American Journal of Multidisciplinary Research and Innovation (AJMRI)

ISSN: 2158-8155 (ONLINE), 2832-4854 (PRINT)

VOLUME 4 ISSUE 4 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Multidisciplinary Research and Innovation (AJMRI)

Volume 4 Issue 4, Year 2025
ISSN: 2158-8155 (Online), 2832-4854 (Print)
DOI: https://doi.org/10.54536/ajmri.v4i4.5086
https://journals.e-palli.com/home/index.php/ajmri

Sustainable Cybersecurity in Healthcare An AI-Integrated Risk and Resilience Framework

Adam Thawbaan[1*], Gilles Dusserre[2], Yusuf Muritala Kolade[1], Yasir Abdulkareem[3]

Article Information

Received: March 18, 2025

Accepted: May 22, 2025

Published: August 05, 2025

Keywords

Cybersecurity Framework, Healthcare Resilience, Machine Learning, Risk Management, Vulnerability Assessment

ABSTRACT

As more healthcare systems are digitalized, the quality of patient care and operational efficiency have improved, but at the same time, the modernization of healthcare systems has made healthcare organizations extra vulnerable to serious cybersecurity threats. This paper reveals major gaps and inconsistencies between healthcare business units, including gaps between healthcare organizations, as it inspects existing cybersecurity practices and policies in the healthcare sector. The NIST Cybersecurity Framework along with GDPR and HIPAA have been adopted but ransomware, breaches, and insider incidents remain ongoing threats to healthcare organizations. The study proposes a comprehensive three-layered approach to address the above three challenges: (1) mathematical vulnerability assessment model based on Asset Vulnerability Impact Assessment Model (A-VIAM), (2) integration of advanced technologies such as machine learning for threat detection and response, and (3) development of a sound security management framework tailor-made for healthcare facilities. The contribution of this research is a comprehensive approach for mitigating risk from cyber to a reduced level which is at acceptable level using Hybrid methods such as Content Analysis and Quantitative Modeling with Comparative Analysis. Managers, policy makers and digital security specialists in healthcare will benefit from the research results increasing their knowledge about digital resilience in healthcare.

INTRODUCTION

The cost of a single EHR on the black market is 10-to 100-fold more than a single credit card (Bhuyan *et al.*, 2020). Data cannot be 'reset' in case of loss or theft of medical records (Yeng *et al.*, 2019).

The healthcare industry has witnessed a rapid digital transformation over the past years with the aid of telemedicine, electronic health records (EHRs) and other digital technologies (Watson, 2016). While access and patient care may have improved, the industry is more susceptible to new and evolving cybersecurity threats. A particularly crucial and critical issue is the security of patient data and health infrastructure, since the increasing frequency and technical complexity of cyberattacks against healthcare organisations has been highlighted by recent literature (Lindner *et al.*, 2022). The COVID-19 pandemic accelerated implementation of remote patient monitoring and telemedicine, raising the importance of effective cybersecurity measures in rapidly changing healthcare environments (Smith *et al.*, 2021).

Impact to Healthcare: With the large amount of Protected Health Information (PHI) and Personally Identifiable Information (PII) being handled, healthcare entities have a unique set of issues in cybersecurity. Sensitive information is processed by practically every unit in the health sector, not something that can be said for other industries where cybersecurity is generally confined to one or more departments (Aijaz *et al.*, 2023). The newness of cybersecurity to healthcare and its associated budget constraints lead to questions around where to put resources. The complexity of connected medical devices as well as diverse business processes should also be considered by cybersecurity of healthcare (Rajamaki *et al.*, 2018).

When stolen PHI cannot be changed by victims, a healthcare breach has dramatic implications. In the shadowy corners of the internet, information like that can be more precious than a credit card number or a social security number. While they pose organisational and technical challenges, policy frameworks such as the GDPR in the EU and HIPAA in the US have emerged to safeguard data (Manzuik *et al.*, 2006). Some critical hospital services, such as the treatment of patients with medication and surgery, can mean death instead of harm when placed on an indefinite hold by a cyberattacker. Digital forensics and liability assignment are complex, and the operations of a hospital and the patients' trust are threatened (Argaw *et al.*, 2020).

Cyberattacks have risen in the healthcare sector, including more than in the financial industry. These cases demonstrate just how critical it is for the healthcare industry to enhance its cybersecurity to protect patient information, patient safety, and hospital functioning (Coventry & Branley, 2018). And in healthcare, even though we have known about the threats for some time, we are still struggling against cybersecurity attacks that could lead to data breaches, loss of profits, and perhaps even the ending of patient lives. Recent research suggests that ransomware, data breaches, and unauthorized access to medical devices continue to prey upon healthcare

[1] IMT Mines Ales, France
[2] University of Nîmes, Nîmes, France
[3] University of Derby, Derby, United Kingdom
[*] Corresponding author's e-mail: adasabaa1@gmail.com

groups (Wasserman & Wasserman, 2022). Such incidents present a significant public health threat, as they violate patient privacy and disrupt necessary healthcare. To effectively face this issue, practicing cybersecurity, building security frameworks, and deploying advanced threat detection and defense solutions are required (Wang *et al*., 2023). This led to the following research questions: What is the current state of cybersecurity practices and policies pointing to vulnerabilities in healthcare? What gaps still remain in the healthcare industry? How can our proposed model be used to strategically control cyber risk within the healthcare environment at an acceptable level?

The goal of this research is to tackle this important problem by

• Evaluating the healthcare industry's current level of cybersecurity preparedness, including an assessment of the industry's vulnerabilities and threats, and highlighting the best practices in the industry.

• Recommending the ideal next-generation threat detection and response approaches using the latest in machine learning and threat intelligence

• Personalized security management frameworks to suit the needs and regulation of healthcare organizations.

LITERATURE REVIEW

Cybersecurity in Healthcare

In this modern digital age, the health sector has become increasingly reliant on internet-based communication, networked medical devices, and electronic health records (EHRs) (Hodge *et al*., 2016). According to Yusuf *et al*. (2024), electronic healthcare technology is widely used and presents numerous chances to improve clinical results and change care models around the world. Yet, worries about the security of medical devices and data are becoming more prevalent. The innovations have made sharing information and delivering care easier, but they have also led to pressing cybersecurity problems. The industry now considers protecting non-public patient information and healthcare infrastructure from cyberattacks a top priority (Singh *et al*., 2023). To identify weaknesses, as well as strengths and developmental needs, we provide an extensive analysis of the review of existing cybersecurity practices and policies within the healthcare sector in this paper.

Due to the nature of the sensitive patient information they possess, healthcare organizations are attractive targets for online criminals (Hodge *et al*., 2016). Healthcare organizations have been bombarded with cyberattacks, especially over the past several years, as ransomware attacks, data breaches, and various other security issues have become more common. In instances such as these, patient safety, confidentiality, and the broader integrity of healthcare may be placed under tremendous risk (Carthey & de Leval, 2001).

Existing Theories of Cybersecurity in Healthcare

Several theories and models provide implications on how to protect patient data and hospital systems, and cybersecurity in health contexts is an emerging area of research and practice. These theories embody a range of strategies and concepts that guide the development and enactment of medical cybersecurity countermeasures.

Here are a few interesting theories

1. Defense in Depth: Multiple layers of security defenses are particularly important as per the Defense in Depth concept (Nifakos *et al*., 2021). This includes implementing an array of administrative, technical, and physical defenses that can protect varying forms of cyber threats within the healthcare sector. It also underscores the importance of tracking security measures as well as keeping them updated.

2. Zero Trust: The Zero Trust approach to network trust questions the typical concept of trust. It also encourages verifying the identity of every user and device attempting to access resources – even when they belong to the same company's network (Argaw *et al*., 2020). When it comes to healthcare, we need to regulate and verify that we are controlling patient data accordingly, and I work in healthcare, so this concept is very applicable.

3. Threat Modeling: Identifying and assessing various threats to healthcare systems and health data is called threat modeling. Healthcare organizations may develop strategies to reduce these risks by identifying risks and vulnerabilities. This approach aligns with the proactive nature of cybersecurity in the healthcare space (Aijaz *et al*., 2023).

4. NIST Cybersecurity Framework: The National Institute of Standards and Technology (NIST) framework provides a structured manner for cybersecurity (Argaw *et al*., 2020). Healthcare providers can use the functions and the categories and subcategories to assess their cybersecurity readiness and adapt their methods accordingly.

5. Human-Centric Theories: Theories such as the "Human Firewall" emphasize the importance of training staff in healthcare and focused on identifying and responding to these behavior-based threats, which recognize that people in healthcare are vital components of cybersecurity (Nifakos *et al*., 2021). The risk introduced by insiders and the need for prevention and detection are also supported by the concept of Insider Threat.

MATERIALS AND METHODS

To understand the current condition of cybersecurity practices in healthcare towards a comprehensive solution for identified vulnerabilities, this research has adopted a mixed-methods research approach including qualitative content analysis, quantitative modelling and comparative analysis.

Content Analysis

The qualitative content analysis method was employed to analyze academic papers, policy papers, and case studies in healthcare cybersecurity. By using this method,

we were able to identify areas of commonality, security concerns, and possible transposition within the policies and standards for information security that existed. The sources are peer-reviewed journals, legal documents such as HIPAA and GDPR regulations, and previous evidence of cyberattacks on healthcare organizations (Argaw *et al.*, 2020; Singh *et al.*, 2023; Patel, 2020). Analyses of structured content provided a scoping structure and specific features of an enhanced and integrated security framework.

Quantitative Analysis

Mathematical modeling for the analysis of cybersecurity vulnerabilities, we based the mathematical model on the Asset Vulnerability Impact Assessment Model (A-VIAM) of Kure *et al.* (2018). This model created the basis for a systematic and ordered estimation of vulnerability degree throughout healthcare systems, instruments, and infrastructures. Key elements included:

• Device Criticality (DC): It is obtained through asset-weighted importance (by organizational decision-makers) multiplication by the impact importance, varying from 0.01 to 1.00 and 1.00 to 10.00, respectively.

• Vulnerability Impact Rating (VR): Ranging from 1 to 5 (very low to very high) indicating the potential risk of the asset to cyber threats.

• Vulnerability Impact (VI): A weighted score average of the vulnerability across crucial services, classified as low (1.00–3.99), medium (4.00–6.99), and high (7.00–10.00).

This quantitative evaluation was necessary in order to allocate resources and design a focused response plan under the prospective security model.

Comparative Analysis

The healthcare industry's existing cybersecurity practices were contrasted with the best practices and standards of the industry (e.g., ISO/IEC 27001; NIST Cybersecurity Framework). This approach allowed the identification of gaps between current organizational techniques and the accepted international standards (Ntantogian *et al.*, 2021; El Rob, 2023). The study identified areas for improvement, including 'staff training, infrastructure modernization, and policy harmonization' by contrasting current practices with those advised by regulatory agencies and the literature.

Observation and Evaluation

Observation and assessment methods are prescribed for use in practice to help inform the implementation pathway of the proposed solution. AI solutions outperform traditional rule-based processes in detecting and thwarting cyberthreats (Khan *et al.*, 2025), this includes applying machine-learning-based threat detection technologies, staff interaction with simulated attacks, and system resistance against penetration tests, these approaches involve iterative observation of the performance of the security framework within a healthcare environment. Feedback loops over time and real-time system assessments are required for flexibility and adaptation owing to the ever-evolving nature of cybersecurity threats (O'Brien *et al.*, 2020; Pappalardo *et al.*, 2020).

