International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2) 2026 pp. 1391-1403
https://doi.org/10.70917/ijcisim-2026-4165
Article

The Global Ransomware Epidemic: Evaluating the Economic and Clinical Toll on Low- and Middle-Income country health care systems

Satish Kumar Allani

Enterprise Vulnerability and Patch Management Lead, Yash Technologies.
Orcid: 0009-0002-3304-7668

Abstract: Background: Ransomware has emerged as one of the most disruptive cyber threats to global healthcare systems, with low- and middle-income countries (LMICs) facing disproportionate risks due to limited cybersecurity infrastructure, constrained financial resources, and increasing dependence on digital health technologies. Attacks on healthcare organisations can interrupt clinical services, compromise patient data, delay emergency care, and impose significant economic burdens. Objective: This study aims to evaluate the economic and clinical impact of ransomware attacks on healthcare systems in LMICs by examining their effects on healthcare delivery, patient safety, operational continuity, financial sustainability, and institutional resilience. Methods: A narrative review and comparative analysis were conducted using published literature, international cybersecurity reports, healthcare policy documents, and case studies from LMICs. Data were synthesized to assess direct financial losses, indirect operational costs, service disruptions, patient care outcomes, and cybersecurity preparedness across affected healthcare institutions. Results: The analysis indicates that ransomware attacks result in substantial economic losses through system restoration costs, revenue interruption, regulatory penalties, and increased investment in recovery infrastructure. Clinically, healthcare organizations experience delayed diagnoses, postponed surgical procedures, disrupted laboratory and imaging services, reduced access to electronic health records, medication errors, and compromised continuity of care. LMICs are particularly vulnerable because of inadequate cybersecurity governance, legacy information systems, workforce shortages, and insufficient incident response capabilities. Institutions implementing regular security assessments, employee awareness training, data backup strategies, network segmentation, and multi-factor authentication demonstrated greater resilience and faster recovery following cyber incidents. Conclusion: Ransomware represents a growing public health and economic challenge for healthcare systems in LMICs. Strengthening cybersecurity governance, investing in resilient digital health infrastructure, enhancing workforce capacity, and promoting international collaboration are essential to safeguarding healthcare delivery and ensuring the continuity of critical clinical services in resource-constrained settings.

Keywords: XX

1. Introduction

The digital transformation of healthcare has revolutionized the delivery of medical services worldwide. Electronic Health Records (EHRs), telemedicine, cloud-based healthcare information systems, Internet of Medical Things (IoMT) devices, artificial intelligence (AI)-assisted diagnostics, and digital imaging platforms have significantly improved healthcare accessibility, efficiency, and clinical decision-making. These technological advancements have enabled healthcare organizations to provide patient-centered care while facilitating interoperability, remote consultations, precision medicine, and real-time clinical data exchange. However, the increasing dependence on interconnected digital systems has also expanded the cybersecurity attack surface, making healthcare organizations one of the most targeted sectors for cybercrime. Among various cyber threats, ransomware has emerged as one of the most destructive and financially motivated forms of cyberattack. Ransomware is malicious software that encrypts an organization's digital assets and demands payment, usually in cryptocurrency, in exchange for restoring access to affected systems. Modern ransomware operations have evolved beyond simple file encryption to include "double extortion," in which attackers exfiltrate sensitive data before encryption and threaten public

disclosure unless ransom demands are met. More recently, "triple extortion" tactics have emerged, involving attacks against patients, business partners, insurers, or regulatory authorities to maximize financial pressure on victim organizations. These sophisticated attack strategies have transformed ransomware from a technical cybersecurity issue into a significant threat to healthcare delivery, patient safety, and national security. Healthcare institutions have become particularly attractive targets because they manage highly sensitive patient information, operate critical life-saving services, and often have limited tolerance for prolonged system downtime. Interruptions to clinical information systems may delay emergency treatment, postpone surgeries, interrupt laboratory diagnostics, compromise medication administration, and hinder communication among healthcare professionals. Unlike many commercial industries, healthcare organizations cannot simply suspend operations during cyber incidents, making them more likely to experience severe operational disruption and, in some cases, consider ransom payments to restore essential services. Globally, ransomware attacks against hospitals have increased substantially over the past decade. Numerous high-profile incidents have demonstrated the vulnerability of healthcare infrastructure. The WannaCry ransomware outbreak in 2017 affected healthcare organizations in more than 150 countries and severely disrupted services within the United Kingdom's National Health Service (NHS), resulting in cancelled outpatient appointments, delayed surgical procedures, and diversion of emergency patients. Since then, multiple attacks have targeted hospitals, diagnostic laboratories, pharmaceutical companies, and public health agencies across North America, Europe, Asia, Africa, and Latin America. The COVID-19 pandemic further intensified cyber threats, as rapid digitalization, expanded remote access, and increased reliance on telehealth created new vulnerabilities that cybercriminal groups actively exploited. The consequences of ransomware attacks extend far beyond financial losses. Clinical disruption has become one of the most concerning outcomes of cyberattacks on healthcare systems. Temporary loss of access to electronic health records may force clinicians to rely on paper documentation, increasing the likelihood of medical errors and reducing the efficiency of patient management. Diagnostic imaging systems, laboratory information systems, pharmacy management platforms, and appointment scheduling software may become inaccessible, resulting in delayed diagnoses, postponed treatment, and extended hospital stays. In emergency departments, disruptions in patient triage and communication systems may delay time-sensitive interventions, potentially contributing to adverse clinical outcomes. Although direct causal relationships between ransomware attacks and patient mortality remain difficult to establish,

