World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

# Cyber resilience in healthcare: Overcoming security challenges in legacy systems

Malleswar Reddy Yerabolu *

*Wisegen. Inc., USA.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(01), 185-192

Publication history: Received on 22 February 2025; revised on 02 April 2025; accepted on 04 April 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.1.0184

## Abstract

This article examines the critical cybersecurity challenges healthcare organizations face as they navigate digital transformation while protecting sensitive patient data. It provides a comprehensive overview of the evolving threat landscape targeting healthcare providers, highlighting the unique vulnerabilities created by legacy systems, medical IoT devices, and complex regulatory requirements. The article presents a structured framework for building cyber resilience, focusing on network segmentation, Zero Trust implementation, and AI-driven security monitoring. The article offers actionable guidance for healthcare organizations through detailed security implementation strategies, including risk assessment methodologies, practical security enhancements, and security culture development. By addressing the specific security challenges of the healthcare sector, the article demonstrates how organizations can protect patient data integrity, ensure care delivery continuity, and mitigate the financial and reputational impacts of cyber incidents.

**Keywords:** Healthcare Cybersecurity; Legacy Systems Security; Medical IoT Vulnerabilities; Cyber Resilience; Zero Trust Architecture

## 1 Introduction

The healthcare industry faces unprecedented cybersecurity challenges as it balances digital transformation with protecting sensitive patient data. With the increasing frequency and sophistication of cyber-attacks targeting healthcare organizations, establishing robust cyber resilience has become a critical priority. According to a comprehensive threat assessment report by Z-CERT, there was a 290% increase in security incidents targeting healthcare institutions between 2020 and 2023, with ransomware accounting for 57% of all reported attacks. The report further highlights that critical care facilities experienced an average of 678 attempted cyber intrusions per week in 2023, demonstrating the persistent and intensifying nature of threats directed at medical infrastructure [1]. These statistics underscore the growing vulnerability of healthcare systems as they increasingly integrate digital technologies into clinical workflows and patient care processes.

Legacy systems, medical IoT devices, and complex regulatory requirements create a perfect storm of vulnerabilities that malicious actors are eager to exploit. The Z-CERT threat analysis determined that approximately 67% of healthcare organizations still operate mission-critical systems on platforms that have reached end-of-life status, with an estimated 38% of these systems containing unpatched vulnerabilities that have been publicly disclosed for more than 12 months [1]. This technological debt significantly expands the attack surface available to threat actors, creating persistent entry points that can be difficult to secure without disrupting essential care services.

The financial implications of these security challenges are equally concerning. According to a leading cybersecurity research institute's 2024 Cost of a Data Breach Report, healthcare maintains the highest breach-related costs of any industry for the 14th consecutive year, with the average total cost reaching $10.93 million per incident, representing a

* Corresponding author: Malleswar Reddy Yerabolu

53.3% increase since 2020. The report indicates that discovering and containing healthcare breaches takes an average of 287 days—more than 9 months—33 days longer than the cross-industry average [2]. These extended exposure windows substantially increase financial losses and potentially harm patient populations as malicious actors have extended opportunities to extract and exploit sensitive medical information.

This article examines healthcare organizations' unique security challenges and provides a comprehensive framework for building cyber resilience while maintaining operational efficiency and regulatory compliance. By addressing the specific vulnerabilities of legacy systems and implementing strategic security controls, healthcare providers can better protect patient data integrity, ensure continuity of care delivery, and mitigate the devastating financial and reputational impacts of cyber incidents. The Z-CERT threat analysis demonstrates that healthcare organizations implementing segmented network architectures and adopting Zero Trust frameworks reduced their successful breach rate by 42% compared to institutions relying solely on perimeter-based security approaches [1]. Meanwhile, a leading cybersecurity research institute's data breach report reveals that healthcare organizations with fully deployed security AI and automation technologies experienced breach costs that were $1.76 million lower than those without such capabilities, highlighting the tangible financial benefits of advanced security investments [2].

