HealthManagement
Promoting Management and Leadership

KLAS Cybersecurity Report: Healthcare's Key Weaknesses

In the wake of the 2024 Change Healthcare cybersecurity breach, the healthcare industry faces heightened awareness of its digital vulnerabilities. This breach, with widespread consequences for patient safety, operations and financial stability, underscored the critical need for robust and proactive cybersecurity strategies. KLAS 2025 Healthcare Cybersecurity Benchmarking Study presents an updated landscape of how healthcare providers and payers are aligning with national cybersecurity frameworks and best practices. It reveals encouraging signs of resilience but also highlights areas where improvement is essential, particularly in asset and third-party risk management.

Resiliency Through Framework Adoption

The widespread adoption of cybersecurity frameworks signals increased industry awareness of evolving cyber threats. The study evaluates organisational alignment with several major frameworks, including the NIST Cybersecurity Framework 2.0 (NIST CSF 2.0), the Healthcare and Public Health Cybersecurity Performance Goals (HPH CPGs), the Health Industry Cybersecurity Practices (HICP) and the NIST AI Risk Management Framework (NIST AI RMF). These tools form the backbone of industry efforts to assess risk, strengthen resilience and mitigate future disruptions.

Must Read: ***The Escalating Cybersecurity Landscape in Healthcare***

Among the NIST CSF 2.0 functions, coverage of the Respond and Recover categories remains the highest. Organisations are investing in rapid response capabilities, indicating a prevailing assumption that breaches are not just possible but inevitable. However, the study shows significantly lower coverage in the Govern and Identify functions. Notably, for three consecutive years, Asset Management and Supply Chain Risk Management—critical categories within these functions—have had the lowest average coverage, barely exceeding 50%. This suggests that while organisations are prepared to react to incidents, many are underprepared to proactively manage vulnerabilities, particularly those linked to third-party vendors and complex supply chains.

The implications are significant. As the number of third-party breaches continues to rise, incomplete asset inventories and limited oversight of vendor systems increase systemic risk. This is further reinforced by findings from the HPH CPGs, which also report below-average coverage in areas linked to third-party cybersecurity requirements and network segmentation. Coverage of enhanced goals, many of which focus on long-term risk reduction and architecture improvements, remains low, especially where significant infrastructure investments are required.

Financial Correlation and Organisational Ownership

Beyond technical adoption, the study explores the financial and organisational dimensions of cybersecurity performance. A key insight is that organisations using NIST CSF 2.0 as their primary framework experience less volatility in their cybersecurity insurance premiums. Those that fully embraced the framework reported a modest average increase of 3% in premiums, compared to an 11% increase among those with limited or no adoption. This tangible financial benefit illustrates how structured, proactive cybersecurity can directly affect cost management and budgeting.

Nevertheless, implementation success depends on more than policy alignment. Ownership and governance models are critical enablers. For traditional cybersecurity domains, the presence of a strong Chief Information Security Officer (CISO) correlates with higher programme maturity. However, when it comes to emerging areas like artificial intelligence (AI), the study notes a shift. Instead of CISO-led control, effective AI risk management is found in models that encourage shared responsibility across clinical, operational, legal and data governance teams. This is essential as AI introduces unique challenges, such as data bias, transparency concerns and privacy risks, that extend beyond conventional security threats.

Despite its promise, AI risk management is in its infancy. Only a small subset of organisations reported on their use of the NIST AI RMF, and among these, coverage of the framework's functions—Govern, Map, Measure and Manage—remains limited. Most participants are still establishing governance foundations and beginning to map out risks. The broader involvement of stakeholders is essential to advance from foundational stages toward comprehensive, ethical AI implementation.

Operational Gaps and Strategic Next Steps

Although healthcare organisations report strong communication practices during cybersecurity incidents, the study finds inconsistencies in long-term recovery execution. While incident recovery communications receive high marks, recovery plan execution does not keep pace. This gap can impede the full restoration of operations and slow the return to normal care delivery. Coordinating cross-functional teams, aligning resource allocation and synchronising recovery timelines remain areas in need of further development.

Another critical gap identified is the security of medical devices. The HICP assessment shows that while basic email protections and identity management systems are widely implemented, the security of connected medical devices lags behind. These devices, many of which are outdated or unsupported, pose serious risks if not adequately segmented from the core IT infrastructure. Network segmentation, while complex and costly, is a proven strategy to mitigate these risks. Yet this approach is underutilised, with network segmentation ranking as the lowest-covered Enhanced Goal within the HPH CPGs.

For healthcare organisations aiming to bolster their cybersecurity postures, the study points to several practical steps. These include creating centralised asset inