health Insurance Portability and Accountability Act (HIPAA): HIPAA Privacy Rules set out a standard to protect electronic protected health information, laying down security requirements that healthcare organizations have to comply with. The provisions shall apply in respect of the administration, physical and technically protective measures, including access controls, risk assessment and response to events (U.S. Department of Human Services, 2018).

NIST Cybersecurity Framework: A risk-based approach for managing and improving cybersecurity has been developed by the National Institute of Standards and Technology. It is made up of a set of essential functions that help organizations assess their cybersecurity risks and perform appropriate controls, such as the Identify, Protect, Detect, Response & Recover function (National Institute for Standards and Technologies, 2018).

NIST Special Publication 80053: This publication sets out an extensive list of security and privacy controls for Federal Information Systems and Organizations. It's widely used by hospitals to assess and improve their security postures (National Institute of Standards and Technology, 2020). ISO 27001 International Standard: The requirements for the establishment, implementation, maintenance and continuous improvement of an information security management system referred to as ISMS are laid down in this standard. ISO/IEC 27001 provides a systematic approach to managing information security risks and includes controls specific to healthcare (International Organization for Standardization, 2013). The guidance on the implementation of information security controls for specific healthcare sectors is incorporated in ISO 27799 and complements ISO 27002. The focus is on protecting the confidentiality, integrity and accessibility of health information (International Organization for Standardization, 2016).

Center for Internet Security (CIS) Controls: The CIS Controls provide a prioritized set of best practices to help organizations defend against common cyber threats. The controls are regularly updated and offer specific recommendations for healthcare organizations (Center for Internet Security, n.d.).

HITRUST CSF: The Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) is a comprehensive security and privacy framework specifically designed for the healthcare industry. It integrates various regulatory requirements and industry standards, providing a unified approach to managing risk (HITRUST, n.d). The healthcare institutions can build a robust foundation for cybersecurity by adhering to these standards and frameworks. It provides guidelines for risk assessment, incident response, data protection and compliance that allow organizations to improve their security posture and protect patient information.

2.2. The Concept of Composite Cybersecurity Requirements for Healthcare

The healthcare sector is facing increasing pressures to take strong security measures in the protection of patients' data, ensuring operational continuity and maintaining confidence as it seeks to adopt Digital Technologies more widely. The concept of the common cybersecurity requirement has been developed to deal with emerging problems in healthcare as regards cyber security. The concept of composite cybersecurity requirements and its relevance for the healthcare industry is explored in this section.

A combined set of cybersecurity requirements is an integrated framework that includes current cyber security standards, regulations and good practices into a single set of requirements especially suited to health organizations (El Emam et al., 2018). The convergence approach combines elements from different standards and guidelines to create a coherent and flexible framework for cyber security, which does not rely upon one source or framework. The composite approach recognizes that healthcare environments are unique, with their specific risks, regulatory compliance requirements, and technological complexities. The common framework sets out a structured and comprehensive set of controls in order to address healthcare specific cybersecurity concerns by aggregating and ensuring relevant requirements (Cavoukian et al., 2019).

The advantages of establishing a common framework on cybersecurity standards for health care are numerous. Firstly, this allows healthcare organizations to take advantage of the strengths of a series of standards and frameworks in combination with best practice from different sources. This approach is intended to strengthen the security posture of health care systems, while ensuring that there is a more extensive and inclusive coverage of cybersecurity controls (Kierkegaard et al., 2018). Secondly, a composite framework is helping healthcare organizations to cope with the complexity of regulatory compliance. The composite approach provides a consolidated roadmap for the efficient and effective implementation of multiple compliance obligations, by integrating requirements from relevant regulations such as HIPAA, NIST and ISO (El Emam et al., 2018).

Thirdly, the Convergence Framework makes it possible to adopt a systematic and risk weighted approach to cybersecurity. It enables a more efficient allocation of resources and helps healthcare organizations identify and prioritize security threats, to apply the right checks and to control them. A combination approach increases the organization's ability to respond to most important threats and vulnerabilities through alignment of cyber effort with organizational objectives and risk management strategies (Cavoukian et al., 2019).

