Volume 14 / **2026** ISSN 2344-102X
Issue **3** ISSN-L 2344-102X

ORGANIZATIONAL RESILIENCE: A META-ANALYTICAL FRAMEWORK FOR HEALTHCARE CYBERSECURITY (2021-2025)

Petronela Alice GRIGORESCU
Valahia University of Targoviste, 130004, Romania
alice.grigorescu@valahia.ro
ORCID: 0009-0006-2423-1825
Alexandru Cătălin NEAGU
Valahia University of Targoviste, 130004, Romania
alexandru.neagu.ct@valahia.ro
ORCID: 0009-0001-7547-9226
Dan Marius COMAN*
Valahia University of Targoviste, 130004, Romania
marius.coman@valahia.ro
ORCID:0000-0003-4937-6327
Mihaela Ionela SOCOLIUC
Stefan cel Mare University of Suceava, 720229, Romania
mihaela.socoliuc@usm.ro
ORCID: 0000-0002-7250-2304

Abstract
Healthcare institutions have become primary targets for organised cybercrime, with the period 2021-2025 marking a critical transition toward coordinated attacks combining data encryption and information exfiltration. This meta-analytical study analyses official reports from ENISA, CISA, NIST, Verizon, and IBM Security to identify predominant attack vectors, quantify financial and operational costs, and assess the clinical impact on patient safety. Cybersecurity incident costs increased 77% from 9.23 million USD in 2021 to 16.31 million USD in 2025, with business interruption rising from 25% to 48% of total damages. Supply chain attacks (32%) and IoMT exploitation (26%) together account for 58% of identified attack vectors, while legacy systems represent only 14%, invalidating the assumption that outdated infrastructure remains the primary vulnerability. Clinical indicators reveal severe consequences: triage accuracy decreased 15-25%, medical errors tripled, and 40-60% of surgical procedures were cancelled during incidents. AI-based defence systems reduced attack success rates from 65-75% to 20-30%. The findings reframe cybersecurity in healthcare as a patient safety issue rather than a purely technical problem, demonstrating that digital resilience requires Zero Trust architecture, proportional investment in both technology and human capital, and continuous strategic reassessment aligned with the evolving threat landscape.

Keywords: *Cybersecurity; Healthcare; IoMT; Patient safety; Ransomware*

JEL Classification: *I18, L86, O33*

Received on: September 10, 2026 **Accepted on:** October 8, 2026 **Published on:** October 12, 2026

INTRODUCTION

The digital transformation of healthcare systems has created an unprecedented condition in contemporary medicine, in which the effectiveness of clinical care has become inseparable from the integrity and availability of information infrastructure. Between 2021 and 2025, the large-scale integration of Internet of Medical Things (IoMT) devices, the adoption of electronic health records, and the expansion of telemedicine have delivered undeniable clinical benefits (Sophos, 2024), while simultaneously generating systemic vulnerabilities that hostile actors in the cyber environment have aggressively exploited (Kruse et al., 2017).

Cyberattacks on hospitals have long moved beyond data confidentiality alone. They have become a direct threat to human life. When a medical facility falls victim to a ransomware attack, the immediate consequences are severe: loss of access to patient medical histories, inability to retrieve laboratory results, and paralysis of triage systems. These effects amount to sabotage of the institution's capacity to respond to emergencies. In this context, cybersecurity is no longer an optional feature of hospital management; it is a core component of clinical resilience (Biffi, 2025).

The current threat environment is shaped by the proliferation of digital sabotage-as-a-service operations,

DOI: 10.4316/EJAFB. 2026.14303

Volume 14 / **2026** ISSN 2344-102X
Issue **3** ISSN-L 2344-102X

which use Ransomware-as-a-Service models to target healthcare institutions as high-pressure social leverage points (Novak, 2025). The period under analysis (2021 to 2025) reveals a troubling trajectory. While attacks in the early part of the decade were largely opportunistic, more recent data indicate coordinated, high-precision operations aimed not only at encrypting data but also at extracting sensitive information for extortion (Sophos, 2024).

What distinguishes this study is its integrated treatment of the post-pandemic period, which marks the transition towards AI-driven attacks and selective data exfiltration. Unlike earlier research focused primarily on financial losses (Gordon et al., 2011), this paper examines, from a multidimensional perspective, the intersection of cyber threats, operational disruption to medical services, and implications for the quality of care, reinforcing the concept of "medical information security" as a pillar of modern bioethics (Aliyu et al., 2024).

The literature consistently confirms that the healthcare sector has become the preferred target of cybercriminal activity. According to the annual IBM Security report (2024), the medical industry recorded the highest average cost of a data breach for the fourteenth consecutive year, reaching a record $10.93 million per incident. This vulnerability is compounded by the hybrid nature of hospital IT ecosystems, where the interconnection of legacy medical equipment with modern networks creates potential entry points (Mamuye et al., 2022). Unsecured peripheral devices serve as pivot points from which attackers can paralyse central databases.

Beyond the technical dimension, the literature identifies a shift towards the ethical and clinical aspects of digital security. Khadka and Ullah (2025) argue that protecting medical data is not merely a legal obligation but an intrinsic component of patient safety, demonstrating that the unavailability of IT systems during a ransomware attack directly affects mortality and medical error rates. This reality is compounded by the persistence of the human factor as the weakest link in the chain. The Verizon report (2023) found that over 74% of security breaches involve a human element, whether through error or psychological manipulation.

The European Union Agency for Cybersecurity has warned of emerging supply-chain vulnerabilities, noting that outsourcing cloud services creates dangerous cross-border dependencies that can compromise data confidentiality (ENISA, 2023). Artificial intelligence plays a dual role in healthcare cybersecurity. On the one hand, machine learning algorithms enable proactive, real-time detection of behavioural anomalies in hospital networks, allowing security incidents to be identified with minimal latency. On the other hand, recent literature documents the growing use of AI techniques to automate vulnerability scanning and orchestrate highly personalised phishing campaigns tailored to the dynamics of healthcare environments (Heartfield & Loukas, 2018; Lee et al., 2024; Flowerday et al., 2023). This duality reinforces the case for embedding a Security by Design approach in all medical information systems from the outset, treating security not as an add-on or corrective measure but as a native architectural feature built into systems from the earliest design stages (Sittig & Singh, 2010).

This article explores this evolution through a meta-analysis of official documents and security reports published over the past five years. The primary objective is to identify the dominant attack vectors, quantify the financial and operational impact on healthcare systems, and assess the effectiveness of current defensive strategies. By examining hypotheses at the intersection of outdated technology, human vulnerability, and emerging cyber-extortion strategies, the paper offers a rigorous perspective on how digital resilience can serve as a guarantor of patient safety in an era of total interconnectivity. The remainder of the article is structured as follows: Section 2 presents the literature review; Section 3 details the methodology and source selection criteria; Section 4 presents comparative results and an interpretive discussion of the key indicators; and the final section synthesises the conclusions and proposes strategic recommendations to improve cyber resilience in healthcare institutions.

I. LITERATURE REVIEW

The contemporary academic landscape supports the view that the healthcare sector has become the primary target of cybercriminal activity, having evolved from a systemic vulnerability into a global security crisis (Neprash et al., 2022). The literature reports that the medical industry recorded the highest average cost of a data breach for the fourteenth consecutive year, reaching a record $10.93 million per incident. This reflects a deep asymmetry between the pace of clinical digitalisation and the investments allocated to securing critical infrastructure (IBM Security, 2024; Portela et al., 2023). This vulnerability is compounded by the hybrid nature of hospital IT systems, where the interconnection of legacy medical equipment with modern networks creates gaps in digital defences. Unsecured peripheral devices serve as entry points for compromising databases (Mamuye et al., 2022).

Beyond the technical dimension, literature identifies a shift toward the ethical and clinical aspects of digital security (Aliyu et al., 2024). Researchers argue that the protection of medical data is not merely a legal obligation but an intrinsic component of patient safety, demonstrating that the unavailability of IT systems during ransomware attacks directly affects mortality and medical error rates (Khadka & Ullah, 2025; Li et al., 2025). This is compounded by the persistent vulnerability of the human factor: over 74% of breaches involve a human element, whether through error or psychological manipulation (Verizon Report, 2023). The high operational pressure

DOI: 10.4316/EJAFB. 2026.14303

Volume 14 / **2026** ISSN 2344-102X
Issue **3** ISSN-L 2344-102X

characteristic of clinical environments tends to erode compliance with security protocols, which makes a case for shifting toward user-centred security design (Alanazi, 2023).

Regulatory complexity is another central theme in the literature, particularly in the context of transposing the NIS2 Directive. While GDPR provides a general framework for data protection, healthcare-specific cybersecurity standards require a multisectoral approach that integrates network security with medical device safety. The fragmentation of health systems and the lack of secure interoperability among different healthcare providers creates data silos that are frequently left inadequately protected, facilitating the theft of sensitive information (Kruse et al., 2017; Lascateu & Constantinescu, 2024).

At the regional level, ENISA (2023) has warned about vulnerabilities in supply chain attacks, a threat amplified by the outsourcing of cloud services, which creates dangerous dependencies and compromises data confidentiality on a cross-border scale.

The response to these vulnerabilities cannot be purely technical. Artificial intelligence occupies a dual role in this space: on one side, it enables proactive, real-time detection of behavioural anomalies in medical systems; on the other, recent literature documents the growing exploitation of adversarial attack techniques to automate vulnerability scanning and orchestrate highly personalised phishing campaigns (Zhang, 2023).

This reality reinforces the need for a foundational approach. The Security by Design principle, established by McGraw (2013) and Freund and Jones (2014) and revalidated by Seh et al. (2020) in healthcare contexts, holds that security must be a native feature of any newly implemented IT system, not an additional layer applied after the fact.

Building on this broad theoretical foundation, which links technical deficiencies with clinical risks and regulatory pressures, the present study sets out to test the following research hypotheses:

- **H1:** There is a direct and positive correlation between the level of digitalization of a healthcare facility and the total cost of post-incident remediation in the absence of a Zero Trust security architecture.
- **H2:** Ransomware attacks during the period 2021 to 2025 have evolved toward triple extortion strategies, generating a more severe impact on institutional reputation than on the immediate financial base.
- **H3:** The use of legacy IT systems in diagnostic departments represents the primary vector of technical vulnerability, facilitating the lateral movement of attackers across the network.
- **H4:** The implementation of continuous cybersecurity hygiene training programs reduces the success rate of social engineering attacks among medical staff by at least 30% within the first two years of adoption

II. RESEARCH METHODOLOGY

The research methodology adopts a mixed-methods approach, integrating quantitative and qualitative data from a corpus of official documents published between 2021 and 2025. The central objective of this methodology is to synthesise empirical evidence on the evolution of cyber threats in the healthcare sector and to provide a comprehensive perspective on the mechanisms of compromise and their associated systemic impact (Ewoh & Vartiainen, 2024; Liberati et al., 2009).

The source selection process was guided by strict criteria for authority and sectoral relevance (Kleijnen et al., 2009). Priority was given to strategic reports issued by European and international regulatory bodies: the European Union Agency for Cybersecurity (ENISA), the National Directorate of Cyber Security (DNSC) in Romania, the Cybersecurity and Infrastructure Security Agency (CISA), and the National Institute of Standards and Technology (NIST) in the United States. These were cross-referenced with industry impact studies, including the IBM Cost of a Data Breach Report and the Verizon Data Breach Investigations Report, to ensure a global dimension in the financial and operational analysis (Verizon, 2023; IBM Security, 2024; ISACA, 2023).

To be included in the analytical sample, documents had to meet four cumulative conditions: (1) strict coverage of the specified time interval; (2) the presence of statistical data relating to critical health infrastructure; (3) methodological rigour of the original source; and (4) linguistic accessibility in line with recognised academic quality standards (Kavaler & Spiegel, 2023). From these documents, key variables were extracted and coded: initial access vectors, mean time to identify breaches (MTTI), average cost per compromised record (Conti et al., 2021), and the incidence of emerging technologies such as AI and IoT in attack or defence processes.

The data analysis was carried out across three dimensions. In the first, descriptive stage, the focus was on identifying linear trends and inflexion points in the dynamics of ransomware attacks. In the second stage, quantitative indicators were extracted and analysed, covering cost evolution, predominant attack vectors, and the operational impact on medical services. The data were organised into comparative tables to highlight structural trends across the period under review (2021 to 2025). In the final stage, the synthesis integrated qualitative observations on patient safety, translating raw data into strategic conclusions.

An inherent limitation of this methodology, acknowledged in the study, is incident underreporting (Neprash

DOI: 10.4316/EJAFB. 2026.14303

Volume 14 / **2026** ISSN 2344-102X
Issue **3** ISSN-L 2344-102X

et al., 2022; Marsh-Armstrong et al., 2024). While official reports provide a solid basis for analysis, the hidden portion of cybercriminal activity manifests through undisclosed breaches, often concealed for reputational reasons, particularly in the private sector. This may introduce a margin of error in quantifying the actual volume of attacks (Huda et al., 2024). Nevertheless, by triangulating governmental sources with data from the security industry, the research provides a faithful and rigorous representation of the cyber threat landscape in contemporary healthcare (Sharma et al., 2024; Lascateu & Constantinescu, 2024).

III. RESULTS AND DISCUSSION

The comparative analysis of incidence and costs over the 2021 to 2025 period reveals a fundamental shift in the attackers' business model. Where the average cost of $9.23 million in 2021 was dominated by data recovery efforts, by 2025 the most burdensome component had become business interruption, pointing to a deliberate strategy aimed at maximising economic and social damage.

The data in Table 1 show an average annual cost increase of 15-20%, rising from $9.23 million in 2021 to $16.31 million in 2025, a cumulative increase of 77% over the period under review. Beyond the magnitude of this growth, the analytical significance lies in the structural reconfiguration of cost components, reflecting a fundamental shift in the economic logic of cyberattacks targeting the healthcare sector.

Table 1. Evolution of Average Annual Cyberattack Costs

Year	Total Cost (M USD)	Data Recovery (%)	Business Interruption	GDPR (%)	Other (%)
2021	9,23	45%	25%	12%	18%
2022	10,87	40%	32%	12%	16%
2023	12,54	35%	38%	12%	15%
2024	14,92	30%	45%	12%	13%
2025	16,31	28%	48%	12%	12%

Source: Verizon DBIR (2021-2025); IBM Cost of Breach Report; Fortinet Healthcare Report 2024-2025.

The most relevant structural trend is the reversal in the ratio of data recovery to business interruption. The business interruption component grew from 25% in 2021 to 48% in 2025, while the share attributed to data recovery fell from 45% to 28% over the same period. This dynamic does not indicate a reduction in technical recovery efforts; rather, it reflects a shift in the centre of gravity of costs toward operational downtime, driven by the extensive audits required to certify the complete elimination of advanced persistent threats and backdoors, processes that demand specialised human resources over prolonged periods. The conclusion is that attackers have deliberately identified and exploited vulnerabilities in the operational response capacity of medical institutions, turning service disruption into the primary instrument of economic pressure.

A second significant trend concerns the structure of direct versus indirect costs. GDPR compliance fines remain consistently at 12% of total costs throughout the period under review, while indirect costs, namely patient loss, institutional brand deterioration, and the erosion of public trust, account for over 40% of the total. The stability of the GDPR share, in contrast to the absolute increase in total costs, suggests that regulatory sanctions have not kept pace with the scale of incidents, leaving reputational impact as the primary driver of long-term economic damage.

The analysis of attack vectors and the cascade effect they generate reveals that the shift from traditional phishing to supply chain attacks represents the most significant threat identified for the 2023 to 2025 period (Sophos, 2024; Novak, 2025). Software vulnerabilities have become a privileged entry point. The meta-analysis of incident reports highlights cases in which attackers targeted vendors of prescription management software or billing systems. A single vendor-level breach triggered a cascade that simultaneously compromised dozens of medical facilities across the affected networks (Gordon et al., 2011). This type of attack is more efficient for criminals because it eliminates the need to compromise each medical institution individually.

IoMT devices present a specific category of vulnerability. Approximately 26% of recent attacks used smart medical devices, including infusion pumps and cardiac monitors, as entry points. These devices become invisible bridges to the central database, and attackers exploit the fact that biomedical engineering departments rarely coordinate with IT on security updates (Dzamesi & Elsayed, 2025). This organisational fragmentation creates a complex vulnerability landscape that allows undetected lateral movement across the network.

The distribution of attack vectors presented in Table 2 reflects a deep strategic transformation in cybercrime targeting the healthcare sector between 2023 and 2025. While the traditional attack model was dominated by phishing and social engineering, current data indicate a deliberate reorientation toward vectors with higher success rates and comparatively lower effort for the attacker.