Justification of Methods

All methodological approaches were taken to ensure an in-depth, useful analysis of cybersecurity in healthcare. Comparative approach ensured alignment with international practice, quantitative modelling brought objectivity and prioritization to decision making and content analysis provided depth and context. To guide the development and implementation of an effective cybersecurity management system, this complementarity offered strategic and tactical directions.

State Of The Arts Results

Current cybersecurity practices

Several cybersecurity practices and measures are commonly employed in the healthcare sector to protect patient data and critical infrastructure and some of the existing cybersecurity practices in healthcare are shown in Table

Table 1: Current Cybersecurity Practices in Healthcare.

Literature	Practice Observed	Description
Clarke and Martin, 2023	Access control	Healthcare institutions enforce strong role-based access control so that only appropriate individuals may access patient records and other sensitive information.
Patel, 2020	Encryption	The data should be secured in transit and at rest, through encryption. In order to prevent unauthorized access, private patient data are often encrypted by hospitals while in transit between systems, and while stored in databases.
Rob, 2023	Data Loss Prevention (DLP)	DLP products prevent unauthorized data transfer and access by enforcing outgoing traffic policies and applying encryption.
Yeo, 2023	Security Information and Event Management (SIEM)	SIEM products are deployed to observe, analyze, and respond to events in real time, so pick one that fits your use case the best.

Rajamaki and Nevmerzhitskaya, 2018	User Training and Awareness	Healthcare personnel are trained for cyber threats regarding phishing, social engineering, and other threats to reduce human error by identifying and responding to these kinds of attempts.
Clarke and Martin, 2023	Security Assessments and Audits	Regular security audits and exercise are performed to search out the weakness, compliance issues, and where need improvement.
Nifakos *et al.*, 2021	Compliance with Regulations	In order to ensure patients are kept private and safe, health quotient organisations abide by laws such as HITECH (Health Information Technology for Economic and Clinical Health Act) and HIPAA (Health Insurance Portability and Accountability Act).

Current Cybersecurity Policies

There are several notable cybersecurity policies that are been adopted by the healthcare sector to strengthen their cybersecurity culture and practices as can be seen in Table 2 below.

Table 2: Current cybersecurity policies as observed in healthcare and brief description.

Literature	Practice Observed	Description
Patel, 2020	Health Insurance Portability and Accountability Act (HIPAA)	HIPAA sets forth protections for electronic health information of patients for their security, privacy, and security.
Argaw *et al.*, 2020	Health Information Technology for Economic and Clinical Health (HITECH) Act	The HITECH Act introduces additional privacy and security standards under HIPAA and provides subsidies to medical providers for implementing electronic health records (EHRs).
Ntantogian *et al.*, 2021	The General Data Protection Regulation (GDPR)	GDPR also apply and healthcare bodies treating EU citizens and require these to have more robust data protection measures including cybersecurity as well as obligations to notify of breaches.
Panattoni, 2020	Cybersecurity Information Sharing Act (CISA)	On the healthcare side of cybersecurity, CISA encourages the compatibility of cyber information between federal and private sector entities when it comes to discussing cybersecurity threats and weaknesses.
Argaw *et al.*, 2020	National Institute of Standards and Technology (NIST) Cybersecurity Framework	Voluntary adoption may be more common among healthcare entities who adopt the best practices and standards promulgated by NIST's framework on how to manage and reduce cybersecurity risk.
Koppel *et al.*, 2015	Electronic Health Record (EHR) Certification Requirements	EHR certification programs set standards for EHRs used in healthcare, including those for security and interoperability.
Nifakos *et al.*, 2021	Federal Risk and Authorization Management Program (FedRAMP)	FedRAMP provides cloud security standards for services and products purposes working with government organizations in the healthcare sector.
Yeo, 2023	International Standards and Guidelines	Healthcare entities can also elect to adopt independent standards with respect to information security (such as ISO/IEC 27001, developed by the International Organization for Standardization (ISO)) to reinforce security practices.

Perceived Vulnerabilities of Current Healthcare Cybersecurity practices

• Lack of Standardisation: There are no established cost effectiveness models since guidelines and frameworks for the healthcare cybersecurity programs are not yet provided in a standardized basis (Aljuraid & Justinia, 2022). Due to such heterogeneity, there are also weak links in the system that can be exploited by attackers.

• Ageing Infrastructure: Since many healthcare providers continue to employ outdated medical gear and IT systems, they are more susceptible to hackers. Most of the security dimensions of current technologies are lacking in the older systems (Coucke *et al.*, 2020).

• Insider Threats: Intentional and accidental insider threats are a serious risk. Workers in possession of patient data can intentionally or unintentionally cause patient

records security breaches (Hodge *et al.*, 2016).

Strengths of Current Healthcare Cybersecurity Practices

More Awareness: The value of cybersecurity is getting more attention throughout healthcare. There is a growing investment in security awareness and training to employees among users (Argaw *et al.*, 2019).

Regulatory Compliance: A certain requirement of cybersecurity is that healthcare organizations make cybersecurity a part of the plan of action to comply with the Health Insurance Portability and Accountability Act (HIPAA) and other regulations such as (Biasin & Kamenjasevic, 2020). The result of such regulations has been advancements in the industry's security procedures.

Collaboration: Healthcare organisations are working with governments, cybersecurity specialists and business partners to improve the quality of their security activities and collaborate on threat intelligence (Tovstiga *et al.*, 2010) as part of their security efforts.

Areas in Need of Improvement

- Resource availability: Resource availability in the form of no interest or funding provided for cybersecurity in healthcare organizations tend towards underutilized and understaffed SOC's (Lamba & Jain, 2021). Adequate funding is imperative for protection of sensitive patient data.
- Security Education: Healthcare staff need regular training to recognize and respond to cyber risks. Education development initiatives can act as preventive measures for breaches (Tovstiga *et al.*, 2010).
- Security Auditing and Monitoring: Keep your networks, systems and information under constant surveillance. Robust auditing and monitoring services can be used to detect and respond to threats (Argaw *et al.*, 2019).
- Sharing information: Health systems must find better ways of sharing information about cyber threats. Collaboration can prevent and address making attacks across the industry (She, 2021).

