→ CyberResilience.com

US Healthcare and Cyber Risk

Trends, Threats, and Strategies

resilience

US Healthcare and Cyber Risk: Trends, Threats, and Strategies

Executive Summary

The U.S. healthcare sector faces an unprecedented cybersecurity crisis. In 2023, 168 million healthcare records were breached[1] – more than half the U.S. population's data compromised in a single year. With healthcare now the third most targeted sector and experiencing a 32% surge in ransomware attacks in 2024[2], the industry confronts threats that have evolved from simple data theft to sophisticated campaigns capable of paralyzing critical infrastructure.

The February 2024 Change Healthcare incident, which exposed 190 million records[3] and disrupted healthcare operations nationwide, demonstrates that cybersecurity failures can impact patient safety on a massive scale. Yet organizations that embrace strategic, data-driven approaches to cybersecurity are building genuine resilience and transforming security from a cost center into a strategic advantage.

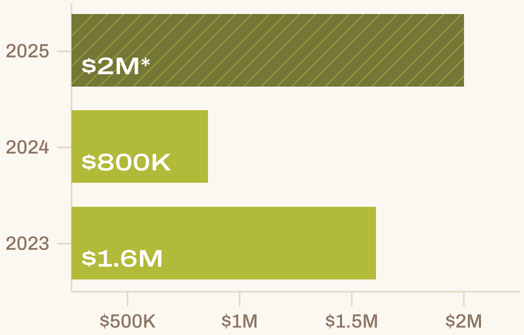
The Healthcare Cyber Crisis

Healthcare cybersecurity statistics reveal an industry under siege. The 239% increase in hacking-related breaches from 2018 to 2023, coupled with a 278% increase in ransomware incidents[1], represents a fundamental shift in how cybercriminals target the sector. Today, 80% of healthcare breaches are attributed to hacking[1], compared to just 25% in 2014. The average healthcare breach now costs over $15 million[5] – nearly double the global average.

In the first half of 2025, we saw demands for extortion fees as high as $4 million

Over the last three years, Resilience has marked a seesaw in the severity of claims among healthcare and social services clients. In 2023, the average severity of incurred losses per claim was $1.6 million, in 2024 it dropped to $800k. We cannot know the severity of claims for 2025 until those claims are settled, but there are indications that average severity may top $2 million. In the first half of 2025, we saw demands for extortion fees as high as $4 million; costs organizations must consider when patient health is at stake[10].

Severity of Cyber Claims in Healthcare



Data for 2025 is still developing

Source: Resilience claims data

Healthcare's emergence as a prime target stems from a convergence of valuable assets and structural vulnerabilities. Electronic Health Records contain identification and financial data that can be exploited for years across multiple attack vectors, making them far more valuable than credit cards on the dark web[6]. The sector's life-critical nature creates additional leverage for attackers, as hospitals cannot afford extended downtime when patients' lives hang in the balance.

Modern healthcare organizations face five interconnected attack vectors that have evolved beyond simple data theft: ransomware, supply chain attacks, insider threats, social engineering, and data disclosures. Ransomware has become the dominant threat, with aggressive groups like RansomHub[7], INC[8], BianLian[8], and Qilin[9] employing double extortion tactics that encrypt systems while stealing data for additional leverage. Analysis of healthcare-specific claims data reveals that causes of loss mirror broader cybersecurity patterns, with ransomware and transfer fraud representing the highest causes of financial impact[10].

Supply chain attacks represent perhaps the most insidious threat, capable of amplifying single incidents across vast networks of care providers, as demonstrated by the Change Healthcare breach affecting 190 million records. The healthcare industry collectively absorbed the financial impact of this incident, highlighting the sector's interconnected vulnerability to third-party compromises[10].

The threat landscape shows interesting patterns in both frequency and success rates. While BlackCat and Cl0p ransomware groups appeared most frequently in healthcare-related incidents, their success rates were lower than expected. Instead, actual successful attacks were more evenly distributed across groups like Interlock, Lockbit, and Medusa, suggesting that healthcare organizations may have developed some defensive capabilities against the most visible threats while remaining vulnerable to lesser-known actors[10].

Human error emerges as the most prominent point of failure across healthcare cyber incidents, but the specific vectors reveal concerning trends. Phishing attacks share the spotlight with data collection errors, particularly issues related to tracking pixels that inadvertently expose patient information. Vendor-related vulnerabilities, exemplified by the Change Healthcare incident, represent a growing attack surface, while faulty or incomplete backup systems continue to undermine recovery efforts when organizations fall victim to ransomware[10].

Insider threats have resurged since 2022, with 70% resulting from errors and privilege misuse rather than malicious intent[11]. Meanwhile, data disclosures continue growing in scale, with 275+ million records breached in 2024[12] despite fewer total incidents, indicating attackers are focusing on high-value targets.