DOI: 10.4316/EJAFB. 2026.14303

Volume 14 / **2026** ISSN 2344-102X
Issue **3** ISSN-L 2344-102X

Table 2. Distribution of Cyberattack Vectors (2023 to 2025)

Attack Vector	Frequency (%)	Notes
Supply Chain Attack	32%	Increasing exponentially
IoMT	26%	Medical entry point
Phishing / Social Eng.	18%	Relatively declining
Ransomware direct	14%	Brute force RDP
Other vectors	10%	Zero-day

Source: Fortinet Healthcare Report 2024-2025; Palo Alto Networks Unit 42; CISA Healthcare Advisories.

The most significant indicator of this transformation is the dominance of supply chain attacks (32%) and the exploitation of connected medical devices (26%), which together account for 58% of all identified attack vectors. This concentration reflects a clear economic logic from the attacker's perspective: compromising a single software vendor or an unprotected medical device provides simultaneous access to multiple institutions, multiplying impact with proportionally fewer resources. The rise of supply chain attacks presents a structural threat. By compromising healthcare service providers, including EHR systems, telemedicine platforms, and technical integrators, attackers gain simultaneous access to multiple institutions while expending minimal effort. This strategy exploits informational asymmetry and medical institutions' dependence on their supply partners, turning the supply chain from a vector of development into a vector of systemic risk.

By contrast, phishing and social engineering, while still present at 18% of attack vectors, show a relative decline compared to earlier levels in the period under review (Verizon, 2023). This dynamic suggests that the systematic investments made by medical institutions in user education have produced measurable results, thereby reducing susceptibility to attacks based on human manipulation.

The impact of cyberattacks on clinical resilience and quality of care demonstrates that such incidents are not conventional IT crises but medical emergencies with direct consequences for patients (Li et al., 2025; Ghafur et al., 2023). Service degradation is immediate and measurable. During the 2023 to 2024 period, triage accuracy fell by 15 to 25% during a ransomware incident. Physicians are forced to practice defensive medicine, slowing patient flow and reducing the number of patients processed per hour.

The data in Table 3 highlights a reality that fundamentally reframes the stakes of cybersecurity in the healthcare sector: a cyberattack is not solely an IT crisis but an event with direct and measurable clinical consequences for patient safety. The four indicators, taken together, describe a systemic degradation of medical operational capacity, with varying intensities and recovery timelines.

Table 3. Post-Attack Clinical Impact Indicators

Indicator	Baseline Value	During Attack	Recovery (days)
Triage Accuracy (%)	95%	70-80%	7-10
Time atendent(min)	45	120-180	14-21
Medical Error Rate (%)	0,8%	2-3%	28
Cancelled Surgeries (%)	2%	40-60%	21-28

Source: Fortinet Healthcare Report 2024-2025; Palo Alto Unit 42.

The most immediate impact is seen in cancelled surgical procedures, which rise from 2% under normal conditions to between 40% and 60% during an attack, an increase of up to 30 times the baseline. This disruption reflects the direct dependence of surgical planning on digital infrastructure: scheduling systems, sterilisation protocols, and operating room coordination become inoperable simultaneously, forcing the suspension of most elective procedures and, in critical cases, emergency interventions. Returning to normal levels takes 21 to 28 days, indicating that the technical restoration of systems is not sufficient on its own; recalibrating organisational workflows and recovering blocked capacities and supplies require additional time.

The indicator with the longest recovery period, however, is the medical error rate, which triples during an attack, rising from 0.8% to 2%-3%, and does not return to baseline until after 28 days. This pattern does not reflect clinical negligence but rather a confluence of operational factors: reduced access to complete medical histories forces physicians to make decisions on incomplete information; extreme time pressure compresses the capacity for critical thinking; and fragmented communication between medical teams hampers coordination across the full spectrum of care. The extended recovery interval, longer than for all other indicators in the table, suggests that the psychological and organisational impact of the attack persists well beyond the technical restoration of systems, generating a period of residual clinical vulnerability.

DOI: 10.4316/EJAFB. 2026.14303

Volume 14 / **2026** ISSN 2344-102X
Issue **3** ISSN-L 2344-102X

Together, waiting times and triage accuracy paint a complete picture of operational degradation. Waiting times rise from 45 minutes to 120 to 180 minutes, with a recovery period of 14 to 21 days, while triage accuracy falls from 95% to 70% to 80%, recovering within 7 to 10 days. The fact that triage recovers most quickly suggests that this process depends more on individual clinical competence than on digital infrastructure, unlike surgical scheduling or interdepartmental coordination.

The role of artificial intelligence in cybersecurity represents one of the most consequential developments in the medical cyber domain, as both attackers and defenders have adopted AI technologies, creating a new inflexion point in the technological evolution of cybersecurity (Zhang, 2023; Patel & Bevinakoppa, 2024). Artificial intelligence and automation have fundamentally redefined the speed of response on both sides of this confrontation.

AI as an offensive element became a concrete reality in 2024 and 2025. Reports from 2025 confirm the existence of automated scripts capable of exploiting a newly disclosed vulnerability in a hospital within 15 minutes of disclosure, eliminating the traditional window for manual intervention (Kalupa & Bauckhage, 2023). This means that an IT team must detect and remediate a vulnerability faster than a machine can exploit it, a task that is nearly impossible for hospitals with limited staff.

AI as a security barrier offers a way out. Medical institutions using User and Entity Behavior Analytics (UEBA) detected attacks during the lateral access expansion phase, reducing the data encryption success rate by 45% compared to traditional systems (Tabassum et al., 2024). UEBA works by continuously learning the normal behaviour of each user and each device. When a compromised device begins accessing files in an unusual pattern, UEBA triggers alerts before the attacker can encrypt the data.