Use Case Description

Case examples

The following examples of cyberattacks illustrate the type and consequences of these attacks in various parts of the world and the measures institutions have taken in response.

Lukaskrankenhaus Neuss (Germany)

Background and Aims

The case highlights the holes in healthcare security, particularly after a relatively small ransomware attack was able to push a hospital to stop performing high-risk procedures. A healthcare-specific security management framework should cover rapid response procedures, employee training and safeguarding of essential healthcare services (Argaw *et al.*, 2020).

To mitigate these exposures, the institution developed action plans and routine training for employees while also strengthening the safety of key healthcare functions, demonstrating the need for a solid security plan (Argaw *et al.*, 2019).

South-eastern Norway regional health authority (Norway)

The attack, which impacted almost half of Norway's population, underscores the importance of legacy systems in health security. A framework would determine the phased roll out of the outdated systems with stringent security audits and save from scopes of mass incident (Bassett, 2023). To Improve Healthcare security, the group advocated for mandated phasing out of aging systems and implementing strict security protocols to thwart major attacks and underscored the value of modernizing infrastructure (Nilsen, 2021).

Hancock regional hospital (United States)

The specific and highly vectored attack on Hancock Regional hospital demonstrates just how much hospital environments need to adopt a proactive security posture. A secure framework ought to be designed with proactive threat monitoring, improved network segmenting, and adequate cybersecurity training to mitigate such attacks (Argaw *et al.*, 2020). To prevent such accidents from occurring in future, the organization has integrated proactive monitoring of threats, network segregation, and training the employees through cybersecurity program, emphasizing on the need for a proactive and comprehensive security framework (Coventry *et al.*, 2020).

WannaCry ransomware attack (Global)

The cyberattack, which left some parts of the world crippled and affected at least 45 NHS Trusts and hospitals in the UK, was launched on Friday, 12 May.

The international scale of the WannaCry assault laid bare the interdependence of healthcare networks. International collaboration may be an important aspect to include in a framework to share threat intelligence and best practices to protect healthcare systems around the world," (Minnaar & Herbig, 2021). Healthcare systems have seen the writing on the wall for global WannaCry attack. A framework was suggested that promotes collaboration to share threat information and best practices on a global level, highlighting the interdependence of health systems and the need for shared security (Minnaar & Herbig, 2021; Harkin & Freed, 2017).

SingHealth Cyberattack (Singapore)

The SingHealth breach serves as a reminder to have round-the-clock security - particularly in healthcare systems teem with sensitive patient data. A framework should provide strong data encryption protocols, access control mechanisms and continuous security reviews to protect patient data (Teoh *et al.*, 2022). In this context, a framework (Teoh *et al.*, 2022; Kandasamy *et al.*, 2022)

was suggested, which proposed data encryption, restricted access and continuous audit to protect sensitive patient data, emphasizing the urgency for strong privacy protection measures.

Allscripts Ransomware Attack (US):
During the Allscripts attack, the disrupted clinical operations served as a timely reminder that healthcare organizations should weigh third-party service providers' security within the larger healthcare umbrella. A framework ought to have heavy-handed cybersecurity requirements for suppliers and service providers (Al-Qartah, 2020). To improve the security of the healthcare ecosystem, a policy was proposed that included a set of robust cybersecurity standards for suppliers as well as for service providers, emphasizing the importance of the role of context-specific requirement in a supply relationship (Al-Qartah, 2020; Tetteh, 2019).

Johns Hopkins Medicine Data Breach (US)
This case illustrates the dangers of insider threats and the importance of thorough training of employees. A framework should include employee awareness program, incident response plans on internal threats, and periodic security audit (Ariyo & Zheng, 2022; Jiang & Bai, 2019). A customized model was suggested for employee awareness activities, the enactment of incident response scenarios targeting inside threats and conducting periodic security tests to highlight the need of having holistic security strategies regarding the handling of insider threats (Ariyo & Zheng, 2022; Jiang & Bai, 2019).

Proposed Solution
It can be observed that healthcare industry faces significant cybersecurity challenges, with vulnerabilities arising from a lack of standardization which is a key problem because there are many frameworks that have been proposed by researchers and other organized bodies amongst others. This lack of standardization causes inconsistent security measures across organizations leading to a variability with the potential to become exploitable vulnerabilities. Thus, to improve healthcare cybersecurity, we would be proposing the integration of three solutions. Namely.

1. Vulnerability assessment (mathematical approach)
2. Integration of advanced technology
3. Robust inclusive security management framework

By addressing these areas, the healthcare sector can better protect sensitive patient data and critical infrastructure, ensuring the continued provision of safe and secure healthcare services.

A mathematical approach to vulnerability assessment
This was adapted from Asset Vulnerability Impact Assessment Model (A-VIAM) by Kure *et al.* (2018) to determine the vulnerability and criticality of the vulnerabilities that exist in healthcare. This represents progress towards harmonizing healthcare approach towards vulnerability assessment and management as a decision-making tool in identifying criticality of existing vulnerabilities in healthcare.

Device Criticality (DC)
This will be determined based on the weight score and the impact value score.
"Device criticality (DC) = Asset weight score × Impact value score"

$$DC = \sum_{i=1}^{10} Wi \times Vi$$

Where:
IV = Impact value will range from 1.00–10.0
W = Weight score will range from 0.01–1.00
NB:
A weight score will be assigned to each asset based on the subjective judgment given by the organization's stakeholders.

Vulnerability Impact Rating
The impact of vulnerability on critical devices will be assigned a Vulnerability Rating (VR) score of VR.1 to VR.5 from very low to very high for the vulnerability found on each critical device.
The VR score, criteria and description can be seen in the Table 3 below.

