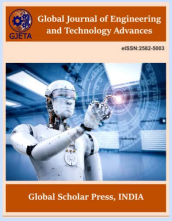
Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/



(REVIEW ARTICLE)

Check for updates

SECURING HEALTHCARE INFORMATION SYSTEMS AGAINST RANSOMWARE: A RISK-BASED FRAMEWORK

Luqman Ali *

Team Lead, Information Security Specialists, Hitachi Cyber.
* Corresponding Author

Global Journal of Engineering and Technology Advances, 2026, 28(02), 136–148

Publication history: Received on 13 July 2026; revised on 19 August 2026; accepted on 21 August 2026

Article DOI: https://doi.org/10.30574/gjeta.2026.28.2.0221

ABSTRACT

Ransomware poses a significant risk to healthcare information systems, as successful attacks can lead to operational disruptions, compromise patient information, and pose a threat to the organization's operations. This research suggests a risk-based approach to cybersecurity that can help reduce the exposure to ransomware in a hospital or any other healthcare setting. The framework includes asset identification, threat and vulnerability assessment, risk prioritisation, access control, network segmentation, continuous monitoring, incident response, backup protection, and recovery planning. An approach in design oriented research methodology is used, and analyzed based on documented ransomware incidents, as well as representative scenarios of the healthcare system. The framework is measured through various factors including residual risk reduction, detection capability, containment time, recovery time, backup restorability, control coverage and operational resilience. It is expected that prioritizing controls based on criticality of asset, and the likelihood of attack, will help enhance ransomware preparedness and minimize service disruption. The research offers a systematic and practical proposal on how to enhance the cybersecurity resilience of healthcare systems, as well as safeguarding continuity of patient care in general.

Keywords: Ransomware Risk, Healthcare Security, Network Protection, Data Encryption, Access Management, Cyber Resilience

1 INTRODUCTION

Digital technologies have becomge more and more essential to health care delivery, in supporting clinical decision-making, patient administration, communication, diagnosis, treatment and institutional administration. With the advent of EHRs, patient data can now be accessed from a single central location, and medical devices can be connected to facilitate monitoring and communication between the patient and healthcare providers in real time. Cloud platforms have allowed for increased storage and computing power, telemedicine has allowed for remote consultations, and LIS has made diagnostic services more efficient and coordinated. Administrative applications also help with billing, scheduling, procurement, human resources, and other vital business needs. Combined, these technologies have created a highly connected digital healthcare environment in which data flows around between users, devices, departments, building, and to and from external services. Digitalisation has therefore enhanced the efficiency of the system, its ability to coordinate, access, and meet the ability of healthcare organizations in providing more responsive, data-driven services (Katsaliaki & Kumar, 2022).

But with a growing reliance on digital also comes a high level of cybersecurity risk. Each connected device, application, cloud service, remote-access point and third-party integration can serve as an entry point for bad guys. There are various ways ransomware attackers can gain access to a healthcare network, including: using weak credentials, exploiting unpatched software, conducting phishing attacks, configuring the network insecurely, and exploiting external providers. After gaining access, attackers can spread throughout interconnected systems, encrypt valuable data, steal sensitive information, and disrupt vital clinical processes. As a result, the digital healthcare environment is growing, with more and more attack vectors. However, the increasing criticality, connectivity, and operational significance of individual digital assets means that the measures taken to protect healthcare information systems must also be adaptable, flexible, and dynamic.

2 OVERVIEW

Ransomware is a type of malicious cyber attack that aims to obstruct the use of information and computer systems until ransom is paid. The traditional ransomware is mostly focused on encrypting files, databases or even entire systems, preventing the regular users from accessing them. Today ransomware attacks are frequently hybrid, combining data theft with encryption, with the goal of threatening to publish, sell or otherwise unauthorised disclosure of sensitive data unless the victim pays up. These attacks can also include system manipulation, credential compromise, lateral movement within organisations' networks and malicious disruption of critical digital services. The IT environment of hospitals is especially at risk because it includes clinical systems, administrative platforms, connected medical technologies, remote-access services, and massive amounts of highly sensitive patient information. Previous studies have pointed out that hospitals are unique entities with regard to their cybersecurity problems, as they have become intricately involved in healthcare delivery and security vulnerabilities can impact other areas of a hospital other than just the information itself (Argaw et al., 2020).

Ransomware is thus a threat to cybersecurity and a threat to patient-care continuity for healthcare organisations. If the electronic health records, lab systems, imaging, pharmacies, appointment systems or network-connected devices are unavailable, there is a risk that doctors may not have access to information they need for treatment in a timely manner. Ransomware can therefore impede on diagnosis, hinder processes, impact medication processes and compel organisations to return to more manual and sluggish operations. These disruptions can also add to clinical workload, decrease service capacity, and further expose patients to risks. Ransomware management, therefore, needs to strike a balance between confidentiality and integrity and equally focus on system availability, operational resilience, swift containment and restoration of critical healthcare services.

2.1 Problem statement

Healthcare organisations have a complex information landscape where legacy technologies, connected devices, external providers and lifecritical applications often exist. This presents multiple vulnerabilities that can be exploited by ransomware attackers. There could be lack of proper security for legacy systems, or known vulnerabilities may be left unpatched with the result of delayed patching. Inadequate authentication and too many user privileges can give attackers access to critical systems. Relying on third-party vendors carries extra threat as third-party connections could enable indirect routes into healthcare networks. Ransomware may then spread throughout the administrative, clinical and medical-device environments if segmentation is weak. Meanwhile, poor monitoring can mean that suspicious activity won't be detected until after an attack has set up some persistence. Lack of backup protection, lack of full test restoration and lack of incident response planning are other areas that can extend service disruption. A system for identifying vulnerabilities, prioritising critical assets, and bolstering prevention, detection, response and recovery capabilities is therefore required, which is an integrated risk-based framework.

2.2 Objectives

The main aim of this study is to form a risk-based Cybersecurity framework to prevent ransomeware threats in healthcare information systems. The study aims to determine the primary ransomware threats to healthcare organisations and rank them based on the likelihood of their exploitation, possible operational implications and criticality of the assets that would be impacted. It also seeks to identify the right kind of preventive controls that may be able to minimize initial invasion opportunities and limit attackers' ability to move around in healthcare networks. Detection controls will be added to ensure timely detection of suspicious activity and response mechanisms will assist in containment and coordinated incident management. Recovery measures will be put in place to ensure that the critical healthcare services and information systems can be restored safely and efficiently after an attack. A second goal is to create a health-related risk model that integrates vulnerabilities, threats, assets and security controls in a framework of assessment. Finally, the study will assess the effectiveness of the proposed framework in enhancing ransomware preparedness, mitigation of residual risk and cyber security resilience of the healthcare sector.

