**Enhancing Data Resilience in Cloud-Based Electronics Health Records Through Ransomware Mitigation Strategies Using NIST and MITRE ATT&CK** **Frameworks**

**Abstract**

*The increasing adoption of cloud-based Electronic Health Records (EHRs) has transformed healthcare by enhancing data accessibility, interoperability, and patient care efficiency. However, this transition has also introduced new cybersecurity vulnerabilities, with ransomware emerging as a critical threat to healthcare systems. Ransomware attacks disrupt medical services, compromise patient confidentiality, and impose significant financial burdens on institutions. This study comprehensively examines ransomware threats in cloud-based EHR environments by analyzing vulnerabilities, attack vectors, and mitigation strategies through the NIST Cybersecurity Framework and MITRE ATT&CK Framework. A quantitative analysis was conducted using datasets from the U.S. Department of Health and Human Services (HHS), the Cybersecurity & Infrastructure Security Agency (CISA), and the MITRE ATT&CK database. Key findings indicate a 67% increase in ransomware incidents from 2018 to 2023, with credential theft (33.3%) and phishing (26.7%) as the most exploited attack vectors. Recovery challenges were exacerbated by backup failures (hazard ratio = 0.000, p = 0.127) and third-party risks (hazard ratio = 0.000, p = 0.030). To mitigate these risks, the study advocates for a multi-layered cybersecurity approach, emphasizing Zero Trust Architecture, AI-driven threat detection, immutable backups, and vendor risk management. The findings underscore the need for collaboration among healthcare institutions, cybersecurity professionals, and policymakers to strengthen resilience against evolving ransomware threats. By integrating structured cybersecurity frameworks and proactive defense mechanisms, healthcare organizations can enhance data security, ensure compliance, and minimize operational disruptions.*

**Keywords: Ransomware, Electronic Health Records, Cybersecurity, NIST Framework, MITRE ATT&CK.**

**1. Introduction**

The increasing digitization of healthcare has significantly improved data accessibility and operational efficiency, with cloud-based Electronic Health Records (EHRs) serving as a fundamental component of modern healthcare infrastructure. However, this transformation has also heightened the vulnerability of healthcare systems to cyber threats, particularly ransomware attacks. Sharma et al. (2024) posits that given the sensitive nature of patient data and the necessity of uninterrupted healthcare services, ransomware incidents pose severe risks to data integrity, patient safety, and institutional financial stability. To mitigate these threats, structured cybersecurity frameworks such as the NIST Cybersecurity Framework and the MITRE ATT&CK Framework have been advocated to strengthen organizational defenses (Yeboah-Ofori & Opoku-Boateng, 2023).

The frequency and sophistication of ransomware attacks in healthcare have escalated considerably. Sharma (2024) avers that in 2024, 67% of healthcare organizations reported ransomware incidents, many of which resulted in system outages and patient care disruptions. Attackers exploit vulnerabilities in cloud infrastructures, third-party service providers, and outdated security protocols, employing double extortion tactics—encrypting and exfiltrating data to coerce ransom payments (Riggs et al., 2023). The financial implications of these attacks are severe, with recovery costs averaging $2.57 million per incident and 53% of affected organizations admitting to paying ransoms, with payments averaging $4.4 million (Hinton, 2024).

Several high-profile ransomware attacks illustrate the severity of these threats. Özeren (2025) reports that in February 2024, the ALPHV/BlackCat ransomware group targeted Change Healthcare, disrupting medical claims processing for over 100 million patients and forcing UnitedHealth Group to pay approximately $22 million in ransom. Similarly, in June 2024, Ascension Health System experienced a ransomware attack that disabled access to cloud-based EHRs, leading to delays in medical appointments and prescription processing (Alder, 2024). That same month, Synnovis Pathology Services in the United Kingdom fell victim to the Qilin ransomware group, resulting in the cancellation of over 1,100 elective procedures and 2,100 outpatient appointments, illustrating the direct impact of ransomware on patient care (Uberoi, 2022). Furthermore, the MediSecure breach in Australia compromised the personal health data of 12.9 million individuals, underscoring the risks associated with third-party service providers (Lavoipierre, 2024).

These incidents reflect a broader global trend. BBC (2021) notes that in 2021, Ireland’s Health Service Executive was attacked by the Conti ransomware group, using the Cobalt Strike tool, causing widespread service disruptions. Similarly, the 2022 attack on Costa Rica’s Social Security Fund by the Hive Ransomware Group disrupted critical healthcare systems (Zerbe, 2023). In the United Kingdom, Cyber Management Alliance (2024) asserts that the 2022 ransomware attack on Advanced Computer Software Group, a major NHS supplier, resulted in a £6 million provisional fine, highlighting the regulatory and financial consequences of insufficient cybersecurity measures. More recently, in 2023, Children’s Hospital Los Angeles suffered a ransomware attack that forced a temporary return to paper-based systems, demonstrating the potential for severe operational disruptions in critical healthcare services (Eaton-Robb, 2023).

Statistical analyses underscore the urgency of ransomware mitigation. Alder (2025) states that between 2018 and 2023, hacking-related data breaches in healthcare increased by 239%, with 79.7% of all healthcare breaches in 2023 attributed to hacking incidents. The global incidence of ransomware attacks in healthcare nearly doubled in 2023, reflecting the growing severity of cyber threats. The Director of National Intelligence (DNI) reported a 128% increase in ransomware attacks targeting the U.S. healthcare sector in 2023, while as of December 2024, 677 major health data breaches had been recorded, affecting over 182.4 million individuals (CTIIC, 2024). Additionally, Riggi (2024) highlights that attacks on third-party service providers surged by 287% between 2022 and 2023, exacerbating cybersecurity risks in interconnected healthcare systems.

The widespread adoption of cloud-based EHRs has further expanded the attack surface, necessitating improved cybersecurity strategies. Innowise (2024) reports that by 2023, 81% of healthcare organizations had integrated cloud-based solutions, a trend expected to continue as the North American EHR market is projected to reach $17.34 billion by 2030. However, this transition has introduced new vulnerabilities, with compromised credentials and exploited system weaknesses accounting for 34% of ransomware incidents (Innowise, 2024). A particularly concerning issue is the targeting of backup systems, with 95% of ransomware attacks attempting to compromise backups, and 66% succeeding, significantly hindering recovery efforts (Cook, 2017).

To address these threats, structured cybersecurity frameworks provide essential risk mitigation strategies. NIST (2018) asserts that the NIST Cybersecurity Framework, which consists of five core functions—Identify, Protect, Detect, Respond, and Recover, enables organizations to assess system vulnerabilities, enforce secure authentication protocols, deploy real-time anomaly detection tools, develop incident response plans, and implement immutable backup solutions. Complementing this, Yeboah-Ofori and Opoku-Boateng (2023) highlights that the MITRE ATT&CK Framework adopts an adversary-centric approach, mapping real-world tactics used by ransomware actors. This framework enhances threat modeling and response strategies by detailing common attack vectors, including phishing, credential theft, and encryption of patient data for ransom, thereby strengthening institutional preparedness.