Table 3: VR score table

Score (VR)	Criteria	Description
VR.5	Very high	=>1 major weaknesses identified Device extremely susceptible to attack No capability of healthcare to resist threat
VR.4	High	=>1 major weaknesses identified Highly susceptible to attack Low capacity of healthcare to resist threat
VR.3	Medium	A weakness identified Moderate susceptibility to attack Reasonable capability to resist threat
VR.2	Low	A minor weakness identified Slightly increases the susceptibility to attack Good capacity to resist threat
VR.1	Very low	No weaknesses exist Excellent capability to resist threat

Vulnerability Impact

To determine the vulnerability impact on a device

The calculation of mean value vulnerability is shown below, N is the total number of vulnerabilities:

VI(CD) = (1/N)(VR1+VR2+⋯+VRN)

where: VI = Vulnerability Impact of the critical device CD.

Another possibility is to calculate VI(CD) as the maximal value of VR1,VR2,…,VRN.

Scores range between 1.00 and 10.0: 1.00–3.99 = low, 4.00–6.99 = medium and 7.00–10.0 = high.

VR = Vulnerability Rating. A score of 1–5 is given for the VR as shown in the table before.

CD = Critical device.

To calculate vulnerability impact of an entire system, the Mean Vulnerability Impact of each CD, VI(CD) will be summed together and divided by the total number of assets identified using the equation below:

VI(S) = (VI(CD1) + VI(CD2) . . . + VI(CDn)) / total number of devices

where S = Overall Critical Infrastructure System.

The category of the overall vulnerability system will have a range indicating a vulnerability score on a scale from 10% to 100%.

Calculation can further be used for risk assessment factoring in likelihood of occurrences, level of attacker. As seen in the work of Kure *et al.* (2018).

Integrating Advanced Threat Detection and Response Mechanisms in Healthcare

Advanced threat detection and response analytics, particularly machine learning, complement and harmonize previously developed resources and practices in healthcare cybersecurity (Carrasco & Wu, 2020). This next-generation technology inherits from predecessors and adds to it the ability to voluntarily self-detect and self-mitigate security threats.

Anomaly Detection, As A Refinement of Intrusion Detection Systems (IDS)

Anomaly detection, as part of machine learning systems, complements standard Intrusion Detection complete systems (IDS) used already in healthcare. Although IDS can detect known patterns of attack, machine learning can enhance this capability by the identification of small anomalies in the normality in networking behaviors (Atefi *et al.*, 2020).

Predictive Analytics, Relying on Threat Intelligence

Predictive analytics employs machine learning to forecast potential threats based on historical data, and this approach is compatible with threat intelligence models already in use in the healthcare sector (Mathew *et al.*, 2023).

Rapid Incident Response, Building on Incident Response Plans (IRP)

Machine learning expedites incident response by providing an adjunct to established Incident Response Plans (IRP) used in healthcare (Bonafide *et al.*, 2014).

Adaptability, Enhancing Existing Cybersecurity Strategies

The flexibility of machine learning fits well with the changing landscape of healthcare cybersecurity. Institutions of healthcare likely to keep evolved security forecasts, which help in being in par with the emerging threats (O'Brien, 2020).

Robust Security Management Frameworks

Healthcare providers are stewards of vast quantities of sensitive patient information such that in the event of a data breach the impacts can be catastrophic, impacting patient safety, trust and to an extent, integrity of healthcare systems (Pappalardo *et al.*, 2020). The importance of strong security management tools is emphasized as cyber threats against the healthcare industry grow in complexity.

The conceptual model emphasized a risk-based view of security management. This requires recognising threats, gauging the likelihood of these threats, as well as rating the risk of security events (The Office for Civil Rights, 2022). Prioritizing resources according to risk will enable healthcare organizations to put their efforts where it matters.

And it involves ongoing surveillance and reviews. It is not sufficient to just do it, it must be a continuous process given evolving threat (O'Brien, 2020). Auditing and evaluation are key elements of this system. However, a well-structured incident response plan recommended by The Office for Civil Rights, (2022) was embedded. Healthcare companies must be operationally prepared to react to security incidents quickly. This response went on, limiting the impact of the breach and downtime. Technical and administrative response should be combined in incident response handling. And to help reduce the human element error – continual security training and awareness campaigns around best practices and threats they may face in their specific positions.

Proposed security management frameworks

Knowing that the threat landscape for cyberattacks in the healthcare industry is constantly changing, it is essential to develop strong security management frameworks (The Office for Civil Rights, 2022). Is there some framework that must be in place to protect that data and the healthcare system on which it depends? This research delivers a structured security management process model to meet the specific needs of healthcare facilities by integrating best practices and regulatory requirements. The items in the security management framework for healthcare settings on flowchart 1 are input to the critical areas to be improved. The structured nature of the framework will make it easier for resources to be used effectively by recognizing and prioritizing risks and thus guaranteeing that healthcare providers adequately invest

in cybersecurity. It promotes a culture of security among healthcare personnel and focuses on continuous security education to enable proactive threat identification and prevention. Core elements of the framework, especially those related to monitoring and auditing, provide the tools necessary to rapidly identify and respond to threats. The implicit information sharing in the framework also makes for a partnership and transfer of cybersecurity threat information helping everyone in the healthcare field to work together to stop prevent and minimize attacks. Together these pieces bring an exhaustive and evolving security approach to healthcare entities.