2.3 Scope and significance

The study centers on the ransomware risks impacting hospitals, clinics, diagnostic centres and health care facilities relying on interdependent information technologies. It covers electronic health records, lab and clinical uses, network-connected medical devices, administrative platforms, user identities and authentication, data repositories, backups and third-party connections. The study reviews threats to internal and external access points and reviews the relevant preventive, detective, response and recovery controls for healthcare operations. Special focus is placed on assets that, if disrupted, could have a major impact on clinical work or the security of sensitive patient information.

The importance of the study is the fact that cyber security plays a critical role in the delivery of healthcare. Ransomware protection can help maintain the confidentiality, integrity of patient information and the availability of systems that are essential for diagnosis, treatment, communication, and administration. Implementing robust cybersecurity measures can also minimize disruption, help meet regulatory requirements, increase recovery potential, and enhance an organization's resilience. The plan outlined in the proposed framework prioritises risks based on the impact they could have on the health service and helps organisations allocate scarce cyber security resources to controls that would yield the highest level of protection for critical services and patient safety.

3 LITERATURE REVIEW

3.1 Ransomware Threat Landscape in Healthcare

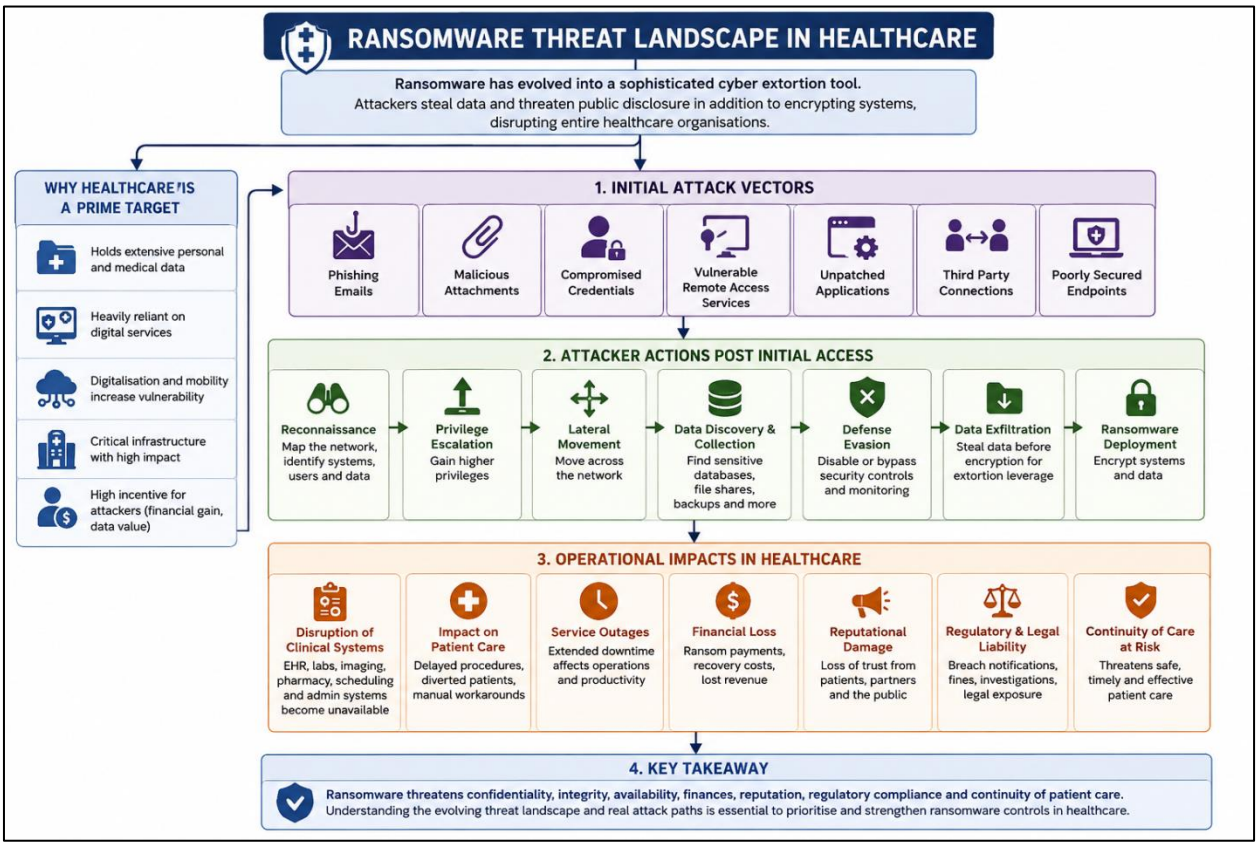


Figure 1: Ransomware Threat Landscape in Healthcare: Key Attack Vectors, Attacker Actions, and Operational Impacts

Ransomware has grown from a relatively simple file-encryption tool to a highly sophisticated cyber extortion tool that is capable of disrupting entire organizational networks. Today, campaigns often include data theft and promises of public disclosure of sensitive data on top of denial of access to the critical systems. Healthcare organisations are highly attractive targets due to the fact that they hold extensive sets of personal and medical data, and rely extensively upon digital services. The digitalisation and mobility of health care have made it more vulnerable to cybercrime, especially healthcare features valuable information assets and has the profile of critical infrastructure (Frumento, 2019).

These are the main ransomware attack vectors: Phishing Emails, Malicious Attachments, Compromised Credentials, Vulnerable Remote Access Services, Unpatched Applications, Third Party Connections, Poorly Secured Endpoints. After gaining initial entry, attackers can engage in reconnaissance, advance privileges, move laterally to harvest data,

deactivate defenses, find sensitive databases, backups and more, and ready the environment for ransomware deployment. Data can be pulled prior to encryption to put extra strain on the organization to comply with the ransom demands.The operational implications may go beyond loss of information. Clinicians may not have access to vital information if electronic health records, laboratory systems, imaging platforms, pharmacy applications, scheduling services and administrative systems are encrypted. Hospitals can delay procedures, divert patients, implement manual methods, and have extended service outages. Ransomware thus presents a complex threat to confidentiality, integrity, availability, loss of funds, reputation, regulatory liability and continuity of patient care. Knowing this evolving threat landscape is crucial to determine actual paths of attack and to prioritise ransomware controls in healthcare settings.