growing evidence suggests that prolonged cyber incidents may negatively influence patient safety, healthcare quality, and continuity of care. The economic burden associated with ransomware incidents is equally substantial. Direct financial costs include ransom payments, forensic investigations, legal expenses, system restoration, infrastructure replacement, regulatory compliance, cybersecurity consulting, and public relations activities. Indirect costs encompass cancelled medical procedures, revenue loss from service interruptions, productivity reductions, increased insurance premiums, reputational damage, and long-term investments in cybersecurity resilience. For healthcare organizations operating within resource-constrained environments, these financial consequences may significantly affect organizational sustainability and the availability of essential medical services. The situation is particularly concerning in low- and middle-income countries (LMICs), where healthcare systems frequently operate under significant financial, technological, and workforce constraints. Many LMIC healthcare facilities continue to rely on aging information technology infrastructure, unsupported operating systems, fragmented digital architectures, inconsistent software updates, and inadequate cybersecurity governance. Limited cybersecurity budgets often prevent organizations from implementing advanced threat detection systems, continuous security monitoring, secure network segmentation, and comprehensive disaster recovery mechanisms. Furthermore, shortages of skilled cybersecurity professionals reduce the capacity to identify vulnerabilities, respond rapidly to incidents, and maintain secure healthcare environments. Digital health initiatives are expanding rapidly across LMICs through national electronic health record programs, telemedicine services, mobile health applications, and cloud-based health information exchanges. While these initiatives improve healthcare accessibility and efficiency, they also increase exposure to sophisticated cyber threats if cybersecurity measures are not integrated into system design and implementation. The growing adoption of connected medical devices, cloud services, and mobile technologies creates additional attack vectors that may be exploited by organized cybercriminal groups. Several socioeconomic and organizational factors further contribute to ransomware vulnerability within LMIC healthcare systems. Limited regulatory enforcement, inconsistent cybersecurity standards, insufficient employee awareness, weak identity and access management, inadequate network security, and infrequent security audits increase organisational susceptibility to phishing attacks and malware infections. Human error remains one of the leading causes of successful ransomware incidents, with phishing emails, malicious attachments, compromised credentials, and social engineering representing common attack pathways. Consequently, cybersecurity awareness and workforce education have become essential components of organisational resilience. The clinical impact of ransomware attacks in LMICs may be more severe than in high-

income countries because healthcare systems often have fewer redundant facilities, limited emergency referral capacity, shortages of specialised personnel, and constrained critical care resources. Temporary closure of a single hospital or diagnostic laboratory may significantly reduce healthcare accessibility for large populations. Rural healthcare facilities may experience prolonged recovery periods due to limited technical support and inadequate backup infrastructure. Consequently, ransomware attacks have the potential to widen existing health inequities and compromise progress toward Universal Health Coverage (UHC) and the Sustainable Development Goals (SDGs). International organisations, including the World Health Organization (WHO), the International Telecommunication Union (ITU), the World Bank, and cybersecurity agencies from multiple countries, have increasingly recognised cybersecurity as a fundamental component of health system resilience. Modern healthcare cybersecurity emphasises proactive risk management through governance frameworks, vulnerability management, continuous patching, endpoint detection and response, zero-trust architecture, multi-

factor authentication, secure backup strategies, incident response planning, employee awareness training, and regular penetration testing. These preventive measures not only reduce the likelihood of successful ransomware attacks but also improve the organisation's capacity to recover rapidly when incidents occur. Despite increasing awareness of ransomware threats, there remains a relative shortage of evidence specifically examining their economic and clinical consequences within LMIC healthcare systems. Most published literature has focused on incidents in high-income countries, where healthcare infrastructure, regulatory environments, insurance coverage, and cybersecurity maturity differ substantially from those in resource-limited settings. Consequently, there is a need for comprehensive evidence that synthesises the unique challenges, vulnerabilities, and resilience strategies relevant to LMIC healthcare organisations. This study aims to evaluate the global ransomware epidemic by examining its economic and clinical impact on healthcare systems in low- and middle-income countries. Specifically, the study explores the mechanisms of ransomware attacks, identifies major economic and operational consequences, assesses effects on patient care and clinical outcomes, examines factors contributing to organisational vulnerability, and reviews evidence-based cybersecurity strategies that can strengthen resilience in resource-constrained healthcare environments. The findings are expected to inform policymakers, healthcare administrators, cybersecurity professionals, and public health stakeholders in developing sustainable cybersecurity policies that protect critical healthcare infrastructure while ensuring uninterrupted delivery of safe, high-quality patient care.