The data presented in Table 4 capture one of the most critical asymmetries in the current cybersecurity landscape of the healthcare sector: the gap between the speed and efficiency of offensive AI and the reactive capabilities of traditional defences. The four indicators, taken together, define a structural imbalance that places medical institutions lacking advanced defensive solutions in a position of systemic vulnerability.

Table 4. Comparison: Offensive AI vs. Defensive AI

Aspect	AI Offensive	AI Defensive (UEBA)
Exploitation Time	15 min post-disclosure	Real-time monitoring
Methods	Scan automation, zero-day	Behavioural analytics
Attack Success Rate	65-75%	20-30%
Detection Phase	Post-breach	Early stages

Source: Deloitte Global Threat 2024; Mandiant M-Trends 2024; Gartner UEBA Magic Quadrant 2024.

The most alarming indicator is the exploitation window for offensive AI, which has been reduced to under 15 minutes after a vulnerability is publicly disclosed. This reaction speed far exceeds human response capacity and effectively nullifies the usefulness of manual patch management processes, which remain an operational standard in medical institutions with limited IT resources. Combined with the 65 to 75% success rate of AI-assisted attacks, this indicator indicates that the absence of defensive automation is no longer an acceptable vulnerability but an existential risk to operational continuity.

By contrast, UEBA (User and Entity Behaviour Analytics) solutions demonstrate significant defensive potential: the attack success rate falls to between 20% and 30% with real-time behavioural monitoring, and detection shifts from the post-breach phase to earlier stages of the attack chain. This repositioning of detection is critical from a remediation cost perspective. Identifying a threat during the reconnaissance or lateral movement phase dramatically reduces both the duration of operational disruption and the volume of data compromised. That said, defensive capabilities remain in deficit relative to offensive ones: defensive AI has not yet reached parity with the automated adversary, and the gap is widened by access barriers specific to the healthcare sector. The high implementation costs and the need for specialised technical expertise to properly configure and calibrate UEBA systems represent major obstacles for institutions operating on limited budgets (Zakhmi et al., 2025).

This structural asymmetry has a direct strategic implication: in the absence of investment in automated defensive solutions, medical institutions operate with a reaction window incompatible with the pace of modern threats, regardless of how well prepared their human staff may be. The comparison between public and private healthcare systems reveals a profound cybersecurity discrepancy. While both are vulnerable, the nature of the threats and the capacity to respond differ considerably.

The data presented in Table 5 offer an essential comparative perspective on how the structural profile of a medical institution, whether public or private, determines both the nature of the predominant vulnerabilities and the capacity to respond to and recover from a cyber incident. The five indicators compared describe two distinct risk models with differentiated strategic implications, yet both converge toward the same conclusion: neither sector currently has a defensive architecture adequate to the threats it faces.

DOI: 10.4316/EJAFB. 2026.14303

Volume 14 / **2026** ISSN 2344-102X
Issue **3** ISSN-L 2344-102X

Table 5. Public Sector vs. Private Sector

Criterion	Public Sector	Private Sector
Primary Vulnerability	Legacy systems and rigid budgets	Excessive interconnectivity
Attack Motivation	Social destabilisation	Corporate espionage
Response Capacity	National agencies (DNSC)	Fast internal teams
Recovery Time	72-96 hours	24-48 hours
Security Investment	2-3% of IT budget	5-8% of IT budget

Source: HIMSS Survey 2024; DNSC/CERT-RO Reports 2023-2024.

The public sector is characterised by a structural vulnerability with budgetary and technical roots. Dependence on legacy systems that have exceeded their useful lifecycle but cannot be replaced due to financial constraints creates a rigid attack surface that is difficult to protect through incremental measures (Huda et al., 2024). Cybersecurity investment of just 2 to 3% of the IT budget, compared to 5 to 8% in the private sector, reflects an insufficient prioritisation of digital resilience, with direct consequences for recovery time: 72 to 96 hours versus 24 to 48 hours in the private sector. This discrepancy is compounded by the standardisation of systems across institutions, which can turn an isolated incident into a widely propagating event. The Romanian case from 2024, in which over 40 hospitals were simultaneously compromised by a ransomware attack, illustrates this systemic vulnerability with precision: the administrative and technical interconnections among public institutions, designed for operational efficiency, served as a vector for the attack's amplification.

The private sector presents a distinct risk profile, generated not by underinvestment but by the excessive complexity of the digital ecosystem. Modern private hospitals simultaneously integrate patient management systems, billing platforms, imaging systems, and laboratory infrastructure, often supplied by different third-party vendors and interconnected through interfaces with varying levels of security (Biffi et al., 2025). This architecture delivers superior operational flexibility but creates an attack surface that is exponentially larger than that of a monolithic system. The predominant motivation of attackers in the private sector, namely corporate espionage and the extraction of commercially valuable data, reflects precisely the attractiveness of these interconnected ecosystems as sources of strategic information.

Beyond structural differences, both sectors converge on the same strategic necessity: adopting a Zero Trust architecture, in which no connection is implicitly considered secure, regardless of whether it originates internally or externally (Zakhmi et al., 2025). This convergence is significant: it indicates that security solutions tailored to a single institutional profile are insufficient, and that defensive standards must be flexible enough to address both the rigidity of public systems and the complexity of private ecosystems. In both contexts, the patient's perspective must remain central to any cybersecurity strategy. An incident that compromises continuity of care is not an IT problem; it is a clinical safety issue that must be integrated into institutional governance protocols.