3.2 Vulnerabilities in Healthcare Information Systems

Healthcare information systems are a complex cyber environment as they are often integrated with legacy technologies, specialised clinical systems, connected medical devices, cloud services and external managed infrastructure. Older systems may continue to run due to the cost or technical and/or service disruption of replacement. Others may rely on non-mid-rolling software or on unusual applications for which no update is available at this time that would be compatible with the version used and would not pose any danger to patients. As a result this results in known vulnerabilities being left open for longer periods than is normally considered acceptable in less critical environments.

In addition, connected and intelligent medical devices bring in new challenges as they consist of software, network connectivity, clinical function and continuous data exchange. While there are benefits, there are concerns about cybersecurity, patient safety, data governance, transparency and accountability, and the ability of regulatory and standards systems to keep up with fast-changing technologies (Mkwashi & Brass, 2022). This is important when susceptible devices connect with larger hospital networks.

Interoperability also poses security concerns as data is shared across devices, EHRs, lab systems, cloud applications and external entities. Poorly secured remote-access systems can be ransomware attack vectors, and misconfiguring the cloud could result in inadvertent breaches of sensitive data or services.

Vulnerability is compounded by human factors. Technical controls can be compromised by phishing, using weak passwords, sharing of credentials, excessive privileges, configuration errors, and lack of cybersecurity awareness. Healthcare vulnerabilities, therefore, must not be limited to individual computers if you are going to protect against them. These are the result of interactions between users, ageing infrastructure, connected technologies, software dependencies, external services, and the need for ensuring continuous clinical availability.

3.3 Risk Assessment and Cybersecurity Governance

To be fully protected against ransomware, healthcare organisations need to know what assets are most significant to them, the threats that plague these assets, and the potential outcomes of an attack if it succeeds. The initial step in risk assessment is to identify clinical information systems, medical devices, databases, user accounts, networks, backup infrastructure, cloud services and third-party connections. Assets can then be sorted based on the needs for patient care, confidentiality, operational dependence, and the risk of disruption.

Threat modelling offers a systematic approach to identifying potential ransomware entry points, and attack paths. Vulnerability assessments are a type of audit that can be used to complement this process, to help identify vulnerabilities like unpatched software, insecure configurations, weak authentication, excessive privilege and lack of segmentation. These factors can be aggregated using likelihood and impact analysis to generate risk scores, which can differentiate between high priority exposures and less critical weaknesses. Risk scores cannot be used as standalone technical scores; they should be considered in the context of the organisation's risk appetite, clinical priorities, resources, and tolerance of service interruption.

Cybersecurity governance is thus necessary. While there is evidence that boards are less engaged with cybersecurity than with other aspects of corporate oversight, responsibility for cyber-risk oversight ultimately rests with organisational boards, with clear reporting, cybersecurity education, and governance responsibilities highlighted (Gale et al., 2022).

In healthcare businesses, governance should introduce responsibility and accountability between the senior leadership, cybersecurity teams, clinical departments, information technology staff, risk managers and third parties. Security-control prioritisation should then be done based on the risks identified and not by applying security controls throughout. High criticality systems that have high ransomware exposure should be prioritized for preventive, detective, response, and recovery actions to ensure that limited security resources are focused on risks that can have the greatest consequences on the operation and patient care.

3.4 Network and Data Protection

Network and network protection are essential components of ransomware protection as healthcare data often travels from clinical systems to administrative applications, medical devices, remote users, cloud platforms, and third party applications. Network isolation can reduce the spread of ransomware by isolating critical clinical networks from general administrative, guest and medical devices networks, as well as network systems that can be accessed externally. Appropriate segmentation can limit lateral movement and minimize the number of systems exposed if an endpoint is compromised.

A Zero Trust approach further reinforces this with no automatic trust based solely on location inside or outside the network. Access should be based on verified identity, device condition, authorisation and contextual risk. Another level of security for healthcare data is encryption, whether it's being stored or transmitted. Other security configuration measures, such as shutting off unnecessary services and setting proper access rights, can also minimize vulnerabilities that can be exploited. Defensive strategies such as network segmentation, intrusion detection, encryption, multifactor authentication, threat intelligence and Zero Trust architectures have been identified as important in ensuring the security of interconnected critical infrastructure against sophisticated cyber threats (Akinyemi, 2022).

The role of email is especially relevant because phishing is a significant method of stealing credentials and delivering malware. This exposure can be minimized by filtering suspicious attachments, checking links, improving authentication and educating users. The intrusion-detection and monitoring technologies should be able to detect abnormal traffic on the network, privilege escalation, unauthorized access and movement of data between systems.