In addition, a composite framework is designed to foster consistency and interoperability between healthcare systems and stakeholders. In order to foster communications, collaboration and knowledge sharing between healthcare providers, technology suppliers, regulatory authorities and industry bodies, it is a common language for cybersecurity (Kierkegaard et al., 2018). It is necessary to cooperate with and provide input from different stakeholders in developing a common set of cybersecurity requirements. This entails involving a broad range of experts on cybersecurity, healthcare professionals, policy makers and industry leaders with the aim of ensuring that this framework takes into account diverse perspectives and special needs for health care services (Cavoukian et al., 2019).

3.METHODOLOGY

This paper is aimed at developing a common set of requirements in terms of cyber security for the healthcare industry, by carrying out an overall review of existing standards, frameworks and best practices. In developing the methodology and approach to this paper, these steps shall be taken:

Appropriate scientific articles, research papers, industry reports and the authoritative source for healthcare cyber security requirements will be identified and analyzed in a thorough literature review. The review should help to build on the current state of cyber security in healthcare and provide a sound foundation for understanding. The next step is to identify and evaluate existing standards in the area of cybersecurity, including frameworks and best practices for health care. The key sources are the HIPAA Regulation, NIST Cybersecurity Framework and ISO/IEC Standards as well as other relevant guidelines issued by reputable organizations. This step will give us a glimpse into the state of play in terms of health security requirements.

It is vital to work with the appropriate stakeholders, including cyber security experts, healthcare professionals, policymakers and industry leaders. In order to obtain input, views and insights from the health industry's particular challenges and needs related to cyber security, interviews, surveys or focus groups can be organized. The involvement of the different interested parties will be important in ensuring that the composite framework is adapted to their needs and concerns.

4.IMPLEMENTATION IN HEALTHCARE

Healthcare security team will provide a suitable cybersecurity framework that will be used to evaluate internal and external threats at hospitals based on the historical incidents and analysis conducted by analyzing event logs data from applications, portals, systems, and databases running on the organization infrastructure. Several methodologies and frameworks will be used to reduce the vulnerabilities of network assets, and appropriate strategies were adopted to reduce the organization's risk (Ali, K. A., & Alyounis, S., 2021). The leadership of the hospital will task the security team to ensure that controls were used to facilitate the industry standards and regulatory requirements. In this report, the National Institute of Standards and Technology is the baseline or guideline to conduct a successful risk assessment for hospitals using historical incidents and findings. The organization's cybersecurity requirement will be identified, and controls will be mapped to demonstrate the ability of healthcare to meet regulatory requirements, compliance, and standards (Coventry, L., & Branley, D., 2018).

4.1Healthcare Risk Assessment

The security team must understand that risk assessment is a major component of the CHN risk management process as defined by the NIST 800-53 Rv.5. The security team must manage the information security risk of the organization based on the information system, mission, and cybersecurity goals of the organization (Amiruddin et al., 2021). The healthcare risk management process will be divided into four- steps (frame, assess, monitor, and respond), as shown in Figure 1.

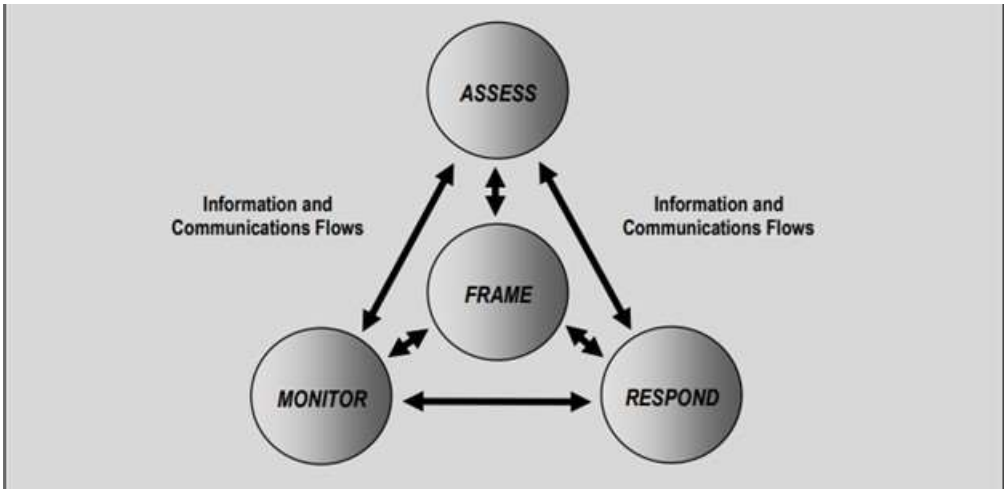

Figure 1: Healthcare Risk Assessment Within Risk Management Process

In the first stage, the security team will address how to frame the organization's risk or establish the risk context environment for the organization. The main goal of the risk context is to develop a risk management strategy to assess, monitor and respond to risk.