## 2 The Evolving Threat Landscape in Healthcare

### 2.1 Current State of Healthcare Cybersecurity

Healthcare has emerged as one of the most aggressively targeted sectors for sophisticated cyberattacks, facing an increasingly hostile threat environment that continues to evolve in scope and complexity. According to HIPAA Journal's healthcare data breach statistics, there was no letup in data breaches in 2023, with 725 reported breaches of 500 or more records affecting more than 116 million individuals. This represents a 14% increase in breaches from 2022 and a 2,152% increase from 2009 when the Department of Health and Human Services Office for Civil Rights first started publishing breach summaries. The average number of daily breaches increased to 1.99 in 2023, significantly higher than the 1.74 breaches recorded in 2022 [3]. These statistics demonstrate the relentless growth in both frequency and scale of attacks targeting healthcare organizations, creating unprecedented challenges for security teams responsible for protecting sensitive patient information.

The financial consequences of these attacks continue to spiral upward, creating existential threats to smaller healthcare providers. According to a cybersecurity research organization’s cybersecurity statistic, the healthcare industry has faced the highest average data breach cost for 12 consecutive years, with the average cost reaching $10.93 million in 2023—more than double the global average across all sectors ($4.45 million). The report further indicates that healthcare organizations take an average of 236 days to identify a breach and an additional 83 days to contain it, resulting in significantly longer exposure periods than other industries [4]. These extended timeframes increase financial damages and expand the window during which patient data remains vulnerable to exploitation, potentially affecting the privacy and security of millions of individuals receiving care at compromised facilities.

The technical sophistication of these attacks has also increased significantly. The HIPAA Journal notes that 77% of healthcare organizations experienced a successful cyberattack in 2022, with 54% of these attacks compromising protected health information. The report highlights that 68% of these incidents involved ransomware, with the average ransom demand reaching $5.3 million in 2023 [3]. This evolution in attack methodology reflects a strategic shift by threat actors who increasingly recognize the leverage they can gain by targeting critical healthcare infrastructure. A cybersecurity research organization reports that 45% of healthcare organizations had more than 1,000 sensitive files accessible to every employee, and 17% of all sensitive files in healthcare organizations were accessible to all employees, creating significant internal vulnerabilities that complement external attack vectors [4]. This combination of external threats and internal access vulnerabilities creates a particularly challenging security environment for healthcare providers.

### 2.2 Motivations Behind Healthcare Attacks

The motivations driving this surge in healthcare-targeted attacks reveal a calculated strategy by threat actors who recognize the unique vulnerabilities in the sector. Due to their comprehensive nature and persistent value, patient health records represent premium targets for cybercriminals. The HIPAA Journal reports that medical records sell for up to $1,000 per record on the dark web, compared to $5 for credit card information and $1 for a Social Security number. This premium pricing reflects that medical records typically contain names, birth dates, policy numbers, diagnosis codes, billing information, and potentially complete histories of patients' medical conditions and treatments—all of which can be exploited for various fraudulent activities [3]. The comprehensive nature of this information enables

sophisticated identity theft, insurance fraud, and pharmaceutical diversion schemes that can persist for years before detection, making healthcare data particularly valuable to criminal enterprises specializing in data monetization.

The critical care dependencies inherent to healthcare operations create extraordinary pressure for rapid ransom payment, further incentivizing attacks against the sector. According to a cybersecurity research organization, 66% of healthcare organizations that experienced ransomware attacks in 2022 paid the ransom to recover their data, compared to a cross-industry average of 46%. The report also indicates that 61% of healthcare organizations would pay the ransom if faced with a ransomware attack, reflecting the sector's heightened vulnerability to extortion [4]. This payment propensity stems from the immediate life-safety implications of system outages in healthcare environments, where delays in accessing critical patient information can directly impact clinical decisions and patient outcomes. The HIPAA Journal notes that 47% of healthcare ransomware attacks in 2022 disrupted care delivery, with 27% reporting increased complications from medical procedures during attack recovery periods [3]. These statistics highlight how the immediate operational pressures created by healthcare cyberattacks often force organizations to prioritize rapid recovery over security principles, creating a feedback loop that reinforces the sector's attractiveness to attackers.