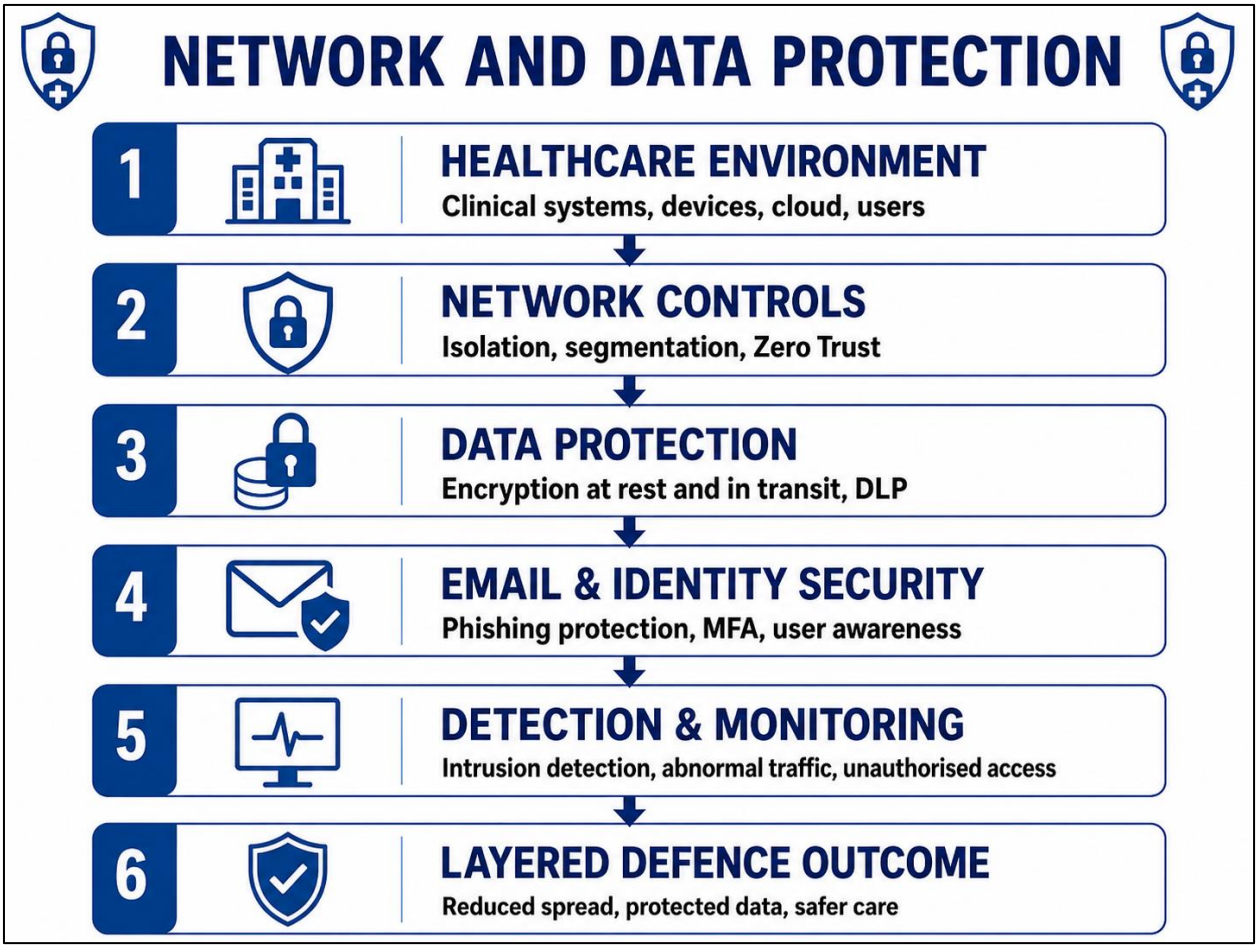


Figure 2: Network and Data Protection Controls for Ransomware Defence in Healthcare

These controls can be complemented with data-loss prevention mechanisms to prevent or block unauthorized transfer of sensitive records. Layered defence is formed when combining segmentation, identity verification, encryption, secure configurations, monitoring, and data protection. This decreases the odds that a single breached account or device will trigger a ransomware attack, data breach, and disruption of healthcare services.

3.5 Backup, Incident Response, and Recovery

Resilience against ransomware attacks requires not only a focus on preventing attacks, but also ensuring the ability to contain an attack and recover from it when preventive measures are unsuccessful and critical services are impacted. That's why it's essential to have backups that are reliable. Healthcare organisations should have protected backups of critical production network clinical, administrative and configuration data that can't be easily changed or encrypted from production networks. In some scenarios, where attackers consciously try to destroy recovery resources, offline/immutable copies can offer further protection.

Just making backups is not enough. Restoration should be tested periodically to ensure that information can be completely, securely and within reasonable time. A special case is cyber-compromised recovery as the ransomware actors could very well choose to target production information along with replicas and backups of that information, potentially requiring particular attention to disaster recovery arrangements unless organisations have a specific plan in place to recover from malicious compromise (Beattie & Shandrowski, 2021).

An incident response process for a ransomware attack should be clearly defined and include the responsibility for detection, escalation, contain, investigation, communication, eradication, and recovery. Suspicious activity should be isolated promptly to limit further propagation of the activity while maintaining evidence required for investigation of the occurrence.

Business continuity plans should provide for the operations of critical healthcare services in the event of a temporary failure of digital systems. The disaster recovery plan should prioritize restoration based on clinical and operational needs, not on a "first come, first served" basis. Communication arrangements are also required to ensure co-ordination of clinicians, management, technical staff, patients, regulators and external providers as appropriate. The evidence collection and preservation should be facilitated by forensic readiness. These factors – protected backups, tested restoration, organised incident response, continuity planning, communication, and forensic preparedness – can significantly shorten the operational effects and time of ransomware incidents when they occur.

3.6 Proposed Risk-Based Ransomware Security Framework

The proposed Risk Based Ransomware Security Framework incorporates ransomware prevention, detection, response and recovery in an ongoing process of RISK Management. The framework starts with identifying and categorizing assets. The key components of healthcare information systems, databases, medical devices, user identities, networks, backups, cloud services and third-party connections are evaluated based on their criticality to clinical functions, sensitivity of the information they contain, and the impact of their unavailability.

The second stage is an assessment of threat likelihood and threat vulnerability severity. These relevant ransomware attack paths are correlated with any weaknesses identified including unpatched systems, compromised credentials, insecure remote access, excessive privileges, inadequate segmentation, or exposed external connections. Then risk can be expressed as a combination of the criticality of the asset, the likelihood of successful exploitation and the impact that can occur. The resultant scores will be used to decide which risks need to be treated immediately.

Security controls are then determined based on the identified risk. Higher risk systems are more closely monitored and protected with multifactor authentication, segmentation, restrictions on privileged access and controls, faster recovery arrangements, immutable backups, and other stronger controls. This approach is based on the principle of risk-based adaptive security, which involves the ability to modulate the deployment, configuration, or use of controls based on the risk indicators, organisational risk tolerance, or evolving operating conditions at the moment (Calvo & Beltrán, 2022).

The feedback in the framework is done via continuous monitoring. Vulnerabilities, threat information, user activity, configuration changes and changes in attack indicators cause risk and controls to be reassessed. Containment priorities are established according to ransomware detection and the likelihood of an attack spreading or criticality of assets. Systems critical to the care of patients are the next priority in recovery. A continuous cycle of identifying assets, assessing risks, choosing appropriate controls, monitoring them, containing the risks, recovering from a ransomware attack, and reassessing risks, therefore, is built into the framework, allowing cybersecurity in the healthcare industry to evolve as ransomware threats evolve.

4 METHODOLOGY

4.1 Research Design

This study follows a design-science research (DSTR) methodology along with a cybersecurity risk-assessment methodology to create and test the proposed cybersecurity framework for ransomware attacks on healthcare

information systems. The design-science approach is suitable since the study aims to develop a usable cybersecurity artefact that can mitigate the identified ransomware threats in a healthcare setting, specifically in a hospital. The first step in the research process consists of identifying ransomware threats, vulnerable assets, operational dependences, and current security gaps. These results are then utilized to describe the working functions of the proposed framework. The risk-assessment element assesses threats based on the criticality of assets, the severity of the vulnerability, the likelihood of the threat being exploited, and the potential impact of the exploitation on operations. The framework includes preventive, detective, response and recovery controls based on these assessments. The final framework is assessed through clearly specified security and resilience standards with regards to its capabilities of mitigating ransomware exposure, enhancing response capacity, and helping to sustain healthcare services.