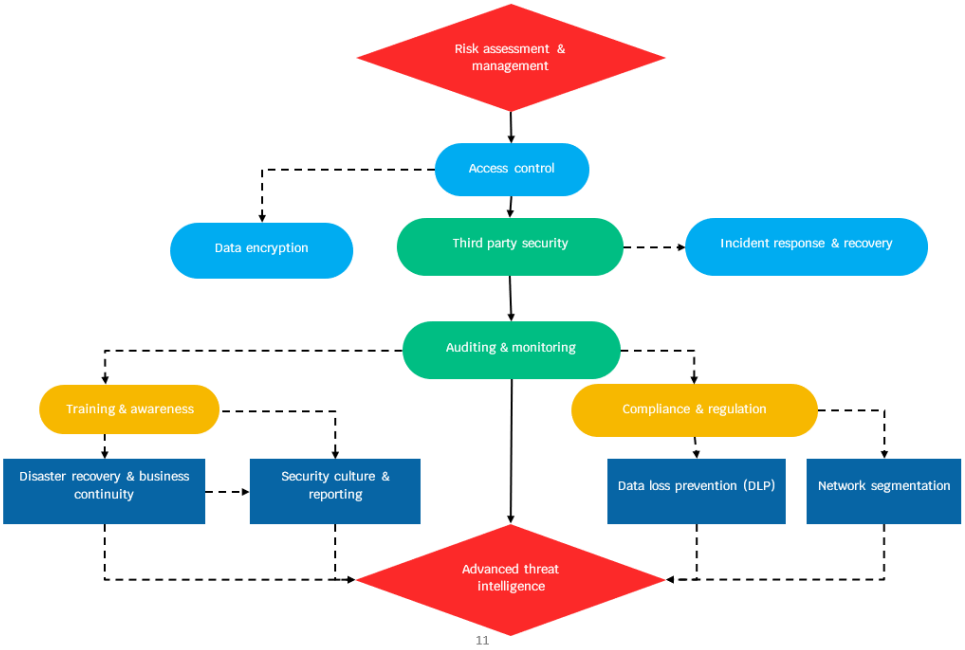

Figure 1: Security Management Framework

Proposed Implementation process of the Framework

It is suggested that to facilitate the successful deployment of the proposed Security Management Framework for healthcare and ensure some measure of reckoning and control over healthcare cybersecurity, it must be implemented in a strategic and phased manner. First, alignment of leadership and engagement of stakeholders is essential to gain commitment and understanding. A gap analysis and risk assessment for prioritizing vulnerabilities is the next step after the initial creation of the detailed documentation of the framework components and operations. Tailoring for the unique requirements of the hospital/ health system is key, and integration with other tools and systems that already exist and working with IT enables a unified approach to cybersecurity.

Then, the execution phase would follow with an extensive training and awareness program for healthcare professionals, with a focus on the guidelines of the framework as well as best-practices cybersecurity. A trial run in a confined area would provide feedback to fine-tune and refined before a full roll out. The company-wide launch is supported by ongoing support and mechanisms for monitoring the performance of the framework. Incident response drills, documentation, and reporting help build flexibility into the framework, which recognizes that the cyber threat landscape is constantly evolving. Building feedback loop and providing regular training refresher coverages to enable a culture of improvement and raise awareness on healthcare staff about cybersecurity.

Discussion

The findings from this research indicate that reactive measures, such as access control, encryption, and regulatory compliance, have been implemented by healthcare organizations, however, the implementation can be characterized by a fragmented or piecemeal approach, which is often inadequate to protect sensitive data within a rapidly evolving threat landscape. The confirmed weaknesses, such as the outdated infrastructure, irregular activities and limited qualified staff training, validate previous literature reports that classified healthcare as one of the most vulnerable sectors in the digital universe (see, for instance, Bhuyan *et al.*, 2020; Coucke *et al.*, 2020). Even those that are compliant with stringent regulations like HI- PAA, HIPAA, or GDPR still fall victim to breaches, putting the point across that being compliant to IT related policies is not the same as being secure (Patel, 2020; Ntantogian *et al.*, 2021).

The integrated three-tier approach, developed in this study, consisting in a vulnerability assessment model, state-of-the-art threat detection technologies, and an efficient security management framework overcomes the limitations of current practices. The mathematical

risk assessment model based on Kure *et al.* (2018) offers an impartial approach to measure and rank risks. Such information would be of immense value to healthcare institutions as most do not have structured approaches for effective resource allocation in view of such risk (Lamba & Jain, 2021). Using a scalable and evidence-based approach, the model bridges a methodology void from current cybersecurity risk management techniques.

Furthermore, the incorporation of machine learning in healthcare cybersecurity represents a major improvement over the existing tools. Compared to conventional IDS, machine learning–enabled ADR can be tailored to address novel threats by learning from historical and real-time data (Atefi *et al.*, 2020; Mathew, 2023). This is particularly critical in healthcare, where new vulnerabilities or are common exploitation vectors in healthcare. Similarly, the forensic application of predictive analytics and automated incident response improve readiness while decreasing time-to-containment – both performance measures critical to minimizing harm of cybersecurity incidents (Bonafide *et al.*, 2014).

The proposed security management framework also covers issues related to organizational and human aspects that are sometimes neglected by purely technical solutions. In healthcare, cybersecurity is not only a technical issue, but also a socio-technical one (Nifakos *et al.*, 2021). Through the integration of ongoing staff training, security culture development, vendor risk management, and compliance auditing the model also resonates with the literature highlighting human-centric safety models and system resilience (Argaw *et al.*, 2019; O'Brien *et al.*, 2020). Additionally, the framework encourages interoperability, which is a crucial issue while matching and integration of the practices as demonstrated in this work and approved with previous studies (Aljuraid & Justinia, 2022).

There are limitations to the research, despite its strengths. First, are theoretically grounded in documented cases and derived from documented use cases, but the model and framework have yet to be implemented or tested in practice. Future empirical validation in preliminary studies in hospital setting could improve the credibility of the framework and give an idea of its implementation challenges. Second, the critical device vulnerability is taken into consideration by the model, but it does not incorporate a threat actor profiling or the environment changes dynamically (e.g., policy change and sudden public health crises).