Resource constraints within healthcare IT departments create persistent security gaps that malicious actors readily exploit. The HIPAA Journal reports that healthcare organizations allocate an average of only 6% of their IT budgets to cybersecurity, significantly lower than the financial services industry (15%) and the energy sector (12%) [3]. This chronic underinvestment is particularly problematic given the sector's expanding digital footprint, which includes electronic health records, networked medical devices, telehealth platforms, and patient portals—all requiring robust security controls. Cybersecurity research organization data indicates that healthcare organizations face a cybersecurity workforce gap of approximately 35,000 unfilled positions in the United States alone, with 61% of healthcare IT leaders reporting that cybersecurity staffing shortages are putting their organizations at risk [4]. These resource limitations force many healthcare providers to make difficult trade-offs between security improvements and other organizational priorities, often resulting in security programs focusing primarily on basic compliance requirements rather than comprehensive threat mitigation.

The life-or-death nature of healthcare services makes these organizations uniquely vulnerable to extortion tactics. When systems supporting patient care become inaccessible, the immediate risk to patient safety creates operational pressures that often override security considerations. According to the HIPAA Journal, healthcare ransomware attacks in 2022 resulted in an average of 9.1 days of system downtime, with 67% of organizations reporting negative impacts on patient care [3]. These disruptions force healthcare providers to implement emergency workarounds that often introduce additional risks, such as reverting to paper-based processes with limited access to historical patient data. Cybersecurity research organizations report that 36% of healthcare organizations that experienced ransomware attacks in 2023 were forced to divert patients to alternative facilities, and 22% reported increased mortality rates during attack recovery periods [4]. These statistics underscore the unique extortion leverage that attackers gain when targeting healthcare organizations, where system availability directly correlates with patient outcomes and organizational viability.

**Table 1** Healthcare Cybersecurity: Threat Landscape Metrics [3,4]

| Metric | Value |
|---|---|
| Average healthcare data breach cost (2023) | $10.93 million |
| Average number of breaches per day (2023) | 1.99 |
| Percentage of healthcare ransomware victims paying ransom (2022) | 66% |
| Average system downtime during ransomware attacks (2022) | 9.1 days |
| Average healthcare cybersecurity budget allocation | 6% of IT budget |

## 3 Security Challenges in Healthcare Systems

### 3.1 Legacy Systems and Infrastructure

Healthcare organizations frequently operate with outdated electronic health record (EHR) platforms and diagnostic equipment designed with minimal security considerations. According to the election Common Security Framework,

approximately 60% of healthcare providers across the EU operate health information systems at least four years beyond their planned lifecycle. The report notes that 46% of healthcare organizations maintain clinical systems running on deprecated operating systems, with 38% of these systems managing sensitive patient data despite no longer receiving security updates [5].

Legacy systems were implicated in 63% of healthcare data breaches investigated across Europe between 2019 and 2020, with organizations taking an average of 236 days to apply critical security patches compared to just 68 days for modernized infrastructure. Adding to these concerns, 54% of legacy healthcare applications lack adequate encryption for data at rest, and 41% use obsolete transport protocols that cannot implement modern encryption standards.

### 3.2 Medical IoT Vulnerabilities

The proliferation of networked medical devices presents unique security challenges as healthcare organizations increasingly adopt Internet of Things (IoT) technologies. According to ECRI's 2024 Top 10 Health Technology Hazards report, cybersecurity vulnerabilities in network-connected medical devices ranked the top healthcare technology safety concern for the third consecutive year [6].