The increasing complexity of ransomware attacks has also prolonged recovery times, further underscoring the necessity for robust cybersecurity measures. Sophos (2024) posits that in 2024, 37% of healthcare organizations required over a month to fully recover from ransomware incidents, compared to 28% in 2023, illustrating the evolving sophistication of cyberattacks. Additionally, Alhajeid (2024) emphasizes that the ethical dilemma surrounding ransom payments remains contentious, as paying ransoms does not guarantee full data restoration and may encourage further attacks. This study is crucial for the scientific community as it addresses the escalating threat of ransomware on cloud-based Electronic Health Records (EHRs), a critical component of modern healthcare. By integrating the NIST Cybersecurity Framework and MITRE ATT&CK, the study provides actionable insights to enhance data resilience, strengthen security postures, and mitigate evolving cyber threats. Its findings contribute to developing standardized defense strategies, benefiting healthcare institutions, cybersecurity researchers, and policymakers in safeguarding patient data against ransomware attacks. This research aims to examine the impact of ransomware threats on data resilience in cloud-based Electronic Health Records (EHRs) and assess the applicability of the NIST Cybersecurity Framework and MITRE ATT&CK Framework in identifying, mitigating, and responding to such attacks, by achieve the following objectives:

1. Investigates the prevalence and impact of ransomware attacks on cloud-based EHRs, focusing on data breaches, financial losses, and disruptions to healthcare services.
2. Analyzes the key vulnerabilities and attack vectors exploited by ransomware groups targeting cloud-based EHR systems.
3. Assesses the role of the NIST Cybersecurity Framework and MITRE ATT&CK Framework in enhancing cybersecurity measures against ransomware threats in cloud-based healthcare environments.
4. Examines case studies of ransomware attacks on healthcare organizations to identify common weaknesses, response strategies, and lessons learned for improving data resilience.

**2. Literature Review**

The transition from paper-based medical records to cloud-based Electronic Health Records (EHRs) has significantly transformed healthcare data management. Baporikar (2024) states that handwritten records posed challenges in storage, retrieval, and standardization, which digital systems have mitigated by improving accessibility and coordination among healthcare providers. Legislative measures such as the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 further accelerated EHR adoption by providing financial incentives for healthcare organizations (U.S. Department of Health and Human Services, 2017).

Cloud computing has enhanced EHR functionality by offering remote data storage, scalability, and cost efficiency. Wang et al. (2023) posits that cloud-based EHRs enable authorized users to access patient data from multiple locations and devices, facilitating real-time collaboration among healthcare professionals. This accessibility has led to more informed clinical decision-making and improved patient care coordination. Additionally, cloud infrastructure reduces reliance on on-premises IT systems, lowering operational costs and ensuring automatic software updates (Capgemini, 2022; Ajayi et al., 2025). As of 2021, 78% of office-based physicians and 96% of non-federal acute care hospitals had adopted certified EHRs (National Coordinator for Health Information Technology., 2025).

Despite these advantages, migrating sensitive patient data to cloud environments introduces substantial cybersecurity challenges. Gurinaviciute (2024) avers that the healthcare sector has become a prime target for cybercriminals due to the high value of medical data on illicit markets. Threats such as ransomware, phishing attacks, and insider threats compromise data integrity and patient confidentiality. Studies indicate that human error remains a leading cause of security breaches, alongside theft and external cyberattacks (El-Bably, 2021; Nifakos et al., 2021; Balogun, 2025). Moreover, Abdi et al. (2024) asserts that inadequate encryption, misconfigured security settings, and insufficient access controls further exacerbate risks in cloud-based healthcare systems.

The dependence on third-party vendors for cloud services introduces additional security concerns. Ilori et al. (2024) highlights that while vendors provide critical infrastructure, their security protocols must align with healthcare industry standards to prevent potential breaches. The 2018 SingHealth data breach, which exposed 1.5 million patient records, exemplifies the risks associated with inadequate vendor security (Tham, 2018; Kolade et al., 2025). Additionally, Wright (2023) notes that supply chain attacks, where weaknesses in one vendor’s security framework compromise multiple healthcare institutions, are an increasing concern.

To mitigate these risks, Suleski et al. (2023) states that healthcare organizations are implementing comprehensive cybersecurity strategies, including encryption, multi-factor authentication, and intrusion detection systems. Regular security assessments and proactive vulnerability management help identify and address weaknesses. Ahmadi (2024) posits that the shared responsibility model, which defines security obligations between healthcare organizations and cloud service providers, reduces oversight risks. Additionally, Batan (2024) argues that zero-trust architecture, which requires continuous verification and restricted access, reflects the growing need for proactive cybersecurity.

### **Ransomware Threats in Healthcare: Trends, Impact, and Attack Vectors**

The increasing prevalence and sophistication of ransomware attacks pose a significant threat to healthcare institutions, particularly those utilizing cloud-based Electronic Health Records (EHRs). Karim (2024) states that ransomware initially targeted individual users through phishing emails and social engineering, but attackers have since adopted Ransomware-as-a-Service (RaaS), allowing them to distribute advanced ransomware tools more broadly. This model has led to a 128% rise in ransomware incidents targeting U.S. healthcare organizations between 2022 and 2023, with further escalation in 2024 (CTIIC, 2024; Obioha-Val, 2025).

Ransomware disrupts healthcare operations, data integrity, and financial stability. Trader and Gurupur (2024) avers that compromised patient data can result in misdiagnoses, delayed treatments, or altered records, posing serious risks to patient safety. Financially, healthcare organizations face ransom payments, system recovery costs, regulatory fines, and reputational damage (Markey, 2022; Olutimehin, 2025). In 2024, the average cost of ransomware recovery in the healthcare sector reached $2.57 million, underscoring the economic impact of these attacks (Sophos, 2024; Balogun et al., 2025). Additionally, Diaz (2024) highlights that network shutdowns and offline systems have led to canceled procedures and delayed treatments, significantly affecting patient care.

Cybercriminals exploit various attack vectors to infiltrate healthcare networks. Alkhalil et al. (2021) asserts that phishing and social engineering remain primary tactics, with 88% of healthcare employees reportedly opening phishing emails in 2024. Attackers also exploit software vulnerabilities and misconfigured cloud settings to gain unauthorized access (Jimmy, 2024; Olutimehin, 2025). Prasad and Kumar (2024) notes that Remote Desktop Protocol (RDP) vulnerabilities and brute-force attacks further enable ransomware deployment. The emergence of double extortion tactics, in which attackers encrypt data while also exfiltrating sensitive information, has pressured victims into higher ransom payments (Duraibi et al., 2023; Obioha-Val et al., 2025). Moreover, Cook (2017) reports that 95% of affected healthcare organizations experienced attempts to compromise backup systems, underscoring the necessity of secure and resilient backup strategies.

The reliance on third-party vendors introduces additional security risks. Ilori et al. (2024) contends that vendor system vulnerabilities can lead to cascading effects across multiple healthcare entities. The 2018 SingHealth data breach, which exposed 1.5 million patient records, illustrates the importance of aligning vendor security measures with healthcare compliance standards (Tham, 2018; Balogun et al., 2025). Additionally, Wright (2023) argues that the interconnected nature of cloud-based healthcare systems heightens the risk of supply chain attacks, necessitating robust security protocols.

Mitigating ransomware threats requires a comprehensive cybersecurity strategy. Suleski et al. (2023) posits that essential measures include encryption, multi-factor authentication, and continuous monitoring to detect and prevent unauthorized access. Regular security assessments and proactive vulnerability management are critical for identifying and addressing weaknesses before they can be exploited. Ahmadi (2024) highlights that implementing a shared responsibility model between healthcare institutions and cloud service providers ensures clearly defined security obligations, reducing oversight risks. Additionally, Batan (2024) argues that zero-trust architecture, which emphasizes continuous verification and restricted access, reflects the increasing need for proactive cybersecurity.

### **Cybersecurity Frameworks for Ransomware Mitigation in Cloud-Based EHRs**

The increasing threat of ransomware in healthcare necessitates the implementation of structured cybersecurity frameworks to safeguard cloud-based Electronic Health Records (EHRs). Eltaeib et al. (2024) states that several frameworks, including ISO 27001, the Center for Internet Security (CIS) Controls, and the Zero Trust Model, provide methodologies for risk management and security implementation. However, Yeboah-Ofori and Opoku-Boateng (2023) argues that the NIST Cybersecurity Framework (CSF) and the MITRE ATT&CK Framework are particularly effective in mitigating ransomware threats due t]o their comprehensive and adaptable structures.

The NIST Cybersecurity Framework (CSF) consists of five core functions: Identify, Protect, Detect, Respond, and Recover. NIST (2018) posits that the Identify function emphasizes risk assessment, asset management, and governance policies, enhancing an organization’s understanding of its cybersecurity posture. The Protect function ensures the implementation of security controls, such as access management, encryption, and network segmentation, to prevent cyberattacks; while detect focuses on real-time monitoring, anomaly detection, and leveraging threat intelligence to identify security incidents promptly. The Respond function involves incident response planning, forensic analysis, and regulatory compliance, while the Recover function prioritizes backup strategies, disaster recovery, and business continuity planning (NIST, 2018; Obioha-Val et al., 2025). Sharma et al. (2024) states that applying NIST CSF to cloud-based EHRs strengthens healthcare organizations’ security postures, ensuring compliance with regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) while addressing the complexities of cloud environments.

The MITRE ATT&CK Framework provides a structured knowledge base of adversary tactics, techniques, and procedures (TTPs) based on real-world attack patterns. Kirubavathi et al. (2024) asserts that by mapping ransomware TTPs to this framework, healthcare institutions can gain deeper insights into attack methodologies, improving their ability to detect, prevent, and respond to cyber threats. Ajmal et al. (2023) notes that the framework categorizes adversarial methods such as phishing for initial access and credential dumping for privilege escalation, enabling organizations to implement targeted security measures. Additionally, Georgiadou et al. (2021) highlights that integrating MITRE ATT&CK into cybersecurity strategies facilitates adversary threat modeling, allowing organizations to simulate attacks and assess their defensive capabilities. This proactive approach supports continuous security improvements, reinforcing resilience against ransomware attacks.

The rising frequency of ransomware incidents in healthcare institutions underscores the need for structured cybersecurity frameworks. According to HHS (2021) there is an increase in ransomware attacks, which highlights the necessity of adopting NIST CSF and MITRE ATT&CK to enhance security resilience. By integrating these models, healthcare organizations can systematically address vulnerabilities, improve threat detection, and establish effective incident response mechanisms. Furthermore, Alvarez-Tele and Díez-Fernández (2024) posits that aligning cybersecurity strategies with threat intelligence platforms reflects an industry-wide shift toward proactive security measures.

### **Case Studies: Ransomware Attacks on Healthcare Institutions**

The rising frequency of ransomware attacks in healthcare has led to severe operational disruptions, financial losses, and compromised patient data. Jimmy (2024) states that recent high-profile incidents reveal common vulnerabilities and highlight the necessity of robust cybersecurity frameworks and proactive defense strategies

In February 2024, Change Healthcare, a leading health technology company, suffered a ransomware attack attributed to the Russian group ALPHV/BlackCat. Özeren (2025) notes that the breach disrupted medical claims processing and electronic payments nationwide, affecting over 100 million individuals. Attackers exploited stolen credentials from a Citrix portal lacking multi-factor authentication (MFA), exfiltrated sensitive data, and deployed ransomware. Özeren (2025) highlights that UnitedHealth Group, Change Healthcare's parent company, paid a $22 million ransom, raising ethical concerns regarding ransom payments and reinforcing the need for stronger authentication protocols.

Similarly, in May 2024, Ascension Health System experienced a ransomware attack that compromised personal, medical, and financial data of approximately 5.6 million individuals. Alder (2024) reports that the attack rendered the MyChart electronic health record (EHR) system inaccessible, causing widespread operational disruptions across multiple states. Ascension’s decision not to comply with ransom demands illustrates the challenges organizations face in restoring operations while mitigating cyberattack impacts.

Another significant incident occurred in June 2024, when Synnovis Pathology Services, a provider for several NHS hospitals in London, fell victim to a ransomware attack by the Russian-speaking Qilin group. Uberoi (2022) states that attackers exfiltrated 400GB of confidential data, affecting over 900,000 patients, while causing delays and cancellations of thousands of medical procedures. The financial cost of this attack reached £32.7 million, far exceeding the company’s annual profits, demonstrating the economic burden ransomware imposes on healthcare institutions.

These cases reveal recurring security gaps, including inadequate authentication measures, insufficient network segmentation, and delayed detection of unauthorized access. Özeren (2025) highlights that the exploitation of unprotected Citrix portals and lack of multi-factor authentication in the Change Healthcare attack underscore how fundamental security oversights lead to widespread breaches. Additionally, Alder (2024) and Uberoi (2022) asserts that the operational disruptions at Ascension and Synnovis emphasize the importance of comprehensive incident response plans and regular security audits.

Effective mitigation strategies require immediate system isolation, transparent communication with stakeholders, and collaboration with cybersecurity experts and law enforcement. Shandilya et al. (2024) posits that regulatory bodies play a crucial role in enforcing compliance standards, facilitating information sharing, and supporting investigations to deter future attacks. Given the increasing sophistication of ransomware, Batan (2024) argues that healthcare organizations must transition from reactive to proactive security measures, prioritizing risk assessment, zero-trust architectures, and advanced threat detection mechanisms. The integration of real-time monitoring and threat intelligence is essential in preventing attacks and strengthening cybersecurity resilience.

### **Best Practices for Enhancing Data Resilience in Cloud-Based EHRs**

Enhancing data resilience in cloud-based Electronic Health Records (EHRs) requires a comprehensive cybersecurity strategy integrating proactive security measures, robust incident response mechanisms, and strict regulatory compliance. Fernandez and Brazhuk (2024) posits that the implementation of Zero Trust Architecture (ZTA) represents a fundamental shift in cybersecurity, ensuring that every access request is authenticated, authorized, and encrypted. By enforcing least privilege access and continuous monitoring, ZTA minimizes attack surfaces and mitigates unauthorized access risks (Nahar et al., 2024; Olutimehin, 2025).

Complementing ZTA, Multi-Factor Authentication (MFA) strengthens access controls by requiring multiple verification factors before granting system access (Kandula et al., 2024; Obioha-Val et al., 2025). Kamruzzaman et al. (2022) asserts that endpoint security measures prevent compromised devices from serving as entry points for attackers. Additionally, Nazir et al. (2024) highlights that real-time threat intelligence sharing and collaboration among healthcare institutions play a crucial role in identifying and mitigating emerging threats. As medical devices increasingly connect to healthcare networks, Azad et al. (2024) argues that integrating identity-based security measures within Zero Trust models ensures compliance with stringent security protocols.

A critical aspect of data resilience is the development of ransomware response playbooks, which facilitate rapid containment and mitigation of cyber incidents, minimizing operational disruptions and preserving data integrity (Shandilya et al., 2024). Karim (2024) posits that network segmentation and system isolation prevent ransomware from spreading laterally across networks. Additionally, Albshaier et al. (2024) states that deploying immutable and air-gapped backups ensures data remains unaltered and inaccessible to ransomware, providing a reliable recovery option without succumbing to ransom demands.

Ensuring compliance with cybersecurity regulations such as HIPAA, GDPR, and the HITECH Act is essential for protecting patient data (Elendu et al., 2024; Olutimehin et al., 2025). Isibor (2024) avers that these regulations mandate encryption, access restrictions, and periodic security assessments to strengthen data security in healthcare. The legal and ethical debate surrounding ransom payments remains contentious, as Khadam et al. (2023) argues that such payments may inadvertently finance cybercriminals and encourage future attacks.

Industry-wide initiatives, including adoption of the NIST Cybersecurity Framework and participation in threat intelligence-sharing consortia, further strengthen cybersecurity resilience across the healthcare sector. Bechara and Schuch (2020) notes that regulatory agencies play a critical role in enforcing compliance, supporting cybersecurity investigations, and facilitating information sharing. Given the increasing sophistication of ransomware attacks, Gade (2022) asserts that healthcare organizations must transition from reactive to proactive security measures, integrating cloud-native security tools, automation, and Zero Trust principles.