During this step, the security team's input is to develop risk tolerance, assumptions, risk assessment methodology, constraints, and business priorities. The goal is to delineate the organization's risk boundaries for effective risk-based decisions (Ganin et al., 2020). The second risk management stage focuses on risk assessment within the healthcare risk context framework. At this step, the threats to the organization are identified in the form of individuals, operations, and assets or threats from other organizations or countries. The security team determines internal and external vulnerabilities, and the adverse effect of an attack on the hospital network infrastructure will be evaluated based on the vulnerability of the organization's assets. Also, the security team will determine the likelihood of an attack, and the end goal at this step is to determine the magnitude and likelihood (Tully, J. et. al., 2020).

The third stage is how the security team will respond to risk once it has been established that a risk has been determined based on the risk assessment conducted. The focus at this point is to provide a constant and consistent organization-wide risk response plan under the approved organization risk frame. It is important that alternative ways are in place to respond to risk, and the alternative actions need to be evaluated. The appropriate action must be consistent with the organization's risk tolerance rate or value. The implementation of the risk response plan must be based on the approved and selected courses of action by the leadership and the security team (Alharam, A. K., & Elmedany, W., 2017).

The fourth stage will require the security team to constantly monitor risk to determine the effectiveness of the risk responses at step three. The risk monitoring will focus on the organization's risk frame to identify the impact of risk changes. The security team will implement a requirement that covers the organization's information security, missions, and vision of risk assessment for a more secure cyberspace (King et al., 2018). Over and above, the security team will ensure an appropriate risk assessment information security architecture that suits healthcare business operation is developed. The developed architecture will support the requirement for the organization's information and security system and other services that support the hospital network infrastructure. The risk assessment will support using security controls that will grant employees the right to operate an information system. Implementing information security solutions is important during the assessment process, but the technology configuration must meet the approved requirements by the security team and industry standards (Buzdugan, A., 2020).

4.2 Healthcare Composite Requirements

Healthcare operates based on the Health Insurance Portability and Accountability Act (HIPAA), and healthcare provider must ensure the integrity, confidentiality, and availability of electronically protected health information of the patient is stored, processed, and transmitted securely. The security team will enforce the HIPAA security rule across its operating location to ensure that covered entities' information is protected and safeguarded from the hands of threat actors. The covered entity information must be protected from impermissible uses and disclosures against unauthorized persons (Coronado, A. J., & Wong, T. L., 2014).

To track the vulnerabilities of the assets running on the healthcare network, the security team will conduct a risk assessment for each asset based on the network asset inventory. Legacy components will be faced out and replaced with technology that can be integrated into the existing cybersecurity solution used at the centralized security operation center (Kierkegaard, P., et. al., 2018). After the risk assessment of the network architecture, the security team will provide a summary of the risk level and the likelihood of exposure based on the assessment conducted. The security team needs to categorize the threats at hospital into two (internal and external threats). Internal threats can be intentional and non-intentional (King, Z. M., 2018). Regarding the types of internal threats, manual and automated checks must be in place to monitor the activities of employees to prevent attacks. The access control solution will enable the security and Information Technology teams to limit an employee's access.

Employees won't be able to access non-business-related resources, and audit log analysis will be enabled to track the activities of employees in real time. Malicious or suspicious activities will be escalated, and an alert will be sent to stakeholders in real time (Ganin, A. A., et. al., 2020). For external threats, deploying Security and Information Event Management solutions will detect and protect threat actors from attacking the healthcare infrastructure (Ali, K. A., & Alyounis, S., 2021). The security team should conduct an industry review before purchasing the security solution (Dhirani et al., 2021). Trustworthy vendors that will pass the organization's cybersecurity requirements should be onboarded into the healthcare tenants to prevent vendor-risk attacks. Many structural errors have resulted in poor configurations, late software upgrades or patches, and allowing non-expert cybersecurity personnel to handle network security solution installation, upgrade, or maintenance. Healthcare must hire experienced experts that have industry experience in deploying security solutions that will ensure healthcare infrastructure is protected from threat actors (Landoll, D. J., 2017).