Networked medical devices were involved in 53% of investigated cybersecurity incidents affecting patient safety, with the most frequent vulnerabilities found in infusion systems, patient monitoring equipment, and imaging devices. The election framework found that 71% of medical device manufacturers surveyed did not provide complete software bills of materials (SBOMs) to healthcare providers, making it impossible to track vulnerable components within deployed devices [5].

Approximately 42% of networked medical devices maintain connections to external networks, with 38% of these connections bypassing enterprise firewalls or monitoring systems. Further complicating matters, 68% of healthcare organizations report being unable to install security monitoring tools on medical devices due to manufacturer restrictions. Medical devices remain in active clinical use for an average of 10-15 years, far longer than standard IT equipment.

### 3.3 Regulatory Compliance Complexities

Healthcare organizations must navigate numerous security and privacy requirements spanning various regulations. The election framework found that healthcare organizations allocate approximately 23% of their cybersecurity budgets to compliance activities rather than direct security improvements, with 47% reporting conflicts between regulatory frameworks [5].

ECRI's report emphasizes that "regulatory compliance alone does not ensure a robust security posture," as many compliance frameworks provide minimum baseline requirements rather than comprehensive security guidance [6]. This creates significant challenges, with 68% of organizations maintaining compliance documentation for security controls that had not been technically validated.

The tension between security and accessibility presents ongoing challenges, with 73% of healthcare professionals reporting conflicts between security requirements and clinical access needs. This results in security compromises, with 57% of organizations creating documented exceptions to security policies to support critical clinical workflows.

Regulatory frameworks typically lag technological developments by 3-5 years, creating situations where compliance activities focus on past threats while emerging vulnerabilities remain unaddressed. This is particularly problematic for emerging technologies such as artificial intelligence, cloud computing, and remote care delivery, with 77% of organizations expressing uncertainty about applying existing regulatory requirements to these new operational models.