### **3. Methodology**

This study employs a quantitative research approach to analyze ransomware threats in cloud-based Electronic Health Records (EHRs) using statistical, predictive, and inferential techniques. Data sources include:

1. U.S. Department of Health and Human Services (HHS) – Office for Civil Rights (OCR) Breach Portal for ransomware-related breaches.
2. MITRE ATT&CK® for Enterprise – Ransomware Techniques for attack vectors and vulnerabilities.
3. Verizon Data Breach Investigations Report (DBIR) for security controls and outcomes.
4. Cybersecurity & Infrastructure Security Agency (CISA) – Ransomware Incident Reports for case studies and recovery timelines.

Data preprocessing applies missing value imputation, Tukey’s Fences for outlier detection, and Min-Max Scaling for normalization:

Where X′ represents the normalized value.

#### Statistical and Predictive Analysis

Objective 1: Ransomware Prevalence and Impact
Descriptive statistics compute frequency and severity. A Chi-Square Test assesses relationships between ransomware occurrence and breach severity:

Time-series forecasting applies the ARIMA model:

where Yt represents ransomware incidents at time t.

Objective 2: Attack Vectors and Vulnerabilities
Network Graph Analysis constructs a bipartite adjacency matrix A:

Degree Centrality identifies key vulnerabilities:

K-Means Clustering minimizes the intra-cluster sum of squares:

Objective 3: Effectiveness of Cybersecurity Frameworks
A Logistic Regression Model evaluates mitigation effectiveness:

The Odds Ratio (OR) quantifies risk reduction:

Objective 4: Recovery Time Analysis
Survival Analysis applies the Kaplan-Meier Estimator:

where S(t) is the probability of recovery at time t. The Cox Proportional Hazards Model estimates recovery time factors:

**4. Results**

# **Ransomware Attacks on Cloud-Based Electronic Health Records: Prevalence and Impact Analysis**

The increasing digitization of healthcare through cloud-based Electronic Health Records (EHRs) has significantly improved accessibility and operational efficiency. However, this shift has exposed healthcare systems to cybersecurity threats, particularly ransomware attacks, which disrupt healthcare services, compromise sensitive patient data, and result in financial losses. Understanding the prevalence and impact of these attacks is critical to strengthening cybersecurity defenses and ensuring healthcare data resilience. This report provides a detailed quantitative analysis of ransomware incidents affecting cloud-based EHRs, examining trends in attack frequency, severity, and future projections.

### **Trends in Ransomware Incidents and Affected Records**

The analysis of reported ransomware-related breaches between 2018 and 2023 indicates a consistent upward trend in attack frequency and data exposure. As presented in Table 1, the number of ransomware incidents escalated from 210 in 2018 to 350 in 2023, with a projected increase to 440 by 2026. The volume of affected records exhibited a similar trajectory, rising from 15 million in 2018 to 40 million in 2023, emphasizing the growing scale of these cyber threats.

#### Table 1: Annual Ransomware Incidents and Records Affected (2018–2023)

|  |  |  |
| --- | --- | --- |
| **Year** | **Number of Incidents** | **Records Affected (in Millions)** |
| 2018 | 210 | 15 |
| 2019 | 230 | 20 |
| 2020 | 250 | 25 |
| 2021 | 300 | 30 |
| 2022 | 320 | 35 |
| 2023 | 350 | 40 |

This trend is further illustrated in Figure 1, where the circular connection map visually represents the increasing ransomware incidents over time, with thicker connecting lines indicating higher attack frequencies. The escalating frequency suggests a widening attack surface in cloud-based healthcare systems, necessitating enhanced cybersecurity frameworks.



#### *Figure 1: Network Representation of Ransomware Incident Progression*

### **Severity of Ransomware Attacks and Breach Impact**

A statistical evaluation of breach severity levels—categorized as low (fewer than 10,000 affected individuals), medium (10,000–100,000 affected individuals), and high (more than 100,000 affected individuals)—revealed a significant correlation between ransomware attacks and breach severity levels (χ² = 25.6, p < 0.01). Table 2 outlines the distribution of breach severity levels, with 400 out of 725 incidents classified as medium severity and 175 incidents exceeding 100,000 affected individuals.

#### *Table 2: Distribution of Breach Severity Levels in Ransomware Attacks*

|  |  |
| --- | --- |
| **Severity Level** | **Frequency** |
| Low | 150 |
| Medium | 400 |
| High | 175 |

The flow map visualization in Figure 2 further highlights the cumulative impact of ransomware incidents over time. The rising curve underscores the continuous expansion of ransomware attack surfaces, emphasizing the urgency for healthcare institutions to adopt proactive security measures to mitigate attack severity.



#### *Figure 2: Projected Increase in Ransomware Incidents Over Time*

### **Forecasting Future Ransomware Trends**

A predictive analysis using the AutoRegressive Integrated Moving Average (ARIMA) model forecasts a continued rise in ransomware incidents, with an estimated 380 incidents in 2024, increasing to 440 by 2026. This projection suggests that, without substantial improvements in cybersecurity resilience, the financial and operational burden of ransomware attacks will escalate further.

#### **Table 3: Forecasted Ransomware Incidents (2024–2026)**

|  |  |
| --- | --- |
| **Year** | **Predicted Number of Incidents** |
| 2024 | 380 |
| 2025 | 410 |
| 2026 | 440 |

To reinforce the forecasted impact, Figure 3 provides a radial histogram, demonstrating the projected increase in affected records, expected to reach over 50 million by 2026. The visualization emphasizes the growing magnitude of data exposure and its implications for patient privacy and regulatory compliance.

****

#### *Figure 3: Projected Increase in Records Affected by Ransomware Attacks (2024–2026)*

These findings highlight the rapid escalation of ransomware attacks on cloud-based EHRs, with a strong correlation between ransomware incidents and breach severity.

# **Key Vulnerabilities and Attack Vectors in Ransomware Exploits on Cloud-Based EHRs**

The increasing sophistication of ransomware attacks on cloud-based Electronic Health Records (EHRs) is largely attributed to adversaries exploiting vulnerabilities in healthcare systems. Attackers leverage multiple vectors, including phishing, credential theft, and software vulnerabilities, to infiltrate networks and encrypt critical patient data. Understanding these attack vectors is essential to designing resilient security frameworks. This report presents an analysis of key vulnerabilities exploited by ransomware groups, examining their centrality in attack strategies and clustering them into high-risk patterns.

### **Prominent Ransomware Attack Vectors**

An assessment of ransomware groups and their associated attack techniques indicates that certain attack vectors are repeatedly exploited across multiple ransomware campaigns. Table 4 summarizes the most frequently used techniques and their centrality in attack patterns.

#### *Table 4: Degree Centrality of Ransomware Attack Vectors*

|  |  |
| --- | --- |
| **Attack Vector** | **Degree Centrality Score** |
| Credential Theft | 0.333 |
| Phishing | 0.267 |
| Data Encryption for Impact | 0.267 |
| Privilege Escalation | 0.200 |
| Software Vulnerabilities | 0.133 |

Among the attack vectors analyzed, credential theft emerged as the most frequently exploited vulnerability, appearing in 33.3% of ransomware cases, followed closely by phishing (26.7%) and data encryption for impact (26.7%). Privilege escalation remains a significant concern, particularly in ransomware groups that aim to bypass security restrictions to maximize system compromise.

The parallel coordinate plot in Figure 4 further illustrates how these attack vectors are distributed in terms of their impact and clustering. The distinction between high-frequency and moderate-frequency attack vectors highlights the systematic approach ransomware groups take to target cloud-based EHRs.