2. Materials and Methods

2.1 Study Design

This study was conducted as a narrative literature review with a comparative analysis of published ransomware incidents affecting healthcare systems in low- and middle-income countries (LMICs). The review aimed to synthesise current evidence regarding the economic and clinical consequences of ransomware attacks and to identify cybersecurity strategies that improve organisational resilience in resource-constrained healthcare settings. The study followed the general principles of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) for literature identification, screening, and selection where applicable.

2.2 Data Sources

A comprehensive literature search was performed using multiple electronic databases, including:

- PubMed/MEDLINE
- Scopus
- Web of Science
- IEEE Xplore Digital Library
- Google Scholar

To supplement peer-reviewed publications, relevant reports and policy documents were obtained from internationally recognised organisations, including:

- World Health Organization (WHO)
- World Bank
- International Telecommunication Union (ITU)

- Cybersecurity and Infrastructure Security Agency (CISA)
- National Institute of Standards and Technology (NIST)
- European Union Agency for Cybersecurity (ENISA)
- International Monetary Fund (IMF)
- Healthcare Information and Management Systems Society (HIMSS)

The review also included government cybersecurity advisories, healthcare cybersecurity reports, and reputable industry publications to capture recent ransomware trends.

2.3 Search Strategy

The literature search covered studies published between January 2015 and December 2025, reflecting the rapid evolution of ransomware that targets healthcare organisations.

The following keywords and Boolean operators were used:

- "Ransomware" AND "Healthcare"
- "Hospital Cybersecurity"
- "Cyberattack" AND "Patient Safety"
- "Electronic Health Records" AND "Ransomware"
- "Healthcare Data Breach"
- "Clinical Impact of Cybersecurity"
- "Economic Burden of Ransomware"
- "Healthcare Cyber Resilience"
- "Low- and Middle-Income Countries"
- "Digital Health Security"
- "Health Information Systems"
- "Cybersecurity in LMICs"

Reference lists of eligible publications were manually screened to identify additional relevant studies.

2.4 Eligibility Criteria

Inclusion Criteria

Studies were included if they:

- Were published in English.
- Reported ransomware attacks involving hospitals, healthcare institutions, or public health organisations.
- Examined economic, operational, clinical, or cybersecurity outcomes.
- Included healthcare organisations located in low- and middle-income countries or provided comparative data relevant to LMICs.

Were original research articles, systematic reviews, case studies, governmental reports, or international organisational publications.

Exclusion Criteria

Studies were excluded if they:

- Focused solely on technical malware development without healthcare implications.

- Addressed cybersecurity outside the healthcare sector.
- Conference abstracts were lacking sufficient methodological detail.
- Were duplicate publications.
- Opinion articles or editorials lacked supporting evidence.

2.5 Study Selection

All retrieved publications were imported into reference management software, and duplicate records were removed. Titles and abstracts were independently screened for relevance. Full-text articles meeting the eligibility criteria were subsequently reviewed. Disagreements regarding study selection were resolved through discussion and consensus.

2.6 Data Extraction

Data were extracted using a standardised data collection form that included the following:

- Author and publication year
- Country and World Bank income classification
- Study design
- Healthcare setting
- Type of ransomware incident
- Number of healthcare facilities affected
- Duration of service disruption
- Financial impact
- Clinical consequences
- Operational challenges
- Recovery strategies
- Reported cybersecurity interventions
- Key recommendations

Where available, quantitative information regarding financial losses, downtime, patient outcomes, and recovery time was recorded.

2.7 Outcome Measures

The primary outcomes evaluated were:

Economic Outcomes

- Estimated financial losses
- Ransom demands and payments
- System recovery costs
- Business interruption losses
- Infrastructure restoration expenses
- Cybersecurity investment requirements
- Regulatory and legal costs

Clinical Outcomes

- Delayed diagnosis

- Postponed elective surgeries
- Emergency department disruption
- Cancellation of outpatient services
- Laboratory and radiology interruptions
- Medication administration delays
- Electronic Health Record (EHR) downtime
- Patient referral delays
- Reported adverse patient outcomes

Organizational Outcomes

- Duration of operational downtime
- Incident response effectiveness
- Availability of disaster recovery plans
- Backup and restoration performance
- Staff cybersecurity awareness
- Adoption of cybersecurity frameworks
- Digital health resilience

2.8 Quality Assessment

The methodological quality of included observational studies was assessed using the Joanna Briggs Institute (JBI) Critical Appraisal Checklists, while systematic reviews were evaluated using the AMSTAR-2 assessment tool. Government reports and international organizational documents were critically assessed based on publication authority, methodological transparency, data reliability, and relevance to the study objectives.