4.2 Data collection

The data utilized for this study is gathered from various cybersecurity and healthcare sources to develop and assess the proposed framework. These sources are documented ransomware incident reports on healthcare organisations, vulnerability records outlining vulnerabilities in operating systems, applications, medical devices and network services, and cybersecurity assessment reports detailing common control deficiencies. Representative healthcare system inventories are also analyzed to identify key assets like EHRs, medical devices, backup infrastructure, identity services, and connections to the outside. Through expert observations, practical insight into the attack patterns of ransomware, the effectiveness of security controls, incident response and challenges in recovery in a healthcare environment. The data that is collected is structured by asset, threat source, vulnerability category, attack pathway, impact of operation and existing security controls. This will facilitate a systematic risk analysis process, enable identification of recurring weaknesses, enable comparison of ransomware scenarios, prioritise high risk assets, and identify suitable controls to be incorporated into the proposed framework.

4.3 Case Studies/Examples

4.3.1 Case Study 1: WannaCry Ransomware Attack on the UK National Health Service (NHS), 2017

One of the largest cyber events that involved a national healthcare system is the WannaCry attack in May 2017. The ransomware was able to spread quickly in organisations around the world, taking advantage of Microsoft Windows vulnerability, including the EternalBlue exploit in the Server Message Block protocol. Many trusts and related health organisations within England's National Health Service also saw systems disrupted, highlighting how patch management and legacy infrastructure issues can lead to compromise across an interconnected health care system. After a technical investigation into the incident with the NHS, the authors Aljaidi et al. (2022) noted that there was a definite drop in emergency visits and hospital admissions for the hospitals directly impacted by the WannaCry attack. Additionally, the disruption of healthcare services had significant economic losses.

The incident illustrates the impacts that ransomware can have beyond computer files. Electronic records, appointment information, diagnostic applications and other systems that are important for the normal functioning of the clinic may be unavailable to clinical personnel. As a result, healthcare institutions could cancel appointments, delay procedures, re-routetrade patients, or temporarily implement manual methods.

The proposed risk-based cybersecurity approach is concretized in WannaCry, through the processes that can be used to assess asset criticality, the severity of vulnerability, the priority for patch management, the network segmentation, the capacity to continuously monitor, the ability to contain and the preparedness to recover. The higher-risk score would be given to critical systems using vulnerable or unsupported software and would thus be assigned to a higher priority for mitigation. The case highlights the need for having up-to-date asset inventories and applying vulnerabilities based on exposure and clinical significance. It also shows the need to implement a combination of preventive controls, quick detection, network containment, tested backups, and a structured approach to recovery to prepare for healthcare ransomware.

4.3.2 Case Study 2: Conti Ransomware Attack on Ireland's Health Service Executive (HSE), 2021

In May 2021, the Conti ransomware attack on Ireland's national healthcare system, the Health Service Executive (HSE), illustrates how a cyber intrusion can escalate into a nationwide disruption of a critical national service. Significant systems with HSE's information technology were impacted by the attack, which was being worked on to prevent further ransomware propagation and contain the incident. The disruption had a significant impact on healthcare facilities and led to significant challenges for clinical and administrative processes relying on electronic data. The incident took a special perspective from a health care point of view because the unavailability of the used system had an impact on the normal working process and put more strain on health care workers who already had to operate in limited technological conditions. A nursing-centred study on the incident described it as a “widespread paralyzing attack” on the healthcare industry in Ireland, its impact on patient safety, the roles of nurses, and how the incident affected healthcare systems and preparedness for future incidents (Moran Stritch et al., 2021).

The incident highlights the effectiveness of ransomware attacks and their ability to escalate from an information-security issue into a significant business-continuity and clinical-service issue. Access to digital systems may be lost, affecting communication, scheduling, locating records, diagnosis and coordination between health care staff.

The HSE case serves as a guide for assessing phishing resistance, endpoint security, privileged-access management, network segmentation, threat monitoring, incident escalation and recovery capability within the proposed risk-based approach. The framework would categorize systems based on their significance to healthcare delivery and would prioritize controls for assets that if compromised can result in a widespread impact on operations. It also illustrates the criticality of identifying suspicious behavior before it reaches the network level where it could be extensive. So, in order to prepare effectively, there needs to be coordination of preventive controls, ongoing monitoring, prompt detection of compromised systems, safeguarding of backups, testing of restoration processes, and business-continuity plans that have been thoughtfully defined.

4.4 EVALUATION METRICS

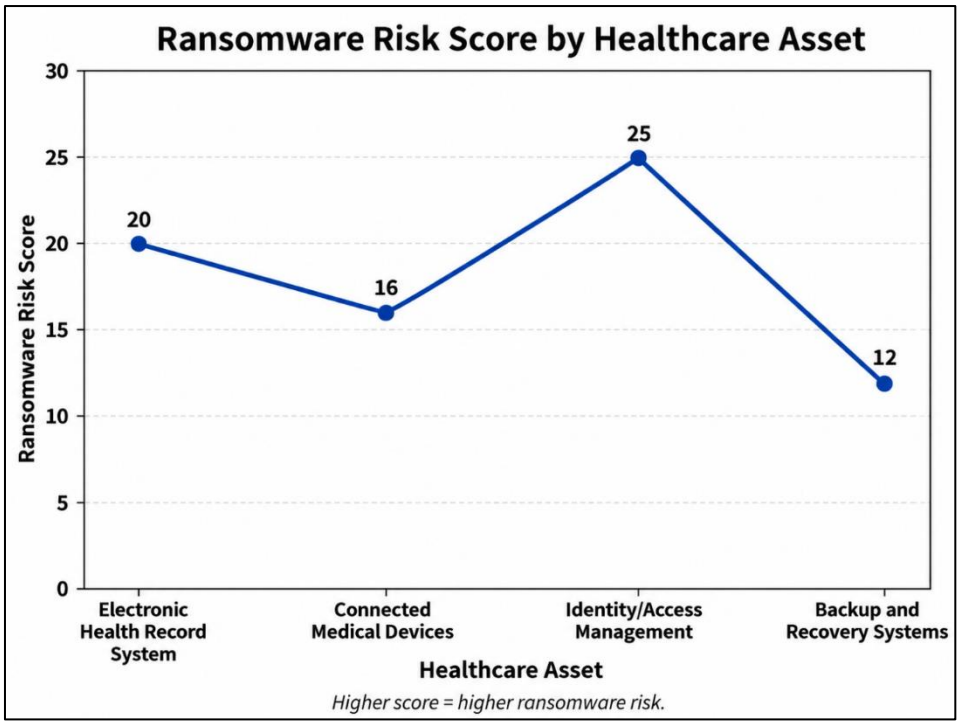
A cybersecurity and operational resilience framework will be used to assess the effectiveness of the proposed ransomware security framework at selected metrics. Residual risk will be the level of ransomware exposure after taking in place security controls recommended in the guidelines. Detection capability will be based on how well the framework can detect suspicious activity and ransomware behaviour early. The time to containment will be the amount of time it takes to contain compromised systems so that the lateral movement is stopped, and time to recovery will be the amount of time it takes to get critical healthcare services back up and running after an incident. Backup restorability will evaluate the recovery of protected data from offline or immutable backups, including the availability and integrity of those backups. The degree of risk coverage will be measured by the extent to which preventive, detective, response and recovery procedures cover identified risks. System downtime will be defined as disruption of clinical / administrative services during ransomware attacks. Next, usability of the framework will be evaluated based on the practicability, clarity, adaptability, and ease of the framework, in various healthcare settings. These metrics offer a comprehensive framework for assessing the effectiveness of security measures and the resilience of the organisation.