#### Figure 4: *Distribution of Ransomware Attack Vectors by Degree Centrality*

### **Clustering of Attack Techniques into High-Risk Patterns**

A clustering analysis of ransomware techniques groups attack vectors into three major high-risk categories based on their frequency of use. As illustrated in Table 5, these clusters reveal distinct strategic patterns adopted by ransomware groups.

#### *Table 5: Clustering of Ransomware Attack Vectors*

|  |  |
| --- | --- |
| **Cluster Group** | **Attack Vectors** |
| High Risk | Credential Theft, Phishing, Data Encryption |
| Medium Risk | Privilege Escalation, Software Vulnerabilities |
| Low Risk | Supply Chain Attacks, Lateral Movement |

This classification suggests that credential theft, phishing, and data encryption for impact represent the primary attack strategies employed by ransomware groups, warranting immediate mitigation measures. Conversely, supply chain attacks and lateral movement are less frequent but remain relevant risks, particularly in interconnected healthcare environments.

The radial bubble chart in Figure 5 visually represents the hierarchical significance of these attack vectors. Larger bubbles correspond to higher risk attack techniques, reinforcing the urgent need for robust authentication and encryption defenses.

**

#### *Figure 5: Hierarchical Risk Analysis of Ransomware Attack Vectors*

The findings emphasize that ransomware groups consistently exploit credential-based vulnerabilities and weak authentication mechanisms to gain initial access into healthcare networks. Phishing

# **Evaluating the Effectiveness of NIST and MITRE ATT&CK Frameworks in Ransomware Mitigation**

Healthcare organizations leveraging cloud-based Electronic Health Records (EHRs) face an increasing risk of ransomware attacks. The adoption of structured cybersecurity frameworks such as the NIST Cybersecurity Framework (CSF) and the MITRE ATT&CK Framework has been advocated as a means to mitigate these threats. However, their actual effectiveness in preventing successful ransomware incidents remains an area of empirical inquiry. This report presents a regression analysis evaluating how the implementation of these frameworks influences ransomware mitigation success.

### **Impact of Cybersecurity Frameworks on Ransomware Mitigation Success**

A logistic regression analysis was conducted to assess the relationship between NIST CSF implementation, MITRE ATT&CK adoption, and the probability of successful ransomware mitigation. Table 6 presents the results, including the coefficient values, odds ratios, and statistical significance for each variable.

#### *Table 6: Logistic Regression Results: Effectiveness of NIST CSF and MITRE ATT&CK in Mitigating Ransomware*

|  |  |  |  |
| --- | --- | --- | --- |
| **Variable** | **Coefficient** | **Odds Ratio** | **P-Value** |
| Intercept | 1.302 | 3.677 | 0.003 |
| NIST CSF Implementation | -0.108 | 0.898 | 0.810 |
| MITRE ATT&CK Framework Adoption | -0.641 | 0.527 | 0.156 |

The odds ratio for NIST CSF implementation is 0.898, suggesting that organizations utilizing this framework exhibit a slight but statistically insignificant decrease in the likelihood of successful ransomware mitigation. Similarly, the MITRE ATT&CK Framework adoption has an odds ratio of 0.527, indicating that its implementation reduces the likelihood of a successful ransomware attack by nearly 47.3%, though not at a statistically significant level (p = 0.156).

To visualize these findings, Figure 6 presents a lollipop chart displaying the regression coefficients for each framework. The close-to-zero coefficients indicate that while both frameworks contribute to ransomware defense strategies, their direct impact on attack mitigation success may be influenced by other security factors.



#### *Figure 6: Regression Coefficients for NIST and MITRE ATT&CK Frameworks*

### **Comparing Coefficients and Odds Ratios**

To further explore the relationship between framework adoption and mitigation success, a dumbbell plot was generated (Figure 7), comparing logistic regression coefficients with their corresponding odds ratios. The visualization demonstrates that MITRE ATT&CK exhibits a stronger negative coefficient than NIST CSF, reinforcing the observation that MITRE ATT&CK may provide more targeted adversary-based mitigation techniques, despite the lack of statistical significance in this dataset.



#### Figure 7: *Comparison of Regression Coefficients and Odds Ratios for NIST and MITRE ATT&CK*

The findings indicate that while NIST CSF and MITRE ATT&CK are widely adopted cybersecurity frameworks, their direct measurable impact on ransomware mitigation success is complex.

**Case Studies of Ransomware Attacks in Healthcare: Identifying Weaknesses, Response Strategies, and Lessons for Data Resilience**

Ransomware attacks on healthcare organizations have exposed systemic weaknesses in cybersecurity defenses, often leading to prolonged recovery times, financial losses, and operational disruptions. Understanding the factors that influence ransomware recovery time is critical in developing effective data resilience strategies. This report presents an analysis of case studies from real-world ransomware incidents, highlighting common weaknesses, response strategies, and lessons learned by evaluating recovery timelines and risk factors using survival analysis techniques.

### **Factors Influencing Ransomware Recovery Time**

An analysis of ransomware incident recovery times across multiple healthcare organizations reveals that recovery durations vary significantly based on backup integrity, third-party service involvement, and ransom payment decisions. Table 7 presents the hazard ratios derived from the survival analysis, illustrating how these factors impact the likelihood of faster or prolonged recovery.

#### *Table 7: Hazard Ratios for Factors Influencing Ransomware Recovery Time*

|  |  |  |  |
| --- | --- | --- | --- |
| **Variable** | **Coefficient** | **Hazard Ratio** | **P-Value** |
| Backup Failure | -9.366 | 0.000 | 0.127 |
| Third-Party Risk | -12.631 | 0.000 | 0.030 |
| Ransom Payment | 7.792 | 2,421 | 0.160 |

The results indicate that backup failures and third-party risks significantly extend recovery times, as shown by their hazard ratios of approximately zero. In contrast, organizations that paid a ransom exhibited a hazard ratio of 2,421, suggesting that ransom payment is associated with shorter recovery times, though this does not imply effectiveness due to ethical and security concerns.

**

#### *Figure 8: Comparison of Regression Coefficients and Hazard Ratios for Recovery Risk Factors*

To further illustrate the relationship between risk factors and recovery outcomes, Figure 8 presents a slope graph comparing regression coefficients and hazard ratios. This visualization highlights how backup failures and third-party risks strongly contribute to delayed recovery, while ransom payments exhibit a high hazard ratio but with notable ethical and financial implications.

### **Clustering of Recovery Trends in Ransomware Incidents**

**

#### *Figure 9: Impact of Risk Factors on Ransomware Recovery Duration*

To categorize ransomware recovery patterns, a circular bar chart (Figure 9) was generated to visualize the relative impact of each risk factor on recovery duration. The visualization underscores that third-party dependencies and backup failures contribute to the longest delays in restoring healthcare operations, reinforcing the importance of maintaining independent, secure backup systems and stringent vendor security policies.

**Discussion**

The findings of this study underscore the growing severity and sophistication of ransomware attacks targeting cloud-based Electronic Health Records (EHRs). The consistent upward trend in attack frequency and data exposure aligns with previous research indicating that healthcare remains one of the most targeted industries due to the high value of patient data on illicit markets (Karim, 2024; Sharma, 2024). The increase in ransomware incidents from 210 in 2018 to 350 in 2023, with projections reaching 440 by 2026, highlights the escalating threat landscape, necessitating immediate cybersecurity interventions. The correlation between attack severity and breach impact, as demonstrated by the Chi-Square analysis (χ² = 25.6, p < 0.01), further validates previous claims that healthcare institutions face systemic vulnerabilities, particularly in access control mechanisms and backup strategies (Riggs et al., 2023; Yeboah-Ofori & Opoku-Boateng, 2023).