THE PRIORITY PARADOX

Cybersecurity's Underestimated Threat

Despite these alarming trends, a concerning disconnect exists between the reality of cyber threats and leadership priorities. A 2025 survey of 250 U.S. healthcare business leaders revealed that cybersecurity ranked last among the top challenges hindering business success, with only 33% citing it as a primary concern. This places cybersecurity behind rising operational costs (53%), maintaining compliance (52%), and protecting patient data (40%)[13].

This prioritization gap becomes particularly troubling when considering the real-world impact. The same survey found that 19% of healthcare leaders admit a cyberattack has already disrupted patient care, while 52% believe a fatal cyber-related incident in a U.S. healthcare facility is inevitable within the next five years[13]. (And, in fact, in June 2025 there was a death in the UK that was partially credited to a cyberattack[14].) With 80% of healthcare organizations targeted by at least one cyberattack in the past year, the threat is not theoretical but immediate and ongoing[13].

The confidence levels among healthcare leaders may contribute to this misalignment. Despite facing constant attacks, 80% expressed confidence in their teams' ability to stop AI-powered cyberattacks. However, this confidence appears misplaced when examined against actual preparedness levels. Nearly a third of organizations don't regularly train employees on cyber threat response, only 53% run phishing simulations, and 17% lack current or effective incident response plans[13].

The gap extends to fundamental security practices. A concerning 40% of organizations do not conduct proactive IT risk assessments, with 18% having no plans to implement them within the next year. More than half acknowledge that outdated infrastructure would delay breach recovery, while 36% admit their current cybersecurity tools cannot protect cloud-based patient data[15].

Case Studies: Reactive vs. Proactive Approaches

Metro Regional Health Center (MRHC; not their real name), a mid-sized health system with approximately 3,000 employees, exemplifies the dangerous gap between perceived and actual cybersecurity posture common across the healthcare industry. Despite investing significantly in security tools, MRHC fell victim to a major cyber incident that revealed fundamental weaknesses in their risk posture[10].

Like many healthcare organizations operating with constrained resources, MRHC made reasonable decisions and tradeoffs that unfortunately created vulnerabilities. Their security assessments hadn't been updated in approximately four years, and while they had initially tested their endpoint protection, they had not maintained rigor through regular testing. Vendor risk management was documented primarily in policy documents rather than being actively monitored and was limited to a few top vendors. Most critically, their annual disaster recovery exercises consistently failed to meet recovery objectives, yet this weakness wasn't addressed due to competing priorities and limited resources.

MRHC had implemented backup systems and believed they were prepared for potential incidents. However, the attack revealed gaps in their preparation that even the most diligent organizations can inadvertently overlook. The threat actor not only accessed and copied their cyber insurance policy – providing insight into coverage limits and response procedures – but also managed to encrypt key clinical imaging files, which had not been included in their backup strategy. This dual exposure left the organization facing both operational disruption and significant leverage in ransom negotiations.

Additionally, MRHC's IT team, though skilled in general operations, lacked specialized cybersecurity expertise, making it challenging to identify and close gaps in their defenses. Critical controls like privileged access management, multi-factor authentication for privileged accounts, and next-generation firewalls were absent entirely. When they came under attack, MRHC discovered their assumed security posture bore little resemblance to their actual defensive capabilities.

This case study highlights the importance of continuous engagement with your risk posture including internal testing, tabletop exercises, and vendor risk management.

In stark contrast, another healthcare client – this one a $200+ million biotechnology company – achieved dramatically different outcomes through strategic, data-driven cyber risk management. Rather than relying solely on traditional compliance-focused approaches, they implemented a comprehensive cyber risk management program that redefined their security strategy. Financial risk quantification capabilities allowed them to model potential losses based on their unique profile, shifting leadership conversations from abstract security concepts to concrete economic impact assessments[16].

A prioritized action plan provided a roadmap of security improvements quantified in terms of actual risk reduction, giving the security leader defensible justification for budget allocation. Regular tabletop exercises provided practical validation of security controls. The transformation yielded measurable improvements: executive engagement increased as security discussions shifted from cost justification to ROI optimization, limited resources focused on the most significant risks, and the organization achieved clear demonstration of security program value.

Building Strategic Cyber Resilience

Healthcare organizations continue falling victim despite significant security investments because traditional approaches focus on regulatory compliance rather than actual risk reduction. HIPAA established baseline privacy protections but wasn't designed for modern cyber threats. Organizations deploying disconnected security tools without strategic coordination create gaps between systems, while annual assessments become check-box exercises using outdated measures of effectiveness.

Effective healthcare cybersecurity requires quantifying cyber risks in financial terms rather than relying on subjective ratings. Loss exceedance curves model potential impacts based on organization-specific factors, enabling leaders to understand exactly what risks could cost in business disruption, recovery expenses, and regulatory fines[15]. When expressed financially, security discussions shift from technical justifications to strategic investment decisions.

Strategic prioritization becomes possible when investments are evaluated based on actual risk reduction potential. Cyber action plans focus limited resources on controls delivering optimal risk reduction, while offering validation through realistic tabletop exercises that test capabilities against actual attack scenarios. Building organizational capability requires qualified security personnel, security champions across departments, and metrics demonstrating program value.