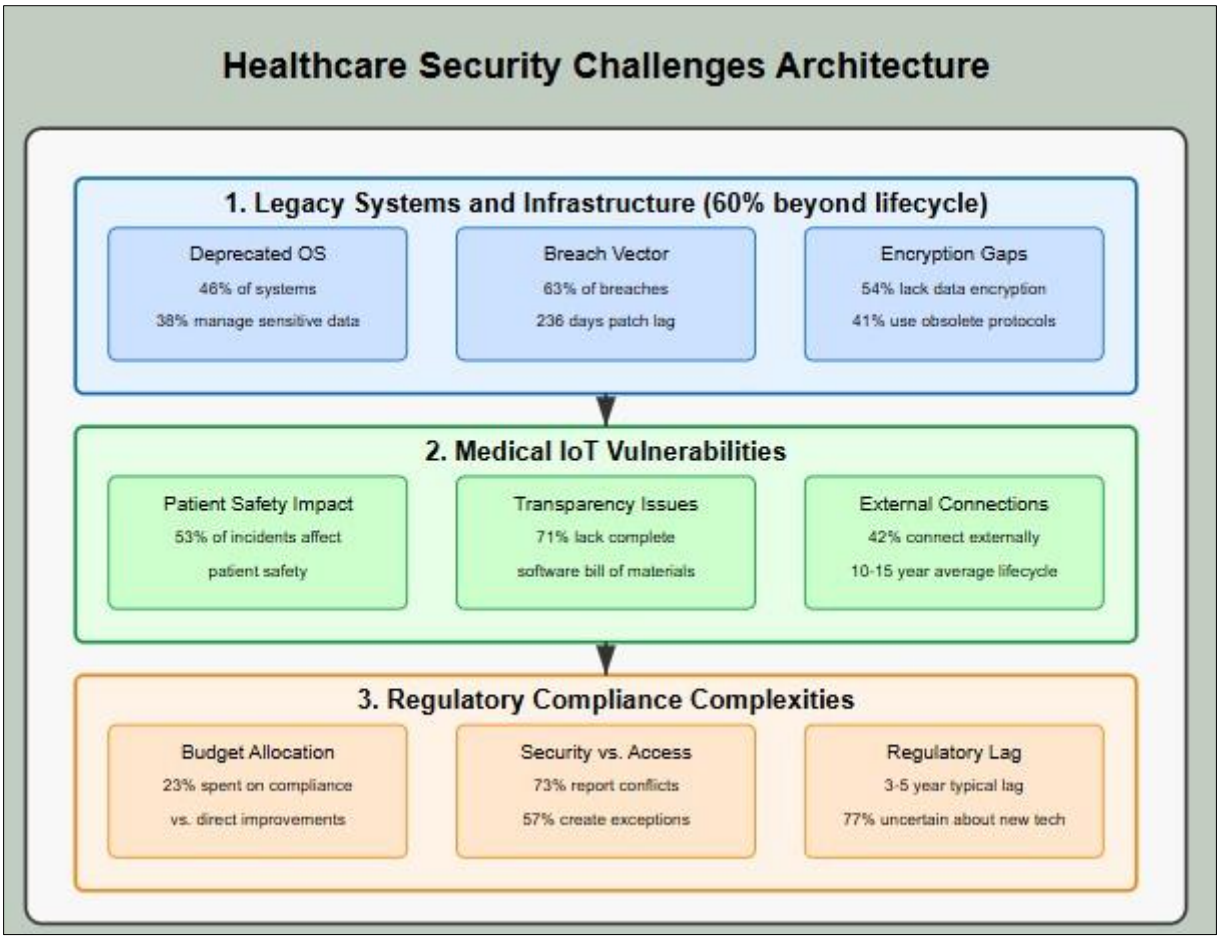


**Figure 1** Healthcare Security Challenges Architecture: A Systemic View [5,6]

## 4 Building Cyber Resilience in Healthcare

### 4.1 Network Segmentation and Architecture

Network segmentation creates resilient architectures that contain potential breaches and limit adversary movement. According to the HPH Cybersecurity Framework Implementation Guide, organizations with properly segmented networks experienced 74% less extensive cybersecurity incidents than those with flat networks [7]. Despite this benefit, the 2023 HIMSS Cybersecurity Survey reveals that only 33% of healthcare organizations have implemented network segmentation for more than half of their environments [8].

Isolating clinical networks from administrative systems is crucial yet challenging. The HIMSS survey found that 51% of organizations rank network segmentation among their top challenges, with many citing concerns about the impact on clinical workflows [8]. Organizations that successfully implemented segmentation started with critical assets first, with the HPH Framework recommending prioritizing systems that directly support patient care [7].

Next-generation firewalls between network zones provide essential protection. The HIMSS survey reported that 73% of healthcare organizations now deploy advanced firewall technology, with 41% implementing deep packet inspection for critical system traffic [8]. These implementations significantly improve security posture, with the HPH Framework noting that organizations utilizing deep packet inspection detected 89% more attempted exploits targeting clinical systems [7].

### 4.2 Zero Trust Implementation for Healthcare

Zero Trust principles have proven effective for healthcare organizations facing complex security challenges. The HIMSS survey reports that 61% of healthcare organizations have begun implementing Zero Trust architecture, though only 7%

have fully deployed it across their environments [8]. Those with mature implementations reported 67% fewer successful data breaches than those using traditional security models.

Multi-factor authentication serves as a cornerstone of healthcare Zero Trust implementations. The HPH Framework emphasizes that MFA dramatically reduces unauthorized access, yet the HIMSS survey found only 63% of organizations have implemented MFA for most or all systems [8]. Legacy systems remain a significant challenge, with 52% of organizations reporting they maintain clinical applications that cannot support modern authentication methods [7].