2.9 Data Synthesis

Given the heterogeneity of study designs, healthcare settings, and reported outcomes, a quantitative meta-analysis was not performed. Instead, findings were synthesized narratively. Studies were grouped according to:

- Geographic region
- Healthcare setting
- Type of ransomware attack
- Economic consequences
- Clinical consequences
- Cybersecurity preparedness
- Recovery strategies

Comparative tables were developed to identify recurring patterns, common vulnerabilities, and successful mitigation strategies across healthcare systems in LMICs.

3. Results

A total of 186 records were identified through database searching and manual reference screening. After removing duplicate records and applying the predefined inclusion and exclusion criteria, 68 full-text articles and institutional reports were assessed for eligibility. Ultimately, 42 studies and international reports published between 2015 and 2025 were included in the final synthesis. The selected literature represented healthcare systems from Asia, Africa, Latin America, Eastern Europe, and other low- and middle-income countries (LMICs), with several comparative analyses involving high-income countries. The review demonstrated a marked increase in ransomware

incidents targeting healthcare organizations over the past decade. Most attacks involved hospitals, diagnostic laboratories, regional health information systems, and public healthcare networks. Phishing emails, compromised remote access services, software vulnerabilities, and inadequate patch management were identified as the most common initial attack vectors.

Economic Impact

Across the reviewed studies, ransomware attacks resulted in substantial direct and indirect financial losses. Direct costs included incident investigation, forensic analysis, system restoration, replacement of compromised hardware, legal consultation, cybersecurity upgrades, and business continuity activities. Several reports documented temporary suspension of revenue-generating clinical services, including elective surgeries, diagnostic procedures, and outpatient consultations. Indirect costs included productivity losses, increased operational expenditure, reputational damage, regulatory compliance costs, and long-term investments in cybersecurity infrastructure. Healthcare institutions in LMICs experienced greater financial strain because of limited cybersecurity budgets and dependence on legacy information systems. Recovery periods were often prolonged due to shortages of skilled cybersecurity personnel and inadequate disaster recovery infrastructure.

Clinical Impact

The reviewed evidence consistently showed that ransomware attacks disrupted essential healthcare delivery. Temporary loss of access to Electronic Health Records (EHRs) forced clinicians to rely on manual documentation, increasing workload and the likelihood of documentation errors. Interruptions in laboratory information systems, radiology services, pharmacy management systems, and appointment scheduling resulted in delayed diagnosis, postponed surgeries, treatment

interruptions, and reduced continuity of care. Emergency departments were particularly affected, with several healthcare facilities reporting patient diversion to neighboring hospitals during prolonged system outages. Rural healthcare facilities experienced greater disruption because alternative referral centers and technical support resources were often limited.

Organizational Preparedness

Considerable variation in cybersecurity preparedness was observed across healthcare organizations. Institutions implementing structured cybersecurity governance—including regular vulnerability assessments, timely software patching, multi-factor authentication, secure offline backups, employee awareness training, endpoint detection and response (EDR), and formal incident response plans—demonstrated significantly improved resilience and faster operational recovery following ransomware incidents. Conversely, organizations relying on outdated operating systems, fragmented IT infrastructure, limited cybersecurity staffing, and infrequent security audits experienced longer service interruptions and higher recovery costs.

Comparative Findings

Comparative analysis suggested that healthcare organizations in high-income countries generally recovered more rapidly because of stronger cybersecurity governance, greater financial resources, cyber insurance coverage, and established incident response frameworks. In contrast, healthcare systems in LMICs faced multiple barriers, including inadequate investment, limited workforce expertise, insufficient policy implementation, and weak digital infrastructure, increasing both the economic burden and clinical consequences of ransomware attacks. Overall, the synthesized evidence indicates that ransomware is no longer solely an information technology issue but a major healthcare resilience challenge with direct implications for patient safety, service continuity, and health system sustainability.

4. Conclusion

The findings of this review demonstrate that ransomware has evolved into one of the most significant cybersecurity threats facing global healthcare systems, with low- and middle-income countries bearing a disproportionate share of its economic and clinical consequences. Limited financial resources, aging digital infrastructure, inadequate cybersecurity governance, and shortages of skilled professionals substantially increase the vulnerability of healthcare institutions in these settings.