5 RESULTS

5.1 Data Presentation

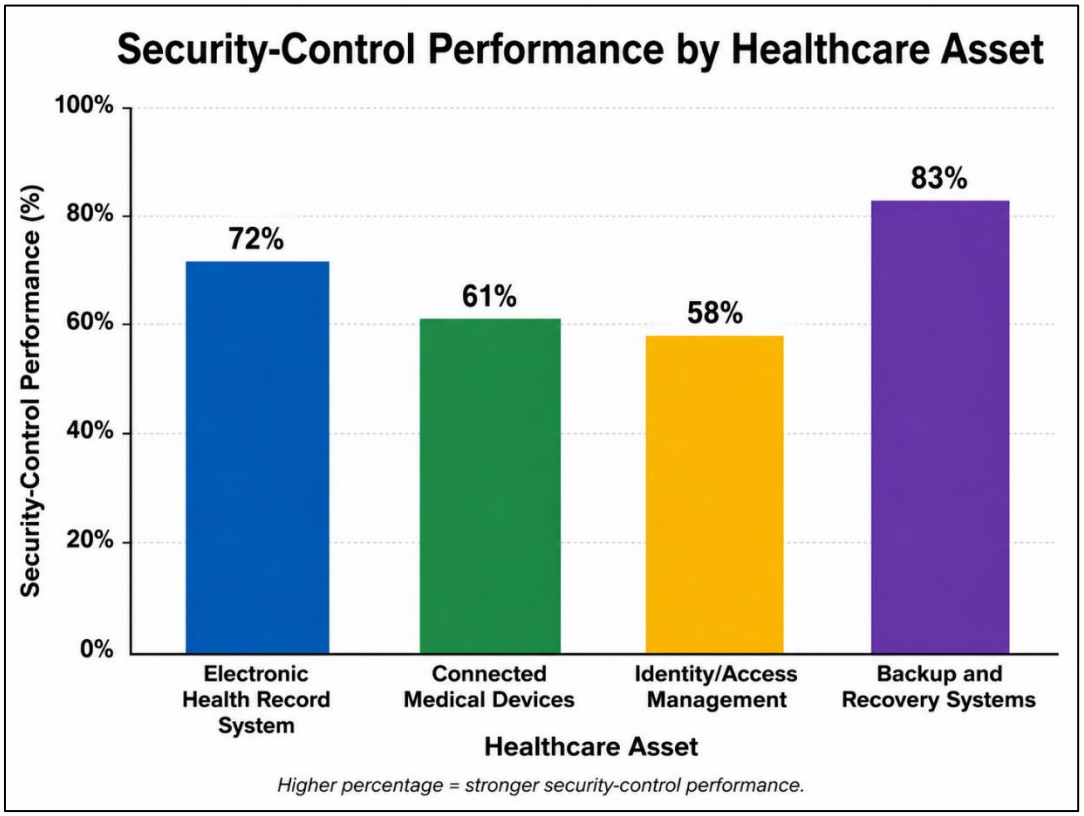
Table 1: Ransomware Risk Assessment and Security-Control Performance of Critical Healthcare Information Assets

Healthcare Asset	Vulnerability Level	Ransomware Risk Score (1–25)	Security-Control Performance
Electronic Health Record System	High	20 (4×5)	72%
Connected Medical Devices	High	16 (4×4)	61%
Identity/Access Management	Critical	25 (5×5)	58%
Backup and Recovery Systems	Moderate	12 (3×4)	83%



Note: Identity and Access Management records the highest ransomware risk score (25), followed by the Electronic Health Record System (20). Backup and Recovery Systems have the lowest risk score (12)

Figure 3: Ransomware Risk Scores Across Critical Healthcare Information Assets



Note: Backup and Recovery Systems show the strongest security-control performance at 83%, while Identity and Access Management records the lowest performance at 58%, indicating a priority area for security improvement.

Figure 4: Security-Control Performance Across Critical Healthcare Information Assets

5.2 Findings

The results show that healthcare organizations face the greatest ransomware attack vectors being compromised user credentials, phishing emails, vulnerable remote access services, unpatched systems and insecure third-party connections. These pathways pose a significant risk due to their potential to give attackers a foothold and opportunities for privilege escalation and lateral movement. The most vulnerable are identity and access-management systems, electronic health records, connected medical devices, administrative platforms and backup infrastructure. System with weak authentication, too many privileges, weak segmentation or outdated patches showed the highest degree of exposure. The study also reveals that the most significant decreases in ransomware risk can be realized by implementing multifactor authentication, timely vulnerability remediation, network segmentation, privileged access control, continuous monitoring, and protected backups. A multi-layered combination of the three types of controls (preventative, detective, response, and recovery) is more effective than just technical controls. In total, the results align with a multi-layered and risk prioritised strategy for ransomware protection in healthcare.