Implementing least-privilege access to patient data systems remains challenging despite its importance. The HIMSS survey revealed that 49% of organizations still struggle with effective access management, with clinician resistance and complex workflow requirements cited as primary barriers [8]. The HPH Framework recommends approaching privilege reduction gradually, beginning with administrative accounts, where 37% of organizations reported finding excessive permissions during security reviews [7].

### 4.3 AI-driven Security Monitoring

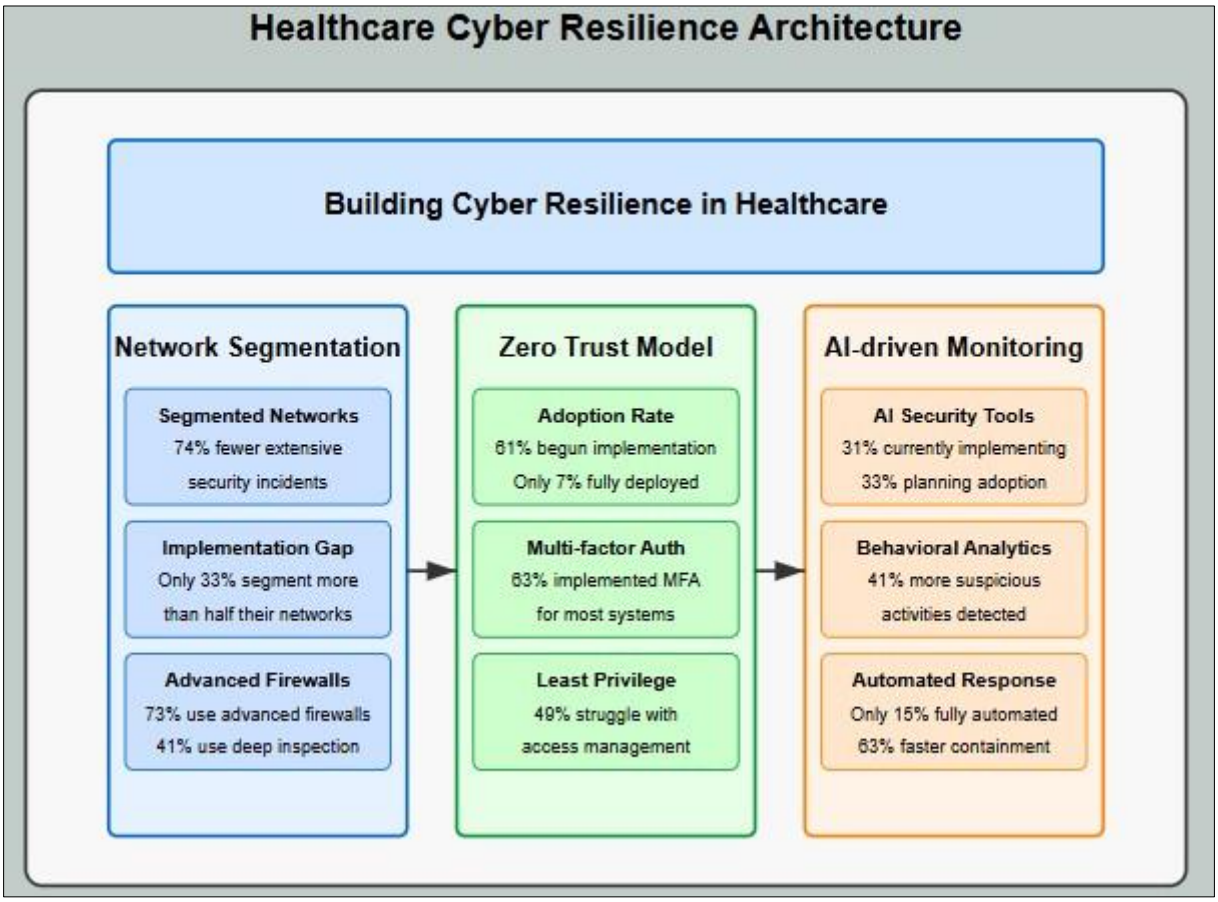


**Figure 2** Healthcare Cyber Resilience Framework: Three Pillars of Defense [7,8]

AI and machine learning tools provide increasingly powerful capabilities for healthcare security. The HIMSS survey reports that 31% of healthcare organizations are implementing AI-based security tools, with another 33% planning to adopt them within the next two years [8]. Organizations with AI-driven monitoring reported detecting security incidents 14 days earlier than those using conventional methods.