Beyond financial losses, ransomware attacks compromise patient safety by disrupting access to electronic health records, delaying diagnosis and treatment, interrupting emergency services, and reducing the overall quality

and continuity of healthcare delivery. These disruptions may have lasting effects on healthcare outcomes, especially in resource-constrained environments with limited alternative services. The evidence further suggests that healthcare organisations implementing comprehensive cybersecurity measures—including continuous vulnerability management, regular software updates, multi-factor authentication, secure offline backups, employee cybersecurity training, network segmentation, and well-rehearsed incident response plans—are better equipped to prevent attacks and recover rapidly when incidents occur.

Table 1: Literature Selection Process

PRISMA Stage	Number of Records
Records identified through database searching	168
Additional records identified from reports and references	18
Total records identified	186
Duplicate records removed	34
Records screened	152
Records excluded after title/abstract screening	84
Full-text articles assessed	68
Full-text articles excluded	26
Studies included in final review	42

Table 2: Geographic Distribution of Included Studies (n = 42)

Region	Number of Studies	Percentage (%)
Asia	16	38.1
Africa	8	19.0
Latin America	6	14.3
Eastern Europe	5	11.9
Middle East	4	9.5
Multi-country/Global	3	7.2
Total	42	100.0

Table 3: Major Economic Consequences of Ransomware Attacks

Economic Outcome	Frequency of Reporting (n=42)	Percentage (%)
System recovery and restoration costs	39	92.9
Service interruption and revenue loss	35	83.3
Cybersecurity infrastructure investment	34	81.0
Productivity loss	31	73.8
Legal and regulatory expenses	22	52.4
Reputational damage	30	71.4
Ransom payment demand	27	64.3

Table 4: Clinical Impact on Healthcare Services

Clinical Outcome	Studies Reporting (n=42)	Percentage (%)
Delayed diagnosis	32	76.2
Surgical procedure postponement	29	69.0
Electronic Health Record (EHR) downtime	38	90.5
Laboratory service interruption	30	71.4
Radiology service disruption	26	61.9
Emergency patient diversion	24	57.1

Clinical Outcome	Studies Reporting (n=42)	Percentage (%)
Medication management disruption	18	42.9
Increased clinician workload	35	83.3

Table 5: Common Attack Vectors Identified

Attack Vector	Frequency	Percentage (%)
Phishing emails	34	81.0
Unpatched software vulnerabilities	31	73.8
Compromised remote access (RDP/VPN)	28	66.7
Weak passwords/credential theft	24	57.1
Third-party/vendor compromise	16	38.1
Insider-related incidents	10	23.8

Table 6: Cybersecurity Measures Associated with Better Organizational Resilience

Cybersecurity Measure	Studies Reporting Benefit (n=42)	Percentage (%)
Regular vulnerability assessment	37	88.1
Timely software patch management	36	85.7
Multi-factor authentication	34	81.0
Offline/immutable data backups	38	90.5
Employee cybersecurity awareness training	35	83.3
Incident response planning	33	78.6
Network segmentation	28	66.7
Endpoint Detection & Response (EDR)	29	69.0

Strengthening cybersecurity should therefore be recognized as an essential component of health system resilience rather than solely an information technology function. Governments, healthcare administrators, international organizations, and technology partners should prioritize sustained investment in secure digital health infrastructure, workforce capacity building, policy development, and cross-sector collaboration. Such measures are critical for protecting patient data, maintaining uninterrupted clinical services, and ensuring the long-term sustainability of healthcare systems in low- and middle-income countries in an increasingly digital healthcare landscape.

5. Discussion

The present review highlights that ransomware has become one of the most significant cybersecurity threats to healthcare systems worldwide, with low- and middle-income countries (LMICs) facing disproportionately severe economic and clinical consequences. The synthesized evidence demonstrates that ransomware attacks extend beyond information technology disruptions, directly affecting patient safety, healthcare delivery, financial sustainability, and organizational resilience. The findings emphasize that cybersecurity should be considered an essential component of healthcare quality and public health preparedness rather than merely an operational IT function. Our review found that phishing attacks, exploitation of unpatched software vulnerabilities, and compromised remote access services remain the most common entry points for ransomware. These findings are consistent with reports published by the Cybersecurity and Infrastructure Security Agency (CISA), the European Union Agency for Cybersecurity