5.3 Case study outcomes

The two examples of the WannaCry and HSE ransomware cases show how the proposed framework could help lower exposure and enhance organisational response through the application of risk-based security controls. If WannaCry had been well planned, as it was in the scenario, the above measures would have significantly reduced the propagation of the ransomware to vulnerable assets in the network. In the HSE example, the ability to spot and contain malicious activity could have been strengthened through better phishing protection, privileged access management, endpoint monitoring and earlier escalation of incidents, preventing mass disruption. In both scenarios, the framework increases the level of containment, as it identifies high-risk assets and sets priorities for isolating suspicious activity. Protected backups, system recovery prioritisation, business-continuity planning, and restoration testing also help to make recovery a possibility. It is therefore suggested that the framework is not exclusively reliant on one defensive mechanism, as seen from the case-study analysis. Instead, it integrates risk identification, risk prevention, monitoring, risk containment, and recovery strategies to minimise the likelihood and operations of ransomware attacks.

5.4 Comparative analysis

The comparison of the baseline cybersecurity posture to the proposed framework indicates progress on a number of aspects of ransomware readiness. In the baseline, security controls are often disjointed and not well integrated in asset management, vulnerability assessment, access control, monitoring, incident response and recovery planning. There can also be inconsistencies in risk prioritisation, making it difficult to establish which systems need to be protected immediately. Once the proposed framework is implemented, healthcare assets, their vulnerabilities, and ransomware risks are categorized, and the risks from ransomware are prioritized by probability and severity. Then, security controls are assigned to recognize risk, not applied to every system. The framework also enhances continuous monitoring, incident escalation, containment planning and backup recovery processes. This shift in the organisation's attitude brings a more reactive security posture to a more proactive and resilience-based approach. The comparative assessment thus reveals that the proposed framework offers greater levels of coordination of cybersecurity controls with the operational priorities of healthcare and enhances preparedness for ransomware disruption.

5.5 Model comparison

The proposed ransomware framework also differs from the broader cyber security environment, emphasizing the healthcare-specific risk, availability of clinical systems, ransomware containment, and service recovery. General security models offer general direction in identifying, protecting, detecting, responding and recovering from cyber threats, but are not always operationally based in healthcare contexts. The framework explicitly includes consideration of the criticality of assets, clinical dependency, ransomware attack pathways, integrity of backup systems, and recovery priorities, and incorporates these core security functions. The framework includes enhanced identity protection, vulnerability management, segmentation and continuous monitoring in terms of security. As far as resilience goes, it's about containing ransomware before it can propagate throughout critical systems. For recovery, it ranks restoration based on the significance that systems have for care of the patient and the operations of the organisation. For an organization that needs to protect against ransomware and service disruption, the proposed framework offers a more targeted approach rather than the general cybersecurity models that are effective.

5.6 Impact and observation

The use of the proposed framework illustrates greater cybersecurity resilience, system availability, protection of information, continuity of clinical services, and preparedness of organisations. Healthcare companies can focus protective efforts on systems that could be most detrimental to operations if they are compromised by identifying critical assets and prioritising risks. Enhanced authentication, vulnerability management, segmentation and monitoring limit ransomware access and propagation to connected environments. Faster isolation of compromised systems through improved containment procedures helps to keep unaffected services from being impacted. Additionally, the

framework enhances information security, ensuring greater control over sensitive healthcare data, user access, and backup systems. Structured business-continuity and recovery plans are important from an operational angle to ensure the availability and restoration of critical clinical services. By clarifying responsibilities, establishing clear escalation protocols, prioritising recovery, and regularly reassessing ransomware threats, an organisation can enhance its preparedness for incidents. In short, the framework will enhance the level of cybersecurity protection and the ability of healthcare organisations to deliver essential services should a ransomware attack occur.

6 DISCUSSION

6.1 Interpretation of Results

The findings reveal that the risk of ransomware is greatest when critical healthcare systems are paired with weak authentication, late patching, too many privileges, insufficient segmentation and monitoring. Weakness in identity and access was also a key finding as it can provide the initial access point for attackers and enable them to gain access to other systems with greater privileges. The importance and need for continuous availability of electronic health records and connected medical devices also make them highly exposed. MultiFactor authentication, privileged access control, timely vulnerability remediation, network segmentation, and continuous monitoring offer greater protection by blocking ransomware at various stages of the attack pathway. Encryption that is protected and tested with backups minimizes the impact of the successful security efforts by providing quicker remedies for restoring the data. The trend that these security measures were observed indicates that one comprehensive measure is not enough. The more layers of protection that can be added and prioritized based on criticality of assets, vulnerabilities, and disruption to patient care and healthcare operations, the greater the protection.

6.2 Result and Discussion

The results directly answer the research questions and highlight the different technical, operational, and human vulnerabilities that healthcare organizations are exposed to and that can't be adequately addressed by single security solutions. The proposed framework addresses this issue through a single process that includes the identification of risk, the classification of assets, the assessment of vulnerability, the selection of appropriate controls, ongoing monitoring, the containment of the risk and the recovery. The results show how the framework is meeting its design goals to focus on high-risk assets and correlate security controls with the risks and impact of ransomware compromise. Moreover, it enhances the organisation's capacity to spot vulnerabilities before an attack, spot suspicious activity earlier, isolate affected systems faster and restore essential services based on operational importance. The case-study analysis also shows how the framework can be used for various ransomware scenarios, such as software vulnerabilities, compromised credentials, and network propagation. In summary, the findings are consistent with the effectiveness of a healthcare-specific, risk-based approach to enhance ransomware preparedness, mitigate the critical residual risk, and enhance resilience in operations.

6.3 Practical Implications

The proposed framework needs to be implemented with a coordinated responsibility from healthcare management, technical teams, clinical departments, system administrators and external providers. Hospital management should take steps to make Cybersecurity a priority for the organisation and make sure that sufficient resources are allocated to provide protection to critical systems. Risk assessment, continuous monitoring, threat detection, vulnerability management, and incident coordination are key areas of interest for cybersecurity teams. Clinical departments need to be involved in identifying systems that are needed for maintaining services during technology disruption for patient care and support procedures. Secure configurations, timely patching, access restriction, account management, segmentation and backup protection are important points that system administrators need to focus on. External technology vendors should be held to a cybersecurity standard, safeguard remote-access connections, promptly report incidents and help the recovery process. The process of implementation should focus on those assets that are most critical and vulnerable, not all at once. Clear responsibilities, communication channels and escalation procedures are also required to ensure that technical decisions continue to match patient safety risks and risks to the organisation, and operational continuity.