IV. CONCLUSIONS

The retrospective analysis of cyberattacks on hospital infrastructure between 2021 and 2025 reveals a fundamental shift in the healthcare sector's risk paradigm. Medical institutions are no longer collateral targets in opportunistic campaigns; they have become primary strategic targets for organised cybercrime. Two critical factors drive this shift: the intrinsic value of medical data on illicit markets, and the systemic vulnerability created by the absolute necessity of maintaining continuity of care. Attackers exploit a straightforward reality: a hospital cannot refuse to pay a ransom and cannot leave patients without their medical data. Public health has been turned into an instrument of extortion.

The evaluation of the four working hypotheses underpinning this research offers insight into the validity of the theoretical premises and their implications for cybersecurity in medicine.

Hypothesis H1, concerning the correlation between digitalisation and remediation costs in the absence of a Zero Trust architecture, is validated with a high degree of confidence. The evidence is multiple and convergent. The costs of cyber incidents increased from $9.23 million in 2021 to $16.31 million in 2025, representing a cumulative increase of 77%. More significantly, the operational downtime component grew from 25% to 48% of total damages. Hospitals that digitalised without building security from the ground up are substantially more vulnerable, and operational downtime has become the dominant cost driver. Recovery is slow and expensive. The message is clear: digitalisation without security transforms institutions from resilient entities into fragile structures dependent on technological continuity.

Hypothesis H2, concerning the evolution of the attack model toward triple extortion with a predominantly reputational impact, is partially validated. The data confirm that the reputational impact of incidents has exceeded the impact of direct legal sanctions. Institutions lose patients, their standing is destabilised, and public trust erodes.

DOI: 10.4316/EJAFB. 2026.14303

Volume 14 / **2026** ISSN 2344-102X
Issue **3** ISSN-L 2344-102X

Indirect costs, including patient loss, institutional brand deterioration, and the erosion of public confidence, account for over 40% of the total cost of incidents. GDPR fines, by contrast, remain relatively stable at around 12% of total costs. This reveals something important: the law is not keeping pace with the reality of the threats. That said, triple extortion, as such, did not prove to be a dominant strategy during the 2021 to 2025 period. It remains a tactic used by a subset of attackers, not a systematic model, with an estimated prevalence of less than 10% among reported incidents. The reputational impact is very real, but triple extortion has not yet become the norm.

Hypothesis H3, which posits that legacy systems are the primary vector of lateral propagation and technical vulnerability, is invalidated by the empirical evidence. The data show the opposite. Supply chain attacks account for 32% of identified attack vectors, and the exploitation of connected medical devices (IoMT) contributes 26%, together representing 58% of all attacks. By contrast, exploitation of legacy systems and traditional vulnerabilities accounts for only 14% of attack vectors. The transformation is not only quantitative but also qualitative: attackers no longer target outdated technological infrastructure directly; they exploit modern integrations, vendor dependencies, and organisational fragmentation between IT and clinical departments. The Romanian case from 2024 illustrates this clearly. Forty hospitals were compromised not because they had old equipment, but because they were connected to a shared supply network. A hospital with new but unprotected systems is more vulnerable than one with older, isolated, and secured systems. This is a decisive strategic finding that calls for a reconsideration of security priorities.

Hypothesis H4, regarding the sustained reduction of social engineering attacks through continuous cybersecurity training programs for medical staff, is validated with a medium-to-high degree of confidence. The evidence converges from multiple perspectives. Phishing and social engineering attacks declined from approximately 26% to 18% of incidents, a drop of 8 percentage points. This is a positive signal. Hospitals that invest in staff education see measurable results. Behavioural monitoring systems (UEBA), which rely on well-trained users, reduce the attack success rate from 65 to 75% to 20 to 30%. The private sector, which invests more (5 to 8% of the IT budget) and trains staff more frequently, recovers faster (24 to 48 hours) than the public sector (72 to 96 hours). This confirms that training works, but it is not sufficient on its own, because attackers adapt and shift to other methods. Training is necessary, but it must be combined with advanced protection systems.

The most important finding of this research is the direct link between digital security and patient safety. This is not an IT problem. It is a medical problem. When a cyberattack disrupts a hospital, people suffer. The data are concrete and alarming: triage accuracy falls by 20%, physicians make three times as many errors, between 50 and 60% of surgical procedures are cancelled, and hospitals need three to four weeks to return to normal operations. These figures say more than any financial loss figure; they show the human cost of delayed or denied treatment. This is why the way we think about cybersecurity in healthcare must change. It is not a technical attribute of the IT department; it is an essential part of medical practice, as important as diagnosis, surgery, and patient monitoring. Cyber safety is patient safety, and it should be embedded in everything medical institutions do.

The evolution of cyber threats points to a major shift in how attackers operate. They no longer target medical infrastructure directly. They target vendors. They target connected devices. This means that traditional perimeter-based defence models no longer work. Zero Trust is not just a buzzword; it is a strategic necessity. Every connection and every device must be treated as potentially compromised. Connected medical devices (IoMT) are particularly dangerous. They are essential to modern medicine, but they also open the door for attackers. An unprotected connection to a monitoring system can allow the modification of critical parameters.

The comparison between the public and private sectors reveals that both have fundamental limitations, though of a different nature. The public sector suffers from insufficient funding and dependence on legacy systems that cannot be replaced immediately. Cybersecurity investment in the public sector is just 2 to 3% of the IT budget, creating collective vulnerabilities that can affect dozens of institutions simultaneously. The private sector, on the other hand, faces the exponential complexity of excessive interconnection, with multiple systems from different vendors and investment levels of 5-8% of the IT budget, creating a vast attack surface. Neither approach is perfect. Both require strategies adapted to their specific realities. What is clear, however, is that the private sector, through more sustained investment, demonstrates measurably superior operational resilience.