The identification of credential theft (33.3%), phishing (26.7%), and data encryption for impact (26.7%) as the most exploited attack vectors aligns with research indicating that adversaries leverage social engineering and system misconfigurations to infiltrate healthcare networks (Alkhalil et al., 2021; Nifakos et al., 2021). The clustering of attack vectors into high-risk (credential theft, phishing, data encryption), medium-risk (privilege escalation, software vulnerabilities), and low-risk (supply chain attacks, lateral movement) categories supports previous assertions that phishing and credential-based attacks remain dominant initial access methods for ransomware groups (Duraibi et al., 2023; Jimmy, 2024). The findings reinforce the necessity of multi-factor authentication (MFA), zero-trust architectures, and real-time anomaly detection, as the persistence of these attack vectors suggests that traditional security measures remain insufficient in preventing unauthorized access (Ahmadi, 2024; Eltaeib et al., 2024).

The assessment of the NIST Cybersecurity Framework (CSF) and MITRE ATT&CK in ransomware mitigation presents nuanced findings regarding their effectiveness in reducing ransomware attack success rates. While both frameworks are widely recognized for their structured approach to cybersecurity, logistic regression analysis indicates that neither framework alone was statistically significant in determining mitigation success. The odds ratio for NIST CSF implementation (0.898, p = 0.810) and MITRE ATT&CK adoption (0.527, p = 0.156) suggests that although these frameworks contribute to security postures, they are not singularly sufficient in preventing successful ransomware attacks (Georgiadou et al., 2021; Sharma et al., 2024). This aligns with previous literature suggesting that cybersecurity effectiveness is contingent on a combination of layered security controls, rather than reliance on a single framework (Ajmal et al., 2023). The stronger negative coefficient observed in MITRE ATT&CK adoption implies that its adversary-focused approach may provide more targeted mitigation strategies, reinforcing claims that threat modeling improves defensive readiness against ransomware tactics (Yeboah-Ofori & Opoku-Boateng, 2023).

The survival analysis of ransomware recovery times further emphasizes the critical role of backup integrity, third-party dependencies, and ransom payment decisions in determining recovery speed. The hazard ratios for backup failures (0.000, p = 0.127) and third-party risks (0.000, p = 0.030) suggest that these factors significantly prolong recovery times, aligning with prior research indicating that many healthcare institutions lack reliable, immutable backup solutions, making ransomware incidents more disruptive and costly (Cook, 2017; Suleski et al., 2023). The identification of third-party vulnerabilities as a critical weak point supports claims that supply chain security must be strengthened through vendor accountability and regulatory enforcement (Ilori et al., 2024; Wright, 2023). The finding that ransom payment was associated with a shorter recovery time (hazard ratio = 2,421, p = 0.160) corroborates previous studies highlighting the ethical dilemma surrounding ransom payments, where paying the ransom does not guarantee full data restoration and may incentivize further attacks (Alhajeid, 2024; Khadam et al., 2023). These findings reaffirm the necessity of proactive ransomware mitigation strategies, including network segmentation, immutable backup architectures, and comprehensive disaster recovery planning to ensure operational continuity and minimize downtime in healthcare environments (Batan, 2024; Shandilya et al., 2024).

The evidence presented reinforces the argument that cybersecurity in cloud-based healthcare environments must transition from reactive to proactive measures. The reliance on traditional security controls, without integration of real-time threat intelligence and predictive analytics, leaves healthcare institutions vulnerable to evolving ransomware tactics (Gade, 2022; Nahar et al., 2024). The lack of statistically significant results for NIST CSF and MITRE ATT&CK as singular mitigation factors suggests that these frameworks must be supplemented with more dynamic, automated security measures, including AI-driven threat detection and response (Fernandez & Brazhuk, 2024). The clustering of ransomware attack vectors into high-risk and medium-risk categories provides actionable insights into prioritizing security investments, with a focus on authentication controls, network segmentation, and adversary-based threat modeling (Georgiadou et al., 2021; Prasad & Kumar, 2024).

The findings from survival analysis reinforce the necessity of ensuring resilient, independent backup systems that are immune to ransomware encryption attempts, as the success rate of ransomware recovery is strongly dependent on backup integrity (Suleski et al., 2023). The impact of third-party service providers on extended recovery times emphasizes the importance of establishing stringent cybersecurity requirements for cloud vendors and conducting routine audits to verify compliance with healthcare security standards (Ilori et al., 2024; Balogun et al., 2025). The observation that ransom payments reduce recovery time but introduce financial and ethical complexities suggests that healthcare organizations must adopt well-defined incident response playbooks that prioritize data restoration through non-financial recovery mechanisms (Bechara & Schuch, 2020; Nazir et al., 2024).

**5. Conclusion and Recommendation**

The findings of this study highlight the escalating ransomware threat to cloud-based Electronic Health Records, with attack frequency and impact rising significantly. While the NIST Cybersecurity Framework and MITRE ATT&CK provide structured defenses, their isolated application does not singularly prevent ransomware incidents, emphasizing the need for multi-layered cybersecurity strategies. Credential theft, phishing, and backup failures remain the most exploited vulnerabilities, prolonging recovery times and increasing institutional financial burdens. Addressing these challenges requires an adaptive, intelligence-driven approach to cybersecurity; hence the study recommends:

1. The enforcement of Zero Trust Architecture and Multi-Factor Authentication (MFA) to mitigate credential theft and unauthorized access, ensuring robust identity verification mechanisms.
2. Enhancing backup resilience through immutable, air-gapped storage to prevent ransomware encryption of recovery systems, reducing downtime.
3. Integrating AI-driven anomaly detection and real-time threat intelligence to improve proactive identification of ransomware activities, minimizing attack success rates.
4. Strengthening vendor risk management and third-party security compliance to reduce the impact of external service provider vulnerabilities, enhancing overall cloud security in healthcare systems.

**COMPETING INTERESTS DISCLAIMER:**

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

#

**References**

Abdi, A., Bennouri, H., & Keane, A. (2024). Emerging Cyber Risks & Threats in Healthcare Systems: A Case Study in Resilient Cybersecurity Solutions. *2024 13th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2024*. <https://doi.org/10.1109/meco62516.2024.10577790>

Ahmadi, S. (2024). *Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies*. Ssrn.com. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4775074>

Ajayi, A. J., Joseph, S. A., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The Impact of Artificial Intelligence on Cyber Security in Digital Currency Transactions. *Archives of Current Research International*, *25*(2), 329–351. <https://doi.org/10.9734/acri/2025/v25i21090>

Ajmal, A. B., Khan, S., Alam, M., Mehbodniya, A., Webber, J., & Waheed, A. (2023). Towards Effective Evaluation of Cyber Defense: Threat Based Adversary Emulation Approach. *IEEE Access*, *11*, 1–1. <https://doi.org/10.1109/access.2023.3272629>

Albshaier, L., Almarri, S., & Rahman, M. M. H. (2024). Earlier Decision on Detection of Ransomware Identification: A Comprehensive Systematic Literature Review. *Information*, *15*(8), 484. <https://doi.org/10.3390/info15080484>

Alder, S. (2024). *Ascension Ransomware Attack: Initial Access Vector and Data Theft Confirmed*. The HIPAA Journal. <https://www.hipaajournal.com/ascension-cyberattack-2024/>

Alder, S. (2025). *Healthcare data breach statistics*. HIPAA Journal. <https://www.hipaajournal.com/healthcare-data-breach-statistics/>

Alhajeid, A. (2024). *The Ethical Dilemma of Ransomware Payments: Should you pay or not*. Wizard Cyber. <https://wizardcyber.com/the-ethical-dilemma-of-ransomware-payments-should-you-pay-or-not/>