However, the implications of this work are significant. This framework offers a modular structure that goes beyond compliance. An extended cybersecurity framework and its application for healthcare hospital leaders, policymakers, and IT leaders need to examine and adopt a strategic, modular approach to cybersecurity which goes beyond a check-box approach and focuses on proactive detection of threats, rational prioritization, and culturized integration. The model also provides a platform for future growth into realms as diverse as AI-based defence systems, blockchain-based health records security and global threat data sharing.

CONCLUSION

This study underscores critical vulnerabilities in healthcare, highlighting inconsistency in current practices and lack of resilience to evolving technological risks. This makes threat response capabilities and adoption of next-generation technologies a necessity for the industry. Despite efforts to comply with standards such as HIPAA and GDPR and adhere to cybersecurity frameworks like NIST, the healthcare sector still grapples with serious cyber threats that threaten the privacy of patients and put the delivery of care at unending risk.

This research suggests the combination of a mathematical vulnerability assessment model, machine learning utilities for more informed threat detection, and an adaptive cybersecurity management framework unique to healthcare space, to transition into a future-focused solution that enables healthcare organizations to evolve from reactive protection to proactive resilience.

This model is theoretical today, but it is based on real-world breach incidents and established best practices for cyber risk management. The next phase is to conduct preliminary testing in healthcare settings, and improve it by connecting it to modern technologies, such as blockchain and zero-trust architecture. As industry continues to advance, the approach offers a means to safeguard such sensitive health data, as well as build patient confidence and secure the future of healthcare systems.

Significance of the Research

The results underscore the need to secure patient information and healthcare systems. Closer to the present, the exponential rise in the number and complexity of cyberattacks, especially in the era of the Telehealth in COVID-19 pandemic, further highlights the relevance of this work.

Recommendations for Future Research and Practical Application

- Studies need to consider the adoption of modern technologies like artificial intelligence and blockchain in the context of healthcare cybersecurity.

From an operational perspective, healthcare organizations need to invest in the allocation of resources (staff, training, and systems) to implement a 'continuous training programs' on-going training programs to prevent against insider threats.

REFERENCES

Adam Teoh, A., Binti Abdul Ghani, N., Ahmad, M., Jhanjhi, N., A. Alzain, M., & Masud, M. (2022). Organizational Data Breach: Building conscious care behavior in incident response. *Computer Systems Science and Engineering, 40*(2), 505–515. https://doi.org/10.32604/csse.2022.018468

Aijaz, M., Nazir, M., & Mohammad, M. N. (2023). Threat

modeling and assessment methods in the healthcare-IT system: A critical review and systematic evaluation. *SN Computer Science, 4*(6). https://doi.org/10.1007/s42979-023-02221-1

Al Qartah, A. (2020). *Evolving Ransomware Attacks on Healthcare Providers* (Doctoral dissertation, Utica College).

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*(1). https://doi.org/10.1186/s12911-020-01161-7

Argaw, S., Bempong, N., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC Medical Informatics and Decision Making, 19*. https://doi.org/10.1186/s12911-018-0724-5.

Ariyo, O., & Zheng, J. (2022). A study on security and privacy risks of self-disclosure on social networking sites during COVID-19 pandemic. *2022 IEEE International Conference on Big Data (Big Data)*. https://doi.org/10.1109/bigdata55660.2022.10021102

Atefi, K., Hashim, H., & Khodadadi, T. (2020). A Hybrid Anomaly Classification with Deep Learning (DL) and Binary Algorithms (BA) as Optimizer in the Intrusion Detection System (IDS). *2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA),* 29-34. https://doi.org/10.1109/CSPA48992.2020.9068725.

Bassett, M. S. (2023). *Cybersecurity in the Norwegian healthcare system-A socio-technical case study of Akershus University Hospital* (Master's thesis, NTNU).

Bonafide, C. P., Localio, A. R., Roberts, K. E., Nadkarni, V. M., Weirich, C. M., & Keren, R. (2014). Impact of rapid response system implementation on critical deterioration events in children. *JAMA Pediatrics, 168*(1), 25. https://doi.org/10.1001/jamapediatrics.2013.3266

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., ... & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems, 44,* 1-9. https://doi.org/10.1007/s10916-019-1507-y

Carrasco, M., & Wu, C. (2020). Review: Deep Learning Methods for Cybersecurity and Intrusion Detection Systems. *2020 IEEE Latin-American Conference on Communications (LATINCOM)*, 1-6. https://doi.org/10.1109/LATINCOM50620.2020.9282324.

Carthey, J. (2006). Involving and communicating with patients and the public. *Nursing standard (Royal College of Nursing (Great Britain): 1987), 2017*, 50-3. https://doi.org/10.7748/NS2006.01.20.17.50.C4033.

Clarke, M., & Martin, K. (2023). Managing cybersecurity risk in healthcare settings. *Healthcare Management Forum, 37*(1), 17–20. https://doi.org/10.1177/08404704231195804

Coventry, L., Branley-Bell, D., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A., & Anastasopoulou, K. (2020). Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. *HCI for Cybersecurity, Privacy and Trust*, 105–122. https://doi.org/10.1007/978-3-030-50309-3_8

El Rob, M. A. (2023). A narrative review of Adavntageous Cybersecurity Frameworks and regulations in the United States healthcare system. *Issues In Information Systems*. https://doi.org/10.48009/4_iis_2023_126

Hady, A. A., Ghubaish, A., Salman, T., Unal, D., & Jain, R. (2020). Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access, 8,* 106576–106584. https://doi.org/10.1109/access.2020.3000421

Harkins, M., & Freed, A. M. (2017). The ransomware assault on the healthcare sector. *JL & Cyber Warfare, 6,* 148.