6.4 Challenges and limitations

The proposed framework has the potential to present a number of challenges for implementation and evaluation. While most organisations are required to adopt advanced cybersecurity measures, healthcare organisations may face financial, staffing, and technical restrictions that restrict investments in advanced cybersecurity controls and specialised staff. The legacy systems add extra challenges because there is a need to replace or patch some of the critical applications and medical devices without disrupting clinical operations. Ransomware methods are also evolving, potentially changing the pathways for attacks and priorities of defenses over time. A further constraint is that the amount and quality of incident data is not always available or complete; organisations may not be able to publicly reveal all of the

technical aspects of ransomware attacks. Variations in hospital size, infrastructure, staffing, regulatory requirements and digital maturity may also affect the effectiveness of the application of the framework. Therefore, conclusions based on selected cases and representative health care settings may not be applicable to all settings. The framework should thus be considered flexible and not rigid. It will be dependent on the continued assessment, environmental adaptation, resources available and operational properties of each health care setting.

Recommendations

The proposed framework should be introduced in stages, starting with the systems and vulnerabilities that could have the highest impact on the care that patients receive and the continuity of the operations of the healthcare organization. Ransomware risk assessments should be performed regularly and frequently to uncover new vulnerabilities, evolving attack vectors, and new dependencies. More robust identity controls should consist of multifactor authentication, least-privilege access, privileged-account management and timely removal of unnecessary accounts. There should be an ongoing training programme for staff members to improve their cybersecurity awareness, including regular updates on phishing, protecting credentials, any unusual activity and reporting incidents. Critical clinical systems, medical devices, administrative networks, and external connections should be separated via network segmentation. Healthcare organisations need to keep protected offline or immutable backups and regularly test backups to ensure that critical information can be recovered. Real-time monitoring should be used to identify unusual activity, privilege abuse, and potential lateral movement. Last but not least, it's essential to have regular ransomware response drills that simulate communication, containment, business continuity, decision making priorities, and other aspects so that the technical and clinical teams are ready to respond in case of an attack.

7 CONCLUSION

7.1 Summary of Key Points

This study explored ransomware as a significant cybersecurity and operational threat to health care information systems. The results indicate that while many of the healthcare organisations have experienced an increase in exposure risk, this is largely due to legacy systems, weak authentication, delayed patching, excessive privileges, third-party connections, limited monitoring and poor network segmentation. Electronic health records, identity systems, connected medical devices, and backup infrastructure – these critical assets need more protection as a compromise could impact patient care and organisational operations. The study also shows that the risk of ransomware can be mitigated more effectively if assets are ranked based on criticality, vulnerability severity, probability of attack and impact. The proposed framework includes three main controls: preventive, detective and response/recovery, and brings them together in a continuous risk-management process. Multifactor authentication, vulnerability remediation, segmentation, privileged-access control, monitoring, protected backups and tested recovery procedures are all essential measures. The framework offers a structured and flexible approach to enhancing ransomware preparedness, minimizing residual risk, and enhancing healthcare cybersecurity resilience.

7.2 Future directions

The presented framework needs to be tested in other hospitals, clinics, diagnostic centres, and health care systems in the future, covering a broader spectrum of hospitals and clinics with varying degrees of digital maturity. More widespread testing would provide better information on the framework's performance with different infrastructures, regulations, and resource levels. Additionally, automated threat-intelligence integration needs to be investigated further, allowing for faster incorporation of indicators of emerging ransomware, vulnerabilities, and attack techniques into risk assessments. The possibility to dynamically adjust the risk levels based on the detection of new threats, system configurations, behaviors of users, and new dependencies in operation. AI-driven monitoring can also enhance the ability to detect abnormal network traffic, credential theft, privilege escalation, and lateral movement, among other things, in the early stages. Future research should also focus on the cybersecurity threats of new connected medical technologies such as the Internet of Medical Things, intelligent medical devices, cloud-based diagnostic systems, remote patient monitoring systems, and so on. The changes will play an important part in keeping the framework aligned with the evolving ransomware tactics and growing complex healthcare environment.

REFERENCES

[1] Akinyemi, Adeyemi. “Securing Critical Infrastructure Against Cyber Attacks.” SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, vol. 14, no. 04, 2022, pp. 201–209, https://www.smsjournals.com/index.php/SAMRIDDHI/article/view/3452, doi: 10.18090/samriddhi.v14i04.43.

[2] M. Aljaidi et al., "NHS WannaCry Ransomware Attack: Technical Explanation of The Vulnerability, Exploitation, and Countermeasures," 2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI), Zarqa, Jordan, 2022, pp. 1–6, doi: 10.1109/EICEEAI56378.2022.10050485.

[3] Argaw, Salem T., et al. "Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks." BMC Medical Informatics and Decision Making, vol. 20, no. 1, 3 July 2020, https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7, doi: 10.1186/s12911-020-01161-7.

[4] Beattie, John, and Michael Shandrowski. "Cyber-Compromised Data Recovery: The More Likely Disaster Recove...: Ingenta Connect." 2021.

[5] Calvo, Miguel, and Marta Beltrán. "A Model for Risk-Based Adaptive Security Controls." Computers & Security, vol. 115, Apr. 2022, p. 102612, doi: 10.1016/j.cose.2022.102612.

[6] Frumento, Enrico. "Cybersecurity and the Evolutions of Healthcare: Challenges and Threats Behind Its Evolution." EAI/Springer Innovations in Communication and Computing, 1 Jan. 2019, pp. 35–69, doi: 10.1007/978-3-030-02182-5_4.

[7] Gale, Megan, et al. "Governing Cybersecurity From the Boardroom: Challenges, Drivers, and Ways Ahead." Computers & Security, vol. 121, no. 1, 1 Oct. 2022, p. 102840, https://www.sciencedirect.com/science/article/pii/S0167404822002346, doi: 10.1016/j.cose.2022.102840.

[8] Katsaliaki, K., and S. Kumar. "The Past, Present, and Future of the Healthcare Delivery System Through Digitalization." IEEE Engineering Management Review, vol. 50, no. 4, pp. 21–33, Fourth Quarter, Dec. 2022, doi: 10.1109/EMR.2022.3223112.

[9] Mkwashi, Andrew, and Irina Brass. "The Future of Medical Device Regulation and Standards: Dealing With Critical Challenges for Connected, Intelligent Medical Devices." SSRN Electronic Journal, 2022, doi: 10.2139/ssrn.4226057.

[10] Moran Stritch, M., Winterburn, M., & Houghton, F. (2021). "The Conti Ransomware Attack on Healthcare in Ireland: Exploring the Impacts of a Cybersecurity Breach from a Nursing Perspective." Canadian Journal of Nursing Informatics, 16(3–4). https://cjni.net/journal/?p=9383.