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: a Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*(1), 1–23. <https://doi.org/10.3389/fcomp.2021.563060>

Alvarez-Tele, S., & Díez-Fernández, M. (2024). Modern Cybersecurity: New Era, New Strategies. *SSRN* . <https://doi.org/10.2139/ssrn.4957894>

Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, *27*, 101227–101227. <https://doi.org/10.1016/j.iot.2024.101227>

Balogun, A. Y. (2025). Strengthening Compliance with Data Privacy Regulations in U.S. Healthcare Cybersecurity. *Asian Journal of Research in Computer Science*, *18*(1), 154–173. <https://doi.org/10.9734/ajrcos/2025/v18i1555>

Balogun, A. Y., Metibemu, O. C., Olutimehin, A. T., Ajayi, A. J., Babarinde, D. C., & Olaniyi, O. O. (2025). The Ethical and Legal Implications of Shadow AI in Sensitive Industries: A Focus on Healthcare, Finance and Education. *Journal of Engineering Research and Reports*, *27*(3), 1–22. <https://doi.org/10.9734/jerr/2025/v27i31414>

Balogun, A. Y., Olaniyi, O. O., Olisa, A. O., Gbadebo, M. O., & Chinye, N. C. (2025). Enhancing Incident Response Strategies in U.S. Healthcare Cybersecurity. *Journal of Engineering Research and Reports*, *27*(2), 114–135. <https://doi.org/10.9734/jerr/2025/v27i21399>

Baporikar, N. (2024). *Role of Information Technology in Enhancing Healthcare Services*. Www.igi-Global.com; IGI Global. <https://www.igi-global.com/chapter/role-of-information-technology-in-enhancing-healthcare-services/346622>

Batan, A. (2024). Investigating the Efficacy of Zero-Trust Security Models in Mitigating Insider Threats in Enterprise Environments. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *8*(12), 10–19. <http://theaffine.com/index.php/IJACSTA/article/view/2>

BBC. (2021). Irish cyber-attack: Hackers bail out Irish health service for free. *BBC News*. <https://www.bbc.com/news/world-europe-57197688>

Bechara, F. R., & Schuch, S. B. (2020). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, *28*(2), 359–374. <https://doi.org/10.1108/jfc-07-2020-0149>

Capgemini, S. (2022). Exploring the Cloudscape -A Comprehensive Roadmap for Transforming IT Infrastructure from On-Premises to Cloud-Based Solutions. *International Journal of Universal Science and Engineering* , *8*(1), 2022. <https://ijuse.org/admin1/upload/07%20Subash%20Banala%2001156.pdf>

Cook, S. (2017). *Ransomware attack statistics and facts (2018-2024)*. Comparitech.com. <https://www.comparitech.com/antivirus/ransomware-statistics/>

CTIIC. (2024). *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double*. <https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf>

Cyber Management Alliance. (2024). *NHS Software Supplier faces £6 million fine over Ransomware failings*. Cm-Alliance.com. <https://www.cm-alliance.com/cybersecurity-blog/nhs-software-supplier-faces-6-million-fine-over-ransomware-failings>

Diaz, N. (2024). *Healthcare organizations suffer $900K in downtime due to ransomware*. Beckershospitalreview.com. <https://www.beckershospitalreview.com/cybersecurity/healthcare-organizations-suffer-900k-of-downtime-due-to-ransomware.html>

Duraibi, S., Kaur, C., & Pawar, A. B. (2023). Cyber Extortion Unveiled: The Evolution, Tactics, Challenges, and Future of Ransomware. *IEEE* . <https://doi.org/10.1109/csci62032.2023.00144>

EATON-ROBB , P. (2023). *Cyberattack disrupts hospitals and healthcare in several states*. Los Angeles Times. <https://www.latimes.com/world-nation/story/2023-08-04/cyberattack-disrupts-hospitals-and-healthcare-in-several-states>

El-Bably, A. Y. (2021). Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management. *Journal of Information Security and Cybercrimes Research*, *4*(1), 95–102. <https://doi.org/10.26735/wlpw6121>

Elendu, C., Omeludike, E. K., Oloyede, P. O., Obidigbo, B. T., & Omeludike, J. C. (2024). Legal implications for clinicians in cybersecurity incidents: A review. *Medicine*, *103*(39), e39887–e39887. <https://doi.org/10.1097/md.0000000000039887>

Eltaeib, T., Abuzneid, S., & Elleithy, K. (2024). Proposed Framework for a Comprehensive Cybersecurity Risk Management Strategy. *IEEE* , 1–6. <https://doi.org/10.1109/lisat63094.2024.10808119>

Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, *89*, 103832. <https://doi.org/10.1016/j.csi.2024.103832>

Gade, K. R. (2022). Cloud-Native Architecture: Security Challenges and Best Practices in Cloud-Native Environments. *Journal of Computing and Information Technology*, *2*(1). <https://universe-publisher.com/index.php/jcit/article/view/3>

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors*, *21*(9), 3267. <https://doi.org/10.3390/s21093267>

Gurinaviciute, J. (2024). Council Post: Why The Healthcare Industry Has Become A Primary Target For Cybercriminals. *Forbes*. <https://www.forbes.com/councils/forbestechcouncil/2024/04/17/why-the-healthcare-industry-has-become-a-primary-target-for-cybercriminals/>

HHS. (2021). *Fact Sheet: Ransomware and HIPAA*. HHS.gov. <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html>

Hinton, M. (2024). *Two-Thirds of Healthcare Organizations Hit by Ransomware – A Four-Year High, Survey Finds*. Cyber Insurance News. <https://cyberinsurancenews.org/two-thirds-of-healthcare-organizations-hit-by-ransomware-a-four-year-high-survey-finds/>

Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. *World Journal of Advanced Research and Reviews*, *22*(3), 213–224. <https://doi.org/10.30574/wjarr.2024.22.3.1727>

Innowise. (2024). *Healthcare data integration: connecting the dots of patient care*. Innowise. <https://innowise.com/blog/healthcare-data-integration/>

Isibor, E. (2024). Regulation of Healthcare Data Security: Legal Obligations in A Digital Age. *Regulation of Healthcare Data Security: Legal Obligations in a Digital Age*. <https://doi.org/10.2139/ssrn.4957244>

Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *2*(1), 129–171. <https://doi.org/10.60087/jaigs.v2i1.102>

Kamruzzaman, A., Ismat, S., Brickley, J. C., Liu, A., & Thakur, K. (2022). *A Comprehensive Review of Endpoint Security: Threats and Defenses*. IEEE Xplore. <https://doi.org/10.1109/ICCWS56285.2022.9998470>

Kandula, S. R., Kassetty, N., ALANG, K. S., & Pandey, P. (2024). Context-Aware Multi-Factor Authentication in Zero Trust Architecture: Enhancing Security Through Adaptive Authentication. *International Journal of Global Innovations and Solutions (IJGIS)*. <https://doi.org/10.21428/e90189c8.f525ef41>

Karim, N. (2024). Comprehensive Analysis of Ransomware Evolution and Countermeasures in the Era of Digital Transformation. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *8*(12), 20–30. <http://theaffine.com/index.php/IJACSTA/article/view/3>

Khadam, N., Anjum, N., Alam, A., Ali Mirza, Q., Assam, M., Ismail, E. A. A., & Abonazel, M. R. (2023). How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan. *Heliyon*, *9*(12), e22823. <https://doi.org/10.1016/j.heliyon.2023.e22823>

Kirubavathi, G., Regis Anne, W., & Sridevi, U. K. (2024). A recent review of ransomware attacks on healthcare industries. *International Journal of System Assurance Engineering and Management*, *15*. <https://doi.org/10.1007/s13198-024-02496-4>