Artificial intelligence has fundamentally changed the threat and defence landscape. From the attacker's perspective, AI can identify and exploit vulnerabilities within 15 minutes of the technical details being published and generate thousands of personalised phishing emails highly tailored to the specific dynamics of medical institutions. From the defensive side, AI-driven UEBA tools can monitor user behaviour and detect anomalies in real time, reducing attack success rates from the 65 to 75% range down to 20 to 30%. AI is not inherently on one side or the other. It is a double-edged tool, and the advantage shifts to the attacker only when medical institutions fail to invest in modern defences.

The transformation underway in how threats evolve demands continuous reassessment of priorities and strategies. What works today may be obsolete tomorrow. Medical institutions that intend to remain secure must treat security as a living process, not something configured once and then forgotten. Zero Trust is not a final destination; it is a starting point for a more mature approach. Security strategies should be reviewed annually in

DOI: 10.4316/EJAFB. 2026.14303

Volume 14 / **2026** ISSN 2344-102X
Issue **3** ISSN-L 2344-102X

light of new attack vectors and emerging threats. The future of hospitals depends on understanding one fundamental point: investment in cybersecurity is not an administrative expense. It is an investment in human lives. Institutions that integrate cyber resilience into their strategic plans and allocate budgets in proportion to the threats they face will remain operational during sophisticated attacks. Those that ignore this will face operational disruptions, massive data losses, and a deterioration in the quality of care.

No technical system, regardless of its sophistication, can replace people. A culture of security awareness and accountability is the most important and most cost-effective defence available. Continuous training programs work and produce measurable results. Integrating security into clinical protocols transforms it from an isolated IT responsibility into a collective one. Physicians, nurses, and administrative staff must understand that they are co-defenders of institutional safety. The cybercriminal industry has identified healthcare as a priority target for three converging reasons: real systemic vulnerabilities, financial motivation because hospitals pay ransoms, and growing technological opportunities. The decision of medical institutions to invest in cyber resilience is therefore no longer an administrative or optional choice. It is a fundamental ethical obligation: to protect both patients' data and their lives.

The data from 2021 to 2025 point to an undeniable reality: threats evolve faster than traditional responses. To remain secure, medical institutions must evolve as well. They must adopt new and adaptable strategies, invest in advanced technology, and develop their human capital. Cybersecurity is not optional; it is a priority. The balance of the research hypotheses confirms that the threat landscape from 2021 to 2025 has evolved faster than traditional defensive frameworks can keep pace with, requiring continuous, deep realignment of security priorities across medical institutions.

Funding: This research received no external funding.
Conflicts of interest: The author declares no conflicts of interest.
Ethics statement: This study is based exclusively on publicly available legal, institutional, policy and secondary academic sources. It does not involve human participants, interviews, surveys, experiments, personal data collection or clinical/biomedical material. Therefore, formal ethical approval was not required.

REFERENCES

1. Alanazi, A.T. (2023). Clinicians' perspectives on healthcare cybersecurity and cyber threats. Cureus, 15(10), e47026. https://doi.org/10.7759/cureus.47026.
2. Aliyu, A., Ogbuju, E., Imoize, A.L., Abari, O.J., Kunya, M.M., Sani, G., Salaudeen, F.A., & Oladipo, F. (2024). The ethics of cybersecurity in emerging healthcare systems. In Cybersecurity in Emerging Healthcare Systems (pp. 363-400). The Institution of Engineering and Technology. https://doi.org/10.1049/PBHE064E_ch12.
3. Biffi, A., Castellini, G., Del Castillo, G., De Nard, F., Vismara, C., Cabitza, F., & Gianola, S. (2025). Effectiveness of computerized decision support systems linked to electronic health records: An updated systematic review with meta-analysis. International Journal of Medical Informatics, 106220. https://doi.org/10.1016/j.ijmedinf.2025.106220.
4. Conti, M., Donadel, D., & Turrin, F. (2021). A survey on industrial control system testbeds and datasets for security research. IEEE Communications Surveys and Tutorials, 23(4), 2248-2294. doi:10.1109/COMST.2021.3094360.
5. Deloitte. (2024). Global threat landscape 2024. Retrieved from https://www2.deloitte.com/us/en/resources.
6. Dzamesi, L., & Elsayed, N. (2025, April). A review on the security vulnerabilities of the IoMT against malware attacks and DDoS. In 2025 IEEE 4th International Conference on Computing and Machine Intelligence (ICMI) (pp. 1-8). IEEE. https://doi.org/10.48550/arXiv.2501.07703.
7. ENISA. (2023). ENISA threat landscape for supply chain attacks. Brussels: ENISA Publications. Retrieved from https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
8. Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. Journal of Medical Internet Research, 26, e46904. https://doi.org/10.2196/46904.
9. Flowerday, S.V., Lipskiy, N., Furnell, S., Flowerday, C.E., & Hale, J. (2026). Bending the curve: Operational cyber epidemiology for ransomware. Computers and Security, 104922. https://doi.org/10.1016/j.cose.2026.104922.
10. Fortinet. (2024). Healthcare threat landscape report 2024-2025. Retrieved from https://www.fortinet.com/resources/reports.
11. Freund, J., & Jones, J. (2014). Measuring and managing information risk: A FAIR approach. Burlington, MA: Butterworth-Heinemann.
12. Gartner, Inc. (2024). Magic Quadrant for Security Information and Event Management (SIEM). [Published: 8 May 2024]
13. Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Digital Medicine, 2(1), 98. https://doi.org/10.1038/s41746-019-0161-6.
14. Gordon, L.A., Loeb, M.P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs. Journal of Computer Security, 19(1), 33-56. https://doi.org/10.3233/JCS-2009-0398.
15. Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers and Security, 76, 101-127. https://doi.org/10.1016/j.cose.2018.02.020.
16. Huda, S., Islam, M. R., Abawajy, J., Kottala, V. N. V., & Ahmad, S. (2024). A cyber risk assessment approach to federated identity management framework-based digital healthcare system. Sensors, 24(16), 5282. https://doi.org/10.3390/s24165282.
17. IBM Security & Ponemon Institute. (2024). Cost of a data breach report 2024. Retrieved from https://www.ibm.com/security/data-breach.
18. Kavaler, F., & Spiegel, A.D. (2003). Risk management in health care institutions: A strategic approach. Sudbury, MA: Jones & Bartlett Learning.