Healthcare organizations should prioritize Zero Trust principles that verify every access request and connection, every time, preventing lateral movement when attackers compromise accounts. Multi-factor authentication must extend to privileged accounts. Comprehensive backup testing must validate recovery capabilities and timeframes under realistic attack scenarios, while vendor risk management requires continuous evaluation of third-party security postures and understanding exposure to vendor risk.

Strategic investments should focus on advanced threat detection for social engineering made more effective by AI use, insider threat monitoring through behavioral analysis, and supply chain security requiring Zero Trust practices from all vendors. Twenty-four hour incident response with specialized healthcare expertise ensures rapid response to limit damage when incidents occur.

The Path Forward

Healthcare stands at a critical juncture where the 32% surge in ransomware attacks[2] demonstrates that reactive approaches are insufficient. Organizations focusing on compliance over risk management will remain vulnerable to sophisticated threats, while those embracing data-driven, business-aligned programs can build genuine resilience and gain competitive advantages through improved efficiency, reduced costs, and enhanced stakeholder trust.

> Healthcare stands at a critical juncture where the 32% surge in ransomware attacks[2] demonstrates that reactive approaches are insufficient

Based on the threat landscape analysis and case studies presented, healthcare organizations should prioritize several key recommendations:

Comprehensive Backup Strategy

Ensure all critical systems and data types are included in backup procedures, with particular attention to imaging files, databases, and system configurations. Regular testing should validate recovery capabilities and timeframes under realistic attack scenarios where primary systems are compromised.

Insurance Policy Security

Treat cyber insurance policies as sensitive documents that should be secured with the same rigor as other confidential materials. Threat actors increasingly target insurance information to understand coverage limits and response procedures.

Human Error Mitigation

Implement robust training programs that address phishing, social engineering, and proper data handling procedures. Pay particular attention to data collection practices, especially tracking pixel implementations that may inadvertently expose patient information.

Vendor Risk Management

Move beyond paper-based assessments to continuous monitoring of third-party security postures. Given the interconnected nature of healthcare systems, a single vendor compromise can impact multiple organizations simultaneously.

Financial Risk Quantification

Adopt methodologies that translate cyber risks into financial terms, enabling leadership to make informed investment decisions based on actual risk reduction potential rather than compliance requirements alone.

Incident Response Planning

Develop and regularly test incident response capabilities that account for the unique challenges of healthcare environments, including patient safety considerations and regulatory notification requirements.

The choice facing healthcare leaders is clear: remain vulnerable to threats where single vendor compromises can impact millions of Americans, or build the cyber resilience necessary to protect patients, preserve operations, and maintain trust in an increasingly hostile digital environment.

References

[1] HIPAA Journal. "2024 Healthcare Data Breach Report." January 30, 2025.

[2] TechTarget (McKeon, Jill). "Healthcare ranks as third-most targeted ransomware victim." January 22, 2025.

[3] Fierce Healthcare (Minemyer, Paige). "UnitedHealth estimates 190M people impacted by Change Healthcare cyberattack." January 24, 2025.

[4] HIPAA Journal. "Healthcare Data Breach Statistics." 2023.

[5] Hussain et al. "Healthcare Data Breaches: Insights and Implications." MDPI, 2020.

[6] Wired. "Why Health Data Is So Valuable." March 2022.

[7] Industrial Cyber (Check Point Research). "32% rise... as healthcare sector faces surge in cyberattacks." September 17, 2024.

[8] TechTarget. "Healthcare ranks as third-most targeted ransomware victim." January 22, 2025.

[9] AHA News. "HHS alerts health sector to cyberthreat from Qilin ransomware group." June 21, 2024.

[10] Internal analysis provided by Resilience (2025), on file with author.

[11] Verizon. "2024 Data Breach Investigations Report." May 1, 2024.

[12] HIPAA Journal. "Healthcare Industry Sees Sharp Increase in Advanced Email Attacks." September 26, 2023.

[13] MedWrench. “Report: Nearly 1 in 5 Leaders Say Cyberattacks Have Impacted Patient Care.” February 28, 2024.

[14] Reuters. “UK health officials say patient’s death partially down to cyberattack.” June 26, 2025.

[15] Fortified Health Security. 2024 Horizon Report: The State of Cybersecurity in Healthcare. January 2024.

[16] Resilience (Mealey, Rob). "Quantifying Cyber Risk for Strategic Business Alignment." March 5, 2025.

This material is not intended as a solicitation or offer of any Resilience insurance product. Any insurance coverage presented herein is for informational purposes only and does not constitute insurance advice. The terms and conditions, including any limitations, of your specific insurance policy will govern. The purchase of insurance is in no way tied to the purchase of security services. Nothing in these materials should be construed as an express or implied endorsement or recommendation of Resilience by any government or government agency. In the United States, insurance products are distributed by Ocrea Risk Services, LLC (NPN 19169260) d/b/a Resilience Cyber Insurance Solutions. Arceo Labs, Inc. d/b/a Resilience provides security services through its expert security team.