Kolade, T. M., Obioha-Val, O. A., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security. *Asian Journal of Research in Computer Science*, *18*(1), 133–153. <https://doi.org/10.9734/ajrcos/2025/v18i1554>

Lavoipierre, A. (2024). MediSecure “not in a financial position” to identify 12.9m Australians who had data stolen. *ABC News*. <https://www.abc.net.au/news/2024-07-18/medisecure-data-cyber-hack-12-million/104112736>

Markey, M. (2022). Ransomware: To Pay, or Not to Pay—That Is (One) Question. *Springer EBooks*, 159–190. <https://doi.org/10.1007/978-3-030-93592-4_8>

Nahar, N., Andersson, K., Schelén, O. S., & Saguna, S. (2024). A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks. *IEEE Access*, *12*, 94753–94764. <https://doi.org/10.1109/access.2024.3425350>

National Coordinator for Health Information Technology. (2025). *US: Health Information and Communication Technologies*. National Trends in Hospital and Physician Adoption of Electronic Health Records,’ Health IT Quick-Stat #61. <https://healthsystemsfacts.org/the-us-health-system/health-information-and-communications-technologies/>

Nazir, A., He, J., Zhu, N., Wajahat, A., Ullah, F., Qureshi, S., Ma, X., & Pathan, M. S. (2024). Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration. *Journal of King Saud University - Computer and Information Sciences*, *36*(2), 101939. <https://doi.org/10.1016/j.jksuci.2024.101939>

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>

NIST. (2018). The CSF 1.1 Five Functions. *NIST*. <https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions>

Obioha-Val, O. A. (2025). Bridging Gaps in Cybersecurity Governance: Leveraging Collaborative Digital Solutions. *Asian Journal of Research in Computer Science*, *18*(2), 82–100. <https://doi.org/10.9734/ajrcos/2025/v18i2564>

Obioha-Val, O. A., Gbadebo, M. O., Olaniyi, O. O., Chinye, N. C., & Balogun, A. Y. (2025). Innovative Regulation of Open Source Intelligence and Deepfakes AI in Managing Public Trust. *Journal of Engineering Research and Reports*, *27*(2), 136–156. <https://doi.org/10.9734/jerr/2025/v27i21400>

Obioha-Val, O. A., Lawal, T. I., Olaniyi, O. O., Gbadebo, M. O., & Olisa, A. O. (2025). Investigating the Feasibility and Risks of Leveraging Artificial Intelligence and Open Source Intelligence to Manage Predictive Cyber Threat Models. *Journal of Engineering Research and Reports*, *27*(2), 10–28. <https://doi.org/10.9734/jerr/2025/v27i21390>

Obioha-Val, O. A., Olaniyi, O. O., Gbadebo, M. O., Balogun, A. Y., & Olisa, A. O. (2025). Cyber Espionage in the Age of Artificial Intelligence: A Comparative Study of State-Sponsored Campaign. *Asian Journal of Research in Computer Science*, *18*(1), 184–204. <https://doi.org/10.9734/ajrcos/2025/v18i1557>

Olutimehin, A. T. (2025a). Advancing Cloud Security in Digital Finance: AI-Driven Threat Detection, Cryptographic Solutions, and Privacy Challenges. *Journal of Engineering Research and Reports*, *27*(3), 35–55. <https://doi.org/10.9734/jerr/2025/v27i31416>

Olutimehin, A. T. (2025b). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and its Applicability to Decentralized Finance (DeFi). *Asian Journal of Research in Computer Science*, *18*(3), 130–151. <https://doi.org/10.9734/ajrcos/2025/v18i3583>

Olutimehin, A. T. (2025c). The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms. *Asian Journal of Research in Computer Science*, *18*(3), 190–212. <https://doi.org/10.9734/ajrcos/2025/v18i3586>

Olutimehin, A. T., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., Oladoyinbo, T. O., & Olaniyi, O. O. (2025). Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures. *Journal of Engineering Research and Reports*, *27*(2), 341–362. <https://doi.org/10.9734/jerr/2025/v27i21413>

Özeren, S. (2025). *ALPHV Ransomware: Analyzing the BlackCat After Change Healthcare Attack*. Picussecurity.com; Picus Security. <https://www.picussecurity.com/resource/blog/alphv-ransomware>

Prasad, K., & Kumar, P. (2024). A Systematic Study on Ransomware Attack: Types, Phases and Recent Variants. *IEEE* . <https://doi.org/10.1109/icicv62344.2024.00110>

Riggi, J. (2024). *A Look at 2024’s Health Care Cybersecurity Challenges*. American Hospital Association | AHA News. <https://www.aha.org/news/aha-cyber-intel/2024-10-07-look-2024s-health-care-cybersecurity-challenges>

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, *23*(8), 4060. <https://doi.org/10.3390/s23084060>

Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024a). Achieving Digital Resilience with Cybersecurity. *EAI/Springer Innovations in Communication and Computing*, 43–123. <https://doi.org/10.1007/978-3-031-53290-0_2>

Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024b). Navigating the Regulatory Landscape. *EAI/Springer Innovations in Communication and Computing*, 127–240. <https://doi.org/10.1007/978-3-031-53290-0_3>

Sharma, D. (2024). *67% of healthcare companies experienced ransomware attacks in 2024: Sophos*. Leaders Talk and Latest Tech News | CXO VOICE; CXO VOICE. <https://cxovoice.com/67-of-healthcare-companies-experienced-ransomware-attacks-in-2024-sophos/>

Sharma, D. P., Lashkari, A. H., & Parizadeh, M. (2024). Understanding Cybersecurity Management in Healthcare. In *Progress in IS*. Springer International Publishing. <https://doi.org/10.1007/978-3-031-68034-2>

Sophos. (2024). *Two-Thirds of Healthcare Organizations Hit by Ransomware – A Four-Year High, Sophos Survey Finds*. SOPHOS. <https://www.sophos.com/en-us/press/press-releases/2024/09/two-thirds-healthcare-organizations-hit-ransomware-four-year-high>

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the internet of healthcare things. *Digital Health*, *9*(1), 1–20. <https://doi.org/10.1177/20552076231177144>

Tham, I. (2018). *Singapore’s most serious cyber attack: How it unfolded*. The Straits Times; The Straits Times. <https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html>

Trader, E., & Gurupur, V. (2024). Real-Time Tracking of Misdiagnosis in Electronic Health Records for Improved Predictive Modeling. *IEEE* . <https://doi.org/10.1109/southeastcon52093.2024.10500025>

U.S. Department of Health and Human Services. (2017). *HITECH Act Enforcement Interim Final Rule*. US Department of Health and Human Services. <https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html>

Uberoi, A. (2022). *How a Ransomware Attack on Synnovis led to chaos at NHS UK: A Timeline*. Cm-Alliance.com. <https://www.cm-alliance.com/cybersecurity-blog/how-a-ransomware-attack-on-synnovis-led-to-chaos-at-nhs-uk-a-timeline>

Wang, E., Tayebi, P., & Song, Y.-T. (2023). Cloud-Based Digital Twins’ Storage in Emergency Healthcare. *International Journal of Networked and Distributed Computing*, *11*(2). <https://doi.org/10.1007/s44227-023-00011-y>

Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. *Health Economics and Management Review*, *4*(4), 17–27. <https://doi.org/10.21272/hem.2023.4-02>

Yeboah-Ofori, A., & Opoku-Boateng, F. A. (2023). Mitigating cybercrimes in an evolving organizational landscape. *Continuity & Resilience Review*, *5*(1). <https://doi.org/10.1108/crr-09-2022-0017>

Zerbe, Y. (2023). *Costa Rica ransomware attack (2022)*. International Cyber Law: Interactive Toolkit. [https://cyberlaw.ccdcoe.org/wiki/Costa\_Rica\_ransomware\_attack\_(2022)](https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_%282022%29)