The HIPAA is the industry standard that governs healthcare business operations. However, some states require that patient data privacy be protected and that the patient must be notified should an incident occur within a specified time frame. The state's attorney general requires data breaches or compromises to be reported, and consumers must be contacted as required by the data privacy law at the state level (Sun, J. et. al., 2019). To prevent healthcare from violating federal and state laws related to its operations, the security team must dedicate a compliance officer who will take responsibility that employees working remotely or onsite comply with the rules and regulations (Landoll, 2017). The compliance officer will review the rule and regulations timely to ensure that he communicates any change in federal and state laws to the employees to prevent violations that may impact the organization's business badly.

4.3Benefit of Mapping Controls

The security team will implement an access control policy and procedures to address the controls within healthcare infrastructure. The risk management strategy will be used to establish policies and procedures per HIPAA and privacy law at the state level. These policies and procedures contribute to covered entities' security and privacy assurance (Coronado, A. J., & Wong, T. L., 2014). The security team will identify authorized system users, and the specification of access privileges reflects the requirements in other controls in the healthcare security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access (Tully, J., et. al., 2020). The importance of mapping in the account management control is to ensure dual authorization, mandatory access control, discretionary access control and security-relevant access control, and role-based access control (Buzdugan, A., 2020).

The security team will enforce flow control restrictions by blocking external traffic that claims to come from the organization tenant, keeping export-controlled information from being transmitted in the clear to the internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. The security team will ensure an inter-organization agreement to transmit information from one organization to the other without data breach or compromise (Romuald, H. et. al., 2020). The security team will create binding techniques to strengthen the information flow enforcement process. This will ensure that healthcare adopts a technique that will prevent an individual's impact when accessing sensitive organization resources without required information flow permission (Sun et al., 2019).

The security team will ensure sufficient audit log storage, and it is advisable to have a dedicated database where the logs are stored for analysis. The log transitioning or transfer will be eliminated to prevent data compromise or breach if the data is not encrypted with the industry-approved technology. The security team will select control enhancement to benefit from increased audit log storage capacity and preserve the confidentiality, integrity, and availability of audit records and logs (Amiruddin, A et. al., 2021).

The security team will create a continuous monitoring program to allow healthcare to maintain system authorizations and create highly dynamic standard controls that cater to the changing healthcare business operation environments, which change in threats, mission, technology, and business needs. Having access to security and privacy information continuously through reports and dashboards allows organizational officials to make effective and timely risk management (Coventry, L., & Branley, D., 2018). The security team will create beginner, intermediate, and advanced cybersecurity literacy training for employees to ensure they are familiar with cyber threat patterns. The security team will design the training and awareness based on the organization's needs. They must ensure the content is easily comprehensible and printed in different languages to cater to non-English speaking overseas employees (Coronado, A. J., & Wong, T. L., 2014).

The organization's requirements will be factors into the training content to ensure that security and data privacy is covered. The content includes an understanding of the need for security and privacy and actions by users to maintain security and personal privacy and respond to suspected incidents. The contract will converge the applicable laws, directives, regulations, and policies and standards that govern healthcare business operations (Alharam, A. K., & Elmedany, W., 2017). The security team will update the literacy training and awareness content timely to ensure that the content remains relevant to healthcare business operations and governing rules and regulations. The following might lead to an immediate update of the literacy training and awareness content: assessment or audit findings, security incidents, executive orders, policies, directives, breaches, and guidelines (Romuald, H. et. al., 2020).

The security team will integrate diverse cybersecurity needs by deploying security controls to ensure the healthcare network infrastructure is secured, and consumer/patient data privacy is protected as required by the law and regulatory bodies (Sun, J. et. al., 2019). Figure 1 summarizes the security controls that will be deployed and integrated into the healthcare network infrastructure to ensure that the organization's cybersecurity needs are met and strategically position the organization's business operation in cyberspace that is free and secured (Landoll, D. J., 2017).

Table 1: Healthcare Controls and Description

Controls	Description
Policies and Procedures	Ensure security and privacy assurance
Account Management	Only authorized users will access the hospital resources.
Information Flow Enforcement	Authorized individual will control information flow within and outside healthcare infrastructure
Security and Privacy Attribute Control	Binding technique will prevent unauthorized access to control information flow.
Content of Audit logs	To preserve the confidentiality, integrity, and availability of audit records and logs.
Continuous Monitoring	Handles change in the organization business environment
Literacy and Awareness Control	Ensure the organization operates with updated rules, regulations, directives, guidelines, policies, procedures, and standards.