Jiang, J. (Xuefeng), & Bai, G. (2019). Evaluation of causes of protected health information breaches. *JAMA Internal Medicine, 179*(2), 265. https://doi.org/10.1001/jamainternmed.2018.5295

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital Healthcare - cyberattacks in Asian organizations: An analysis of vulnerabilities, risks, NIST Perspectives, and recommendations. *IEEE Access, 10,* 12345–12364. https://doi.org/10.1109/access.2022.3145372

Khan, P., Islam, M. Z., & Hossain, S. (2025). AI-Powered Cybersecurity: Revolutionizing Business Threat Detection and Response. *American Journal of Smart Technology and Solutions, 4*(1), 37–48. https://doi.org/10.54536/ajsts.v4i1.4488

Koppel, R., Smith, S., Blythe, J., & Kothari, V. (2015). Workarounds to computer access in healthcare organizations: you want my password or a dead patient? In *Driving quality in informatics: fulfilling the promise* (pp. 215-220). IOS Press.

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. https://doi.org/10.3390/app8060898

Lamba, J., & Jain, E. (2021). Advanced Cyber Security and Internet of Things for Digital Transformations of the Indian Healthcare Sector. *Handbook of Research on Advancing Cybersecurity for Digital Transformation*. https://doi.org/10.4018/978-1-7998-6975-7.ch017.

Lindner, R. (2022). Cybersecurity Threats to Healthcare Data: Recent Trends and Implications. *Journal of Health Informatics, 9*(3), 87-102.

Manzuik, S., Gold, A., & Gatford, C. (2006). *Chapter 10 – Regulatory Compliance*, 221-241. https://doi.org/10.1016/B978-159749101-3/50014-8.

Mathew, A. (2023). The 5 Cs of Cybersecurity and its Integration with Predictive Analytics. *International*

Journal of Computer Science and Mobile Computing. https://doi.org/10.47760/ijcsmc.2022.v12i01.006.

Minnaar, A., & Herbig, F. J. (2021). Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. Acta Criminologica: *African Journal of Criminology & Victimology, 34*(3), 155-185.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors, 21*(15), 5119. https://doi.org/10.3390/s21155119

Nilsen, W. (2021). *Security Culture in the Norwegian HealthCare Domain* (Master's thesis, NTNU).

Ntantogian, C., Laoudias, C., Honrubia, A. J., Veroni, E., & Xenakis, C. (2021). Cybersecurity threats in the Healthcare Domain and Technical Solutions. *Handbook of Computational Neurodegeneration*, 1–29. https://doi.org/10.1007/978-3-319-75479-6_38-1

O'Brien, N., Grass, E., Martin, G., Durkin, M., Darzi, A., & Ghafur, S. (2020). Developing a globally applicable cybersecurity framework for healthcare: a Delphi consensus study. *BMJ Innovations, 7,* 199 - 207. https://doi.org/10.1136/bmjinnov-2020-000572.

Panattoni, C. T. (2020). *Information security compliance in a healthcare setting: A user behavior pilot study*.

Pappalardo, S., Niemiec, M., Bozhilova, M., Stoianov, N., Dziech, A., & Stiller, B. (2020). Multi-sector Assessment Framework - a New Approach to Analyse Cybersecurity Challenges and Opportunities. , 1-15. https://doi.org/10.1007/978-3-030-59000-0_1.

Patel, R. (2020). *Internet of Things (IoT): Cybersecurity Risks in Healthcare*.

Rajamaki, J., Nevmerzhitskaya, J., & Virag, C. (2018). Cybersecurity education and training in Hospitals: Proactive Resilience Educational Framework (Prosilience EF). *2018 IEEE Global Engineering Education Conference (EDUCON).* https://doi.org/10.1109/educon.2018.8363488

Lu, S., Tang, X., Zhu, Y., & She, J. (2021). A cloud-edge collaborative Intelligent Fault Diagnosis Method based on LSTM-vae hybrid model. *2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud* (EdgeCom). https://doi.org/10.1109/cscloud-edgecom52276.2021.00045

Singh, A., Kumar, A., Akhtar, Z., & Khan, M. (2023). Guest Editorial: Cybersecurity Intelligence in the Healthcare System. *IEEE Transactions on Industrial Informatics, 19,* 809-812. https://doi.org/10.1109/TII.2022.3202828.

Smith, J. (2021). Telemedicine Adoption and Its Implications for Healthcare Cybersecurity: A Case Study. *Journal of Telehealth and e-Health, 27*(5), 378-385.

Tetteh, B. M. (2019). Does HIPAA Provide Enough Protection for Healthcare in the Age of Ransomware and Current Cybersecurity Threats.

The Office of Civil Right (2022); Fall 2022 OCR Cybersecurity Newsletter. HIPAA Security Rule Security Incident Procedures. Health and Human services. https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2022/index.html

Wang, S., Ko, R. K., Bai, G., Dong, N., Choi, T., & Zhang, Y. (2023). Evasion Attack and Defense On Machine Learning Models in Cyber-Physical Systems: A Survey. *IEEE Communications Surveys & Tutorials*. https://doi.org/1 0.1109/COMST.2023.3344808

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health, 4,* 862221. https://doi.org/10.3389/fdgth.2022.862221

Watson, A. (2016). *Impact of the Digital Age on Transforming Healthcare*, 219-233. https://doi.org/10.1007/978-3-319-20765-0_13.

Yeng, P. K., Yang, B., & Snekkenes, E. A. (2019, December). Framework for healthcare security practice analysis, modeling and incentivization. In *2019 IEEE International Conference on Big Data (Big Data)* (pp. 3242-3251). IEEE. https://doi.org/10.1109/BigData47090.2019.9006529

Yeo, L. H. (2023). *Unintentional Insider Threat Assessment Framework: Examining the Human Security Indicators in Healthcare Cybersecurity* (Doctoral dissertation, Eastern Michigan University).

Yusuf, M. K., Danladi, A. J., Shombot, E. S., Dusserre, G., Odey, V. A., Baba-Ahmed, N. B., Bestak, R., & Lawan, M. I. (2024). The Growing Cybersecurity Crisis in Healthcare: A Call to Action. *American Journal of Innovation in Science and Engineering, 3*(3), 55–68. https://doi.org/10.54536/ajise.v3i3.3576