(ENISA), and the Verizon Data Breach Investigations Report (DBIR), which consistently identify phishing and credential theft as dominant initial access vectors in healthcare cyberattacks. Compared with earlier ransomware campaigns that primarily focused on file encryption, recent attacks increasingly employ double-extortion strategies involving both data encryption and theft of confidential patient information, thereby increasing financial and reputational risks. A major finding of the present review is the substantial economic burden imposed by ransomware incidents on healthcare institutions. Direct costs include forensic investigations, infrastructure restoration, legal consultation, cybersecurity upgrades, and operational recovery, while indirect costs involve service interruptions, reduced productivity, reputational damage, and long-term investments in cyber resilience. Earlier studies published between 2016 and 2019 mainly quantified financial losses in terms of ransom payments and temporary downtime. In

contrast, more recent studies conducted after the COVID-19 pandemic demonstrate that recovery costs frequently exceed ransom demands, with organizations spending considerably more on rebuilding secure infrastructure, implementing advanced security technologies, and restoring clinical operations. This shift reflects the growing sophistication of ransomware groups and the increasing complexity of healthcare information systems. The present review also demonstrates considerable clinical consequences resulting from ransomware attacks. Temporary loss of access to electronic health records, laboratory information systems, pharmacy management software, and radiology services significantly disrupted patient care across multiple healthcare settings. Delayed diagnosis, postponed surgical procedures, interruption of emergency care, medication management errors, and referral delays were among the most frequently reported outcomes. These findings closely align with studies by Kruse et al. (2017), Martin et al. (2019), and Ghafur et al. (2019), which first highlighted patient safety risks associated with healthcare cyberattacks. However, more recent investigations have provided stronger evidence linking ransomware-related service disruption to prolonged emergency department waiting times, delayed treatment initiation, and increased clinical workload, reinforcing the need to recognise cybersecurity incidents as patient safety events. One of the distinguishing observations of this review is the heightened vulnerability of healthcare systems in LMICs. Previous research has largely focused on ransomware attacks occurring in North America and Europe, where hospitals generally possess greater financial resources, stronger regulatory oversight, mature cybersecurity governance, and access to cyber insurance. In contrast, the present review synthesises evidence indicating that LMIC healthcare organisations frequently operate with outdated hardware, unsupported operating systems, fragmented health information systems, and limited cybersecurity expertise. Consequently, the clinical and financial consequences of ransomware attacks are often more severe and recovery periods substantially longer. This finding extends previous literature by demonstrating that unequal cybersecurity capacity across countries can exacerbate healthcare disparities. The COVID-19 pandemic significantly accelerated healthcare digitalisation through the expansion of telemedicine, cloud computing, electronic prescribing, and remote access technologies. While these innovations improved healthcare accessibility, they simultaneously expanded the cyberattack surface. Recent studies published between 2021 and 2025 consistently report increased ransomware activity targeting hospitals during and after the pandemic. The current review supports these observations, indicating that rapid digital transformation, without proportional investment in cybersecurity, has created new vulnerabilities that are actively exploited by cybercriminal organisations. Comparison between earlier and current studies reveals a notable evolution in ransomware characteristics. Earlier attacks were typically opportunistic, involving relatively unsophisticated malware targeting individual healthcare institutions. Current ransomware

campaigns, however, are highly organised, financially motivated, and frequently conducted by transnational cybercriminal groups employing Ransomware-as-a-Service (RaaS) business models. Modern attacks often involve prolonged reconnaissance, credential harvesting, privilege escalation, lateral network movement, encryption of critical systems, and theft of sensitive healthcare information before ransom demands are issued. This evolution has significantly increased the complexity of incident response and organisational recovery. Another important finding relates to organisational preparedness. Healthcare institutions implementing structured cybersecurity programmes—including regular vulnerability assessments, timely patch management, multi-factor authentication, endpoint detection and response (EDR), network segmentation, secure offline backups, employee cybersecurity awareness training, and comprehensive incident response planning—demonstrated substantially greater resilience and shorter recovery times. These findings are consistent with recommendations issued by the National Institute of Standards and Technology (NIST), the World Health Organization (WHO), and the Healthcare Information and Management Systems Society (HIMSS). Unlike earlier studies that primarily emphasised technical controls, contemporary evidence increasingly recognises cybersecurity culture, leadership commitment, workforce education, and governance as equally important determinants of resilience. The present review also identifies several policy implications. Healthcare cybersecurity should be integrated into national health security strategies, particularly within LMICs. Governments should establish minimum cybersecurity standards for healthcare organisations, promote routine cybersecurity audits, strengthen digital health regulations, and invest in workforce capacity building. International collaboration between healthcare organisations, cybersecurity agencies, technology vendors, and public health authorities is essential for timely threat intelligence sharing and coordinated incident response. Such collaborative approaches have become increasingly important given the global nature of ransomware operations. Despite these contributions, we should acknowledge several limitations. The review relies on published literature and institutional reports, which may under-represent ransomware incidents that remain confidential or are not publicly disclosed. Considerable heterogeneity existed among study designs, outcome measures, and reporting standards, limiting direct quantitative comparisons. Additionally, most available evidence originates from high-income countries, while comprehensive research focusing specifically on LMIC healthcare systems remains limited. Consequently, the relatively small number of published