5.CONCLUSION/RECOMMENDATION

The security team needs to gather the cybersecurity requirements of healthcare and the policies and laws that govern the requirements. The industry standards, policies, guidelines, and procedures template must be created to track any change in the laws and regulations. The organization's security compliance officer must manage it for timely updates. The organization control template must be created and updated to track the activities within and outside the healthcare network infrastructure (Buzdugan, 2020). Also, the organization's cybersecurity assessment process must outline the step-by-step process to conduct an organizational risk assessment to ensure that healthcare network infrastructure is secured with minimal risk value and a better cybersecurity assessment posture (King et. al., 2018).

To ensure that the assessment and the implementation of controls are adequate and successful, the security team will channel the required effort into the cybersecurity awareness program in the form of the literacy and awareness program described in the literacy and awareness control to ensure that healthcare operates with updates regulations, guidelines, rules, and standards (Tully, J. et. al., 2020).

REFERENCE

1. Alharam, A. K., & Elmedany, W. (2017, August). Complexity of cyber security architecture for IoT healthcare industry: a comparative study. In 2017 5th international conference on future internet of things and cloud workshops (FiCloudW) (pp. 246-250). IEEE.

2. Ali, K. A., & Alyounis, S. (2021, July). Cybersecurity in healthcare industry. In 2021 International Conference on Information Technology (ICIT) (pp. 695-701). IEEE.

3. Amiruddin, A., Afiansyah, H. G., & Nugroho, H. A. (2021). Cyber-Risk Management Planning Using NIST CSF v1. 1, NIST SP 800-53 Rev. 5, and CIS Controls v8. In 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS (pp. 19-24). IEEE.

4. Buzdugan, A. (2020). Integration of cyber security in healthcare equipment. In 4th International Conference on Nanotechnologies and Biomedical Engineering: Proceedings of ICNBME-2019, September 18-21, 2019, Chisinau, Moldova (pp. 681-684). Springer International Publishing.

5. Cavoukian, A., Jonas, J., & Nagy, B. (2019). Privacy by Design for the Age of Big Data. Springer.

6. Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. Biomedical instrumentation & technology, 48(s1), 26-30.

7. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48-52.

8. Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. Sensors (Basel, Switzerland), 21(11).

9. El Emam, K., Samet, S., Huot, C., Earle, C., & Tamblyn, R. (2018). A Framework for the Assessment of Security Vulnerabilities in Health Data within a Hierarchical Privacy Model. Journal of Medical Internet Research, 20(6), e10319.

10. Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. Risk Analysis, 40(1), 183-199.

11. Kierkegaard, P., Buntrock, S., & Buus, R. (2018). Toward a Composite Framework for Assessing Security Measures in the Healthcare Sector. International Journal of Cyber Warfare and Terrorism, 8(1), 1-14.

12. King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Frontiers in psychology, 9, 39.

13. Landoll, D. J. (2017). Information security policies, procedures, and standards: A practitioner's reference. Auerbach Publications.

14. National Institute of Standards and Technology. (2008). NIST Special Publication 800-66 Revision 1 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-66/rev-1/final

15. Romuald, H., Jarosław, N., Tomasz, P., & Jerzy, S. (2020). Risk Based Approach in Scope of Cybersecurity Threats and Requirements, Procedia Manufacturing, Volume 44, 2020, Pages 655-662, ISSN 2351-9789

16. Sun, J., Liu, S., & Sun, K. (2019, November). A scalable high fidelity decoy framework against sophisticated cyber-attacks. In Proceedings of the 6th ACM Workshop on Moving Target Defense (pp. 37-46).

17. Topol, E. J. (2019). High-performance medicine: The convergence of human and artificial intelligence. Nature Medicine, 25(1), 44–56.

18. Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. Health security, 18(3), 228-231.

19. U.S. Department of Health & Human Services. (2018). Summary of the HIPAA Security Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

20. U.S. Government Publishing Office. (2014). Federal Information Security Modernization Act of 2014. Retrieved from https://www.govinfo.gov/content/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf

21. Ventola, C. L. (2014). Mobile devices and apps for health care professionals: Uses and benefits. Pharmacy and Therapeutics, 39(5), 356–364.

22. World Health Organization. (2021). Digital health. Retrieved from https://www.who.int/health-topics/digital-health