→ 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 2024, 275 million healthcare records were breached[1] – more than doubling from 2023 and representing the largest healthcare data exposure in U.S. history. 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.

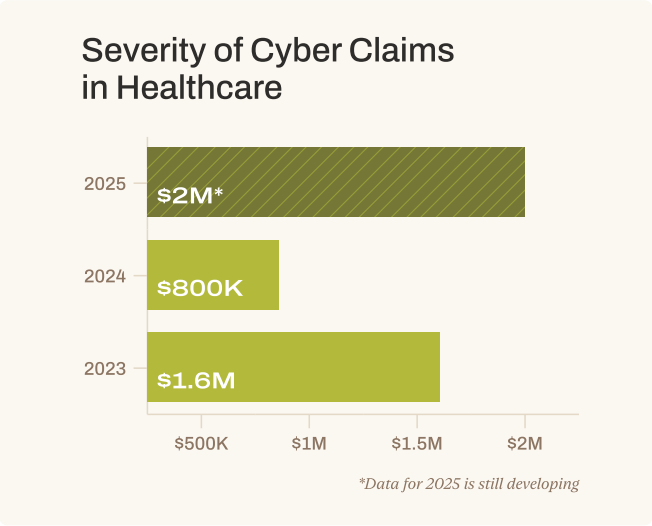
The February 2024 Change Healthcare incident, which exposed 190 million records[3] and disrupted healthcare operations nationwide, demonstrates that cybersecurity failures can impact patient safety on a massive scale. Healthcare organizations often grapple with uniquely complex and difficult security challenges – they maintain vast amounts of sensitive data, require near-zero downtime on digital systems, and must secure digital perimeters that sprawl across a high number of employees and devices.

Yet new analysis from Resilience reveals that organizations embracing specific, proven security practices are achieving measurable reductions in cyber risk. Analysis of healthcare-specific claims data and risk quantification modeling identifies five high-ROI controls that healthcare organizations can implement to meaningfully strengthen their security posture, transforming cybersecurity from a cost center into a strategic advantage.

The Healthcare Cyber Crisis

Healthcare cybersecurity statistics reveal an industry under siege, but Resilience claims data provides unique insight into the financial reality of cyber incidents in the sector. Over the last three years, the severity of claims among healthcare and social services clients has followed a concerning pattern. In 2023, the average severity of incurred losses per claim was $1.6 million. In 2024, it dropped to $800k, but topped $2 million in 2025, and Resilience saw demands for extortion fees as high as $4 million – costs organizations must consider when patient health is at stake[4].

> In 2025, we saw demands for extortion fees as high as $4 million



Source: Resilience claims data

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[4].

Analysis of healthcare-specific claims data in the Resilience portfolio reveals that causes of loss mirror broader cybersecurity patterns, with ransomware and transfer fraud representing the highest causes of financial impact[4]. Most critically, social engineering drove 88% of material losses in 2025, underscoring how threat actors increasingly prey on human error to gain access to sensitive data and mission-critical systems.

Human error emerges as the most prominent point of failure across healthcare cyber incidents in the Resilience portfolio. 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[4].

The Five Security Practices Delivering Highest ROI in Healthcare

Resilience conducted a data-driven analysis to understand which security tools and processes are actually moving the needle for healthcare organizations, identifying the practices that meaningfully reduce cyber risk and improve resilience. This research reveals not just what organizations are doing, but what's working, providing a benchmark for security leaders seeking the

highest-ROI levers to strengthen their posture.

The analysis is grounded in deep understanding of cyber risk in financial terms. By translating cyber exposure into value at risk through advanced risk quantification modeling, organizations can pinpoint the investments, processes, and security tools that deliver measurable reductions in potential loss, rather than relying on intuition or static benchmarks.

Within the healthcare industry, Resilience discovered five factors that are materially improving cyber resilience in the sector. These controls and processes represent actions that most healthcare organizations can implement to meaningfully reduce material risk.

1 Role-based access controls

Role-based access controls (RBAC) had a significant, measurable impact on improving cybersecurity across multiple industries analyzed, but its effect is particularly significant in healthcare. Privileged access protections help secure highly sensitive patient information and support critical compliance and regulatory requirements. For healthcare organizations with sprawling systems, diverse user types, and sensitive data being stored, formalizing access controls dramatically reduces risk exposure and limits the scale of a potential breach.

2 Dual authorization for wire transfers

A seemingly straightforward control, dual authorization is actually one of the most effective defenses against wire fraud. As threat actors continue to improve the pace and sophistication of social engineering attacks, requiring two people to sign off on wire transfers adds a crucial layer of redundancy that can easily disrupt fraud. Resilience data shows that this low-lift practice delivers an important protection against financially motivated attacks.

3 Breach and attack simulation on EDR platforms

Endpoint detection and response (EDR) tools are increasingly becoming a standard across healthcare, but many deployments contain blind spots. Organizations that routinely conducted breach and attack simulations (BAS) to stress-test their EDR systems were significantly better positioned to identify and resolve security gaps. This type of continuous testing and validation ensures that platforms are configured correctly, thereby meaningfully reducing risk.