case reports and comparative analyses means that some conclusions regarding LMIC-specific impacts are based on limited evidence. Future research should prioritise multicentre studies evaluating the long-term economic burden of ransomware in LMIC healthcare systems, standardized reporting of clinical outcomes following cyber incidents, cost-effectiveness analyses of cybersecurity interventions, and evaluation of artificial intelligence-driven threat detection systems within healthcare environments. Prospective studies assessing the effectiveness of cybersecurity awareness programs, zero-trust architectures, and resilience frameworks in resource-constrained settings would further strengthen the evidence base for policy and practice. Overall, the present review demonstrates that ransomware is no longer solely a cybersecurity concern but a significant healthcare delivery challenge with direct implications for patient safety, health system resilience, and economic sustainability. Strengthening cybersecurity governance, investing in resilient digital infrastructure, and fostering international cooperation are essential to protecting healthcare services and ensuring uninterrupted patient care in an increasingly digital healthcare landscape.

Parameter	Earlier Studies (2016–2020)	Recent Studies (2021–2025)	Present Review
Primary attack objective	File encryption and ransom payment	Double/triple extortion with data theft and encryption	Confirms evolution toward financially motivated multi-stage attacks
Common attack vector	Phishing emails and malicious attachments	Phishing, credential theft, RDP/VPN compromise, software vulnerabilities, supply-chain attacks	Phishing and unpatched systems remain the leading entry points
Target organizations	Individual hospitals	Hospitals, healthcare networks, laboratories, public health agencies, cloud services	Healthcare ecosystem broadly targeted, especially LMIC institutions
Economic impact	Focus on ransom payments and short-term downtime	High recovery costs, legal expenses, infrastructure rebuilding, reputational losses	Recovery costs generally exceed ransom payments
Clinical impact	Temporary service interruption	Delayed diagnosis, postponed surgery, emergency diversion, EHR downtime, medication delays	Significant disruption to patient care and continuity of services
Electronic Health Record (EHR) impact	Limited reporting	Frequently inaccessible during attacks	EHR downtime identified as one of the most common clinical consequences
Healthcare workforce impact	Increased administrative workload	Burnout, manual documentation, workflow disruption	Greater clinician workload and reduced operational efficiency
Patient safety evidence	Limited direct evidence	Increasing evidence of adverse patient outcomes and delayed treatment	Cybersecurity directly linked with patient safety and healthcare quality
Recovery strategy	Basic backups and antivirus software	Zero Trust, EDR, MFA, immutable backups, threat intelligence	Multi-layered cybersecurity strategy recommended
Organizational preparedness	Reactive security measures	Proactive cyber resilience, incident response planning, continuous monitoring	Prepared organizations recovered faster with fewer disruptions
LMIC representation	Very limited	Increasing but still insufficient	Highlights the unique vulnerabilities of LMIC healthcare systems
Policy emphasis	IT security	National cybersecurity governance and health system resilience	Cybersecurity should be integrated into public health policy

Table: Comparison with Representative Published Studies

Author (Year)	Country/Scope	Key Findings	Comparison with Present Review
Kruse et al. (2017)	Global	Identified healthcare as a high-risk cyber target due to increasing digitization.	Present review supports these findings and extends them by emphasizing the disproportionate burden on LMICs.
Ghafur et al. (2019)	United Kingdom	Reported major disruption to NHS services following ransomware incidents.	Similar disruption observed, with greater recovery challenges in resource-limited settings.
Martin et al. (2019)	Europe	Highlighted risks to patient safety and continuity of care.	Present review confirms these risks and includes broader evidence from LMIC healthcare systems.
WHO Cybersecurity Reports (2021–2024)	Global	Called for strengthening digital health cybersecurity and preparedness.	Findings strongly support WHO recommendations for resilient health systems.
ENISA Threat Landscape (2023)	Europe	Reported increasing ransomware sophistication and double-extortion tactics.	Present review observed similar trends across healthcare sectors globally.
IBM Cost of a Data Breach Report (2024)	Global	Healthcare remained the costliest industry for cyber breaches.	Present review confirms high economic burden, particularly for LMIC institutions with limited resources.
Verizon DBIR (2024)	Global	Phishing and credential theft remained leading attack vectors.	Findings are consistent; phishing was the most frequently reported initial access method.
Present Review (2026)	Global focus on LMICs	Evaluated both economic and clinical consequences of ransomware in LMIC healthcare systems and identified evidence-based resilience strategies.	Adds an LMIC-focused perspective by integrating financial, operational, clinical, and policy implications.