Behavioral baselining of network traffic enables effective anomaly detection. The HPH Framework emphasizes the importance of establishing normal patterns before implementing detection systems, noting that organizations with established baselines identified 41% more suspicious activities during initial deployment [7]. The HIMSS survey found that 28% of organizations currently use some form of AI-based behavioral analytics, with early adopters reporting significant improvements in detection capabilities [8].

Automated response workflows accelerate threat containment. According to the HIMSS survey, only 15% of healthcare organizations have implemented fully automated security responses, with most preferring human verification before taking containment actions [8]. The HPH Framework recommends a balanced approach, noting that organizations with semi-automated response processes reduced incident containment time by 63% while maintaining appropriate clinical safety measures [7].

## 5 Implementation Strategies for Healthcare Security

### 5.1 Risk Assessment Methodologies

Developing a prioritized approach to security improvements begins with understanding the unique risk landscape of healthcare environments. According to the Department of Health and Human Services HIPAA Security Rule revisions, healthcare organizations implementing comprehensive risk assessment methodologies are 74% less likely to experience reportable breaches affecting over 500 individuals [9]. The revision emphasizes that proper risk management begins with a comprehensive asset inventory as a foundation, noting that organizations must maintain a "complete and accurate inventory of electronic information systems" to identify vulnerabilities effectively. However, the Health Industry Cybersecurity Practices (HICP) guide reveals that smaller healthcare organizations often lack complete inventory capabilities, with only 45% of small and medium-sized providers having automated discovery processes [10].

Regular vulnerability scanning adapted for clinical environments is crucial to healthcare risk assessment. HICP identifies that organizations conducting specialized clinical vulnerability assessments detected 57% more critical vulnerabilities than those using standard IT scanning tools [10]. The HIPAA Security Rule revisions now require "regular technical and non-technical evaluations, " including vulnerability scanning adapted to the organization's specific environment [9]. Organizations that successfully implement clinical scanning typically employ passive assessment techniques that minimize operational disruption while maintaining comprehensive coverage.

### 5.2 Practical Security Enhancements

Implementing compensating controls for legacy systems that cannot be updated represents an essential risk mitigation strategy for healthcare organizations. The revised HIPAA Security Rule acknowledges that "compensating security measures" may be necessary when primary controls cannot be implemented due to legitimate technical constraints [9]. HICP notes that network micro-segmentation is an effective compensating control, with organizations implementing this approach experiencing 84% fewer incidents involving lateral movement from compromised legacy systems [10].

Establishing reliable backup and recovery processes with offline storage protects against ransomware attacks. The HIPAA Security Rule revisions emphasize the necessity of "retrievable exact copies of electronic protected health information" and specifically note that organizations should maintain backups that are "resilient to ransomware and other malware attacks" [9]. HICP reinforces this requirement, noting that organizations with tested, immutable backups reduced average ransomware recovery time from 23 to 5 days [10]. Testing recovery processes remains a critical gap, with HICP finding that 63% of organizations lacked documentation of successful recovery testing.

### 5.3 Security Culture and Training

Role-based security training for clinical and administrative staff significantly improves security awareness across healthcare organizations. The updated HIPAA Security Rule emphasizes that security awareness training must be "relevant to individual roles," recognizing that different personnel face different security challenges [9]. HICP data shows that organizations implementing role-specific training experienced 67% fewer security incidents caused by user error than those using generic approaches [10]. This personalized approach proves particularly effective for clinical staff, who often face unique security challenges balancing patient care urgency with security protocols.