4 MFA for email access

Multi-factor authentication (MFA) for email remains one of the highest-ROI controls for reducing cyber risk. It creates a crucial barrier against phishing and business email compromise attacks, which are common entry points for threat actors. Given the high-value, sensitive nature of Protected Health Information (PHI) that healthcare organizations are often responsible for, securing email platforms is an important step for reducing cyber risk. This foundational security layer continues to outperform many more complex or costly tools in terms of measurable impact on mitigating material risk.

5 Anti-fraud training

Social engineering remains a dominant driver of material losses, fueling 88% of material losses in the Resilience portfolio in 2025. In healthcare specifically, a security-focused culture including continuous, internal training against fraud and phishing scams delivered a high reduction in value at risk. This data underscores the centrality of humans in cybersecurity, particularly in healthcare, which is highly targeted by threat actors who frequently prey on human error to gain access to sensitive data and mission-critical systems. Prioritizing robust training and education represents one of the most effective levers for improving cyber resilience.

Beyond these five practices, Resilience analysis demonstrated the value of other specific controls in healthcare when compared to other industries. Maintaining immutable backups unlocked a particularly strong risk reduction on average in healthcare compared to other industries. Similarly, organizations that adopted a data governance committee yielded an outsized reduction in risk on average – more than three times the risk reduction in comparison to other industries.

Case Studies: Reactive vs. Proactive Approaches

Metro Regional Health Center (MRHC; not their real name), a mid-sized health system with approximately several thousand 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[4].

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 a number of 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. Notably,

MRHC lacked several of the high-ROI controls that Resilience data shows are most effective in reducing risk: they had not implemented role-based access controls, lacked MFA for privileged accounts, did not conduct breach and attack simulations on their EDR platform, and had not maintained continuous anti-fraud training for staff.

In stark contrast, another healthcare client – this one a mid-market 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[5].

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 to fall victim despite significant security investments because traditional approaches focus on regulatory compliance rather than actual risk reduction. HIPAA established baseline privacy protections, but it 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.

Resilience data demonstrates that healthcare organizations are making meaningful, data-driven improvements to mitigate material risk. By focusing on proven controls and processes, healthcare organizations can significantly strengthen their cyber resilience, even as the security landscape becomes more complex and turbulent.

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. When expressed financially, security discussions shift from technical justifications to strategic investment decisions.

Priority investments for healthcare organizations

Based on Resilience's analysis of which controls deliver the highest ROI in healthcare environments, organizations should prioritize the following investments:

- **Implement role-based access controls that formalize access permissions across sprawling healthcare systems**. For organizations with diverse user types and highly sensitive patient data, RBAC dramatically reduces risk exposure and limits the potential scope of breaches.
- **Require dual authorization for wire transfers to add a crucial layer of redundancy against increasingly sophisticated social engineering attacks.** This straightforward control delivers measurable protection against financially motivated fraud.
- **Conduct regular breach and attack simulations on EDR platforms to identify and resolve blind spots in endpoint protection.** Continuous testing and validation ensures that security tools are configured correctly and working as intended.
- **Deploy multi-factor authentication for email access to create a critical barrier against phishing and business email compromise**. Given that social engineering drives 88% of material losses, securing email platforms represents one of the highest-ROI controls available.
- **Establish continuous anti-fraud training programs that build a security-focused culture**. With social engineering remaining the dominant driver of material losses, prioritizing robust training and education represents one of the most effective levers for improving cyber resilience in healthcare.
- **Maintain immutable backups with comprehensive testing that validates recovery capabilities and timeframes under realistic attack scenarios.** Resilience data shows this control delivers particularly strong risk reduction in healthcare compared to other industries, especially when backups include all critical systems and data types with particular attention to imaging files, databases, and system configurations.
- **Create a data governance committee to provide oversight of sensitive information handling and security practices.** This organizational structure yields an outsized reduction in risk in healthcare – more than three times the risk reduction compared to other industries.

Complementary investments

Beyond these proven high-ROI practices, healthcare organizations should address two critical areas that repeatedly surface in claims data:

- **Vendor risk management that moves beyond paper-based assessments to continuous monitoring of third-party security postures.** The Change Healthcare incident demonstrated how a single vendor compromise can impact vast networks of care providers, with the healthcare industry collectively absorbing the financial impact.
- **Twenty-four hour incident response capabilities with specialized healthcare expertise to ensure rapid response that limits damage when incidents occur,** accounting for the unique challenges of healthcare environments including patient safety considerations and regulatory notification requirements.

The Path Forward

Healthcare stands at a critical juncture where the 32% surge in ransomware attacks[2] and the reality that social engineering drives 88% of material losses within the Resilience portfolio in 2025 demonstrate 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.

Resilience data reveals a brighter picture for healthcare organizations willing to take action. By focusing on the five proven controls that deliver the highest ROI, healthcare organizations can achieve measurable reductions in cyber risk and gain competitive advantages through improved efficiency, reduced costs, and enhanced stakeholder trust.

The choice facing healthcare leaders is clear: remain vulnerable to threats where single vendor compromises can impact millions of Americans and social engineering attacks drive the vast majority of material losses, or build the cyber resilience necessary to protect patients, preserve operations, and maintain trust in an increasingly hostile digital environment. The path to resilience is now clearer than ever, grounded in data-driven insights about which practices actually move the needle in reducing cyber risk.

References

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

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

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

4 Internal analysis provided by Resilience (2025), on file with author.

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