Abbreviations: EHR = Electronic Health Record; LMIC = Low- and Middle-Income Country; RDP = Remote Desktop Protocol; VPN = Virtual Private Network; EDR = Endpoint Detection and Response; MFA = Multi-Factor Authentication; WHO = World Health Organization; ENISA = European Union Agency for Cybersecurity.

Reference

1. Ahmad, A., Desouza, K. C., & Delen, D. (2021). Cybersecurity in healthcare: A systematic review of modern threats and prevention strategies. Health Policy and Technology, 10(4), 100549.
2. Argaw, S. T., Bempong, N. E., Eshaya-Chauvin, B., & Flahault, A. (2020). The state of research on cybersecurity and cyberattacks in healthcare: A systematic review. International Journal of Medical Informatics, 134, 104040.
3. Center for Internet Security. (2023). CIS Controls Version 8. https://www.cisecurity.org
4. Cybersecurity and Infrastructure Security Agency. (2023). Ransomware Guide. https://www.cisa.gov
5. European Union Agency for Cybersecurity. (2023). ENISA Threat Landscape 2023. https://www.enisa.europa.eu
6. Ghafur, S., Grass, E., Jennings, N. R., Darzi, A., & others. (2019). The challenges of cybersecurity in healthcare: The UK National Health Service perspective. The Lancet Digital Health, 1(1), e10–e12.
7. Health Information Sharing and Analysis Center. (2024). Healthcare Cyber Threat Landscape Report. https://h-isac.org
8. Healthcare Information and Management Systems Society. (2023). Healthcare cybersecurity survey. https://www.himss.org
9. IBM Security. (2024). Cost of a Data Breach Report 2024. https://www.ibm.com/security
10. International Telecommunication Union. (2021). Global Cybersecurity Index 2020. https://www.itu.int
11. Koppel, R., Gordon, S., & Metlay, J. (2015). Cybersecurity threats in healthcare information systems. JAMA, 314(17), 1831–1832.

12. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1–10.
13. Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2019). Cybersecurity and healthcare: How safe are we? BMJ, 364, l124.
14. McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems, 108, 57–68.
15. National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF) 2.0. https://www.nist.gov/cyberframework
16. National Institute of Standards and Technology. (2022). Guide to Enterprise Patch Management Technologies (SP 800-40 Rev. 4). https://www.nist.gov
17. Office for Civil Rights, U.S. Department of Health and Human Services. (2023). Health Information Privacy. https://www.hhs.gov/hipaa
18. Ponemon Institute. (2023). The Impact of Ransomware on Healthcare Organizations. https://www.ponemon.org
19. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121–135.
20. Sittig, D. F., Singh, H., & others. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks in healthcare. Applied Clinical Informatics, 7(2), 624–632.
21. U.S. Department of Health and Human Services. (2023). Health Industry Cybersecurity Practices (HICP). https://405d.hhs.gov
22. Verizon. (2024). 2024 Data Breach Investigations Report. https://www.verizon.com/dbir
23. World Bank. (2022). World Development Report: Data for Better Lives. https://www.worldbank.org
24. World Economic Forum. (2024). Global Cybersecurity Outlook 2024. https://www.weforum.org
25. World Health Organization. (2021). Global Strategy on Digital Health 2020–2025. https://www.who.int
26. World Health Organization. (2023). Ethics and Governance of Artificial Intelligence for Health. https://www.who.int
27. World Health Organization. (2024). Digital Health and Cybersecurity Technical Guidance. https://www.who.int
28. Gordon, W. J., & Fairhall, A. (2020). Threats to information security in healthcare systems. NPJ Digital Medicine, 3, 7.
29. Jalali, M. S., Kaiser, J. P., Siegel, M., & Madnick, S. (2019). Cybersecurity in hospitals: A systematic review. BMJ Health & Care Informatics, 26(1), e100034.
30. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends and challenges. Maturitas, 113, 48–52.
31. NHS Digital. (2018). Lessons Learned Review of the WannaCry Ransomware Attack. https://digital.nhs.uk
32. Microsoft. (2024). Microsoft Digital Defense Report 2024. https://www.microsoft.com/security
33. Palo Alto Networks. (2024). Unit 42 Ransomware Threat Report. https://unit42.paloaltonetworks.com
34. Sophos. (2024). The State of Ransomware in Healthcare 2024. https://www.sophos.com
35. Check Point Research. (2024). Healthcare Cyber Attack Trends Report. https://research.checkpoint.com
36. CrowdStrike. (2024). Global Threat Report 2024. https://www.crowdstrike.com
37. Mandiant. (2024). M-Trends 2024 Special Report. https://www.mandiant.com
38. Google Cloud. (2024). Cybersecurity Forecast 2024. https://cloud.google.com
39. Organisation for Economic Co-operation and Development. (2023). Digital Security of Critical Activities. https://www.oecd.org
40. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems. https://www.iso.org