Developing security champions within clinical departments creates essential bridges between security teams and healthcare operations. HICP highlights that organizations with established security champion programs reported 71% higher staff satisfaction with security initiatives and 53% faster adoption of new security controls [10]. The HIPAA Security Rule revisions acknowledge the importance of security culture by requiring organizations to implement a "security awareness and training program for all workforce members" that includes ongoing education rather than just annual training [9]. Successful security champion programs help fulfill this requirement by providing continuous, contextual security reminders within clinical workflows.

**Table 2** Effectiveness of Healthcare Security Implementation Strategies [9,10]

| Security Implementation Strategy | Effectiveness Metric |
|---|---|
| Comprehensive risk assessment methodologies | 74% reduction in reportable breaches |
| Specialized clinical vulnerability assessments | 57% more critical vulnerabilities detected |
| Network micro-segmentation for legacy systems | 84% fewer lateral movement incidents |
| Tested, immutable backups | Reduced recovery time from 23 to 5 days |
| Role-specific security training | 67% fewer user error security incidents |

## 6 Conclusion

Building cyber resilience in healthcare demands a strategic approach that directly addresses the unique challenges posed by legacy systems, medical IoT vulnerabilities, and regulatory constraints. Implementing network segmentation, adopting Zero Trust principles, and deploying AI-driven security monitoring can substantially improve organizational security posture while maintaining essential operational capabilities. The stakes extend beyond mere data protection to encompass patient safety and maintaining trust in critical care systems. As threat actors evolve their techniques, healthcare organizations must commit to ongoing security improvements through comprehensive risk assessments, practical security enhancements, and cultivating a strong security-aware culture. By elevating cybersecurity to a strategic priority and integrating it thoroughly into core healthcare operations, organizations can develop the necessary resilience to withstand current and future cyber threats while delivering exceptional patient care.

## References

[1] Z-Cert, "Cybersecurity Threat Landscape for the Healthcare Sector," 2023. https://z-cert.nl/assets/downloads/DEF_EN-RapportDreigingsbeeld2023.pdf

[2] IBM, "Cost of a Data Breach Report," IBM, 2024. https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

[3] Steve Alder, "Healthcare Data Breach Statistics," HIPAA Journal, 2025. https://www.hipaajournal.com/healthcare-data-breach-statistics/#:~:text=There%20was%20no%20letup%20in,were%20exposed%20or%20impermissibly%20disclosed.

[4] Rob Sobers, "157 Cybersecurity Statistics and Trends," Varonis, 2024. https://www.varonis.com/blog/cybersecurity-statistics

[5] eHAction, "D7.3 – Practical cybersecurity guide for healthcare provider," eHAction, 2021. http://ehaction.eu/wp-content/uploads/2021/06/eHAction-D7.3-Common-security-framework-for-eHealth-_-for-adoption_19th-eHN.pdf

[6] ECRI, "Top 10 Health Technology Hazards for 2024," 2024. https://www.draeger.com/Content/Documents/Content/ECRI-2024-Top-10-Hazards-Executive-Brief.pdf

[7] "Health Care and Public Health Sector Cybersecurity Framework Implementation Guide," 2023. https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Documents/HPH-Sector-CSF-Implementation-Guide-508.pdf

[8] HIMSS, "2023 HIMSS Healthcare Cybersecurity Survey," 2024. https://gkc.himss.org/sites/hde/files/media/file/2024/03/01/2023-himss-cybersecurity-survey-x.pdf

[9] Department of Health and Human Services, "HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information," Federal Register, 2025. https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information

[10] Lee Barrett et al., "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients," 2023. https://405d.hhs.gov/Documents/HICP-Main-508.pdf