DOI: 10.4316/EJAFB. 2026.14303

Volume 14 / **2026** ISSN 2344-102X
Issue **3** ISSN-L 2344-102X

19. Khadka, K., & Ullah, A.B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. International Journal of Information Security, 24(3), 119. https://doi.org/10.1007/s10207-025-01032-0.
20. Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. PLoS Medicine, 6(7), e1000100. https://doi.org/10.1371/journal.pmed.1000100.
21. 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. https://doi.org/10.3233/THC-161263.
22. Lascateu, C., & Constantinescu, M. (2024). Bridging the maturity gap: Adaptive strategies for advancing cybersecurity in Romanian healthcare institutions. Romanian Cyber Security Journal, 6(2), 3-13. https://doi.org/10.54851/v6i2y202401.
23. Lee, J., Kim, H., & Choi, S.J. (2024). Do hospital data breaches affect health information technology investment? Digital Health, 10, 20552076231224164. https://doi.org/10.1177/20552076231224164.
24. Li, S., Surineni, K., & Prabhakaran, N. (2025). Cyber-attacks on hospital systems: A narrative review. The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice, 7, 30-39. https://doi.org/10.1016/j.osep.2025.03.002.
25. Liberati, A., Moher, D., Tetzlaff, J., & Altman, D.G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Medicine, 6(7), e1000097. https://doi.org/10.1371/journal.pmed.1000097.
26. Mamuye, A.L., Yilma, T.M., Abdulwahab, A., Broomhead, S., & Zondo, P. (2022). Health information exchange policy and standards for digital health systems in Africa: A systematic review. PLOS Digital Health, 1(10), e0000118. https://doi.org/10.1371/journal.pdig.0000118.
27. McGraw, G. (2012). Software security: Building security in. Datenschutz und Datensicherheit, 36(9), 662-665.
28. Neprash, H.T., McGlave, C.C., Cross, D.A., Virnig, B.A., Puskarich, M.A., Huling, J.D., & Nikpay, S.S. (2023). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. JAMA Health Forum, 4(2), e230001. doi:10.1001/jamahealthforum.2023.0001.
29. Novak, C. (2025, March 3). Ransomware evolution: From encryption to extortion. Bank Info Security. Retrieved from https://www.bankinfosecurity.com/.
30. Palo Alto Networks. (2024). Unit 42 threat intelligence report: Healthcare sector 2024. Retrieved from https://unit42.paloaltonetworks.com/.
31. Patel, D., & Bevinakoppa, S. (2024, November). Machine learning-based automated threat detection network security in healthcare. In 2024 IEEE 9th International Conference on Engineering Technologies and Applied Sciences (ICETAS) (pp. 1-6). Bahrain: IEEE. https://doi.org/10.1109/ICETAS62372.2024.11120139.
32. Portela, D., Nogueira-Leite, D., Almeida, R., & Cruz-Correia, R. (2023). Economic impact of a hospital cyberattack in a national health system: Descriptive case study. JMIR Formative Research, 7, e41738. doi:10.2196/41738.
33. Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R., & Khan, R.A. (2020). Healthcare data breaches: Insights and implications. Healthcare, 8(2), 133. doi:10.3390/healthcare8020133.
34. Sharma, D.P., Habibi Lashkari, A., & Parizadeh, M. (2024). Cybersecurity challenges, best practices, and future work in healthcare. In Understanding Cybersecurity Management in Healthcare. Progress in IS (pp. 1-30). Cham: Springer. https://doi.org/10.1007/978-3-031-68034-2_10.
35. Sittig, D.F., & Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. BMJ Quality and Safety, 19(Suppl 3), i68-i74.
36. Sophos. (2024). State of ransomware in healthcare 2024: The double extortion evolution. Retrieved from https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-healthcare-2024.
37. Tabassum, M., Mahmood, S., Bukhari, A., Alshemaimri, B., Daud, A., & Khalique, F. (2024). Anomaly-based threat detection in smart health using machine learning. BMC Medical Informatics and Decision Making, 24(1), 347. doi:10.1186/s12911-024-02760-4.
38. Verizon Communications Inc. (2023). 2023 data breach investigations report. Retrieved from https://www.verizon.com/business/resources/reports/dbir/.
39. Zakhmi, K., Ushmani, A., & Ranjan Mohanty, M. (2025). Evolving Zero Trust architectures for AI-driven cyber threats in healthcare and other high-risk data environments: A systematic review. Cureus, 17(6), e85446. doi:10.7759/cureus.85446.
40. Zhang, H. (2023). Artificial intelligence in healthcare: Opportunities and challenges. Theoretical and Natural Science, 21, 130-134. https://doi.org/10.54254/2753-8818/21/20230845.
41. Healthcare Information and Management Systems Society. (2024). 2024 cybersecurity and ransomware impact survey. Retrieved from https://cdn.sanity.io/files/sqo8bpt9/production/4f1c1968050411b8bf9335a187301881f9153b9f.pdf
42. Directia Nationala de Securitate Cibernetica. (2024). Raport anual privind incidentele de securitate cibernetica 2023-2024. Retrieved from https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024.

DOI: 10.4316/EJAFB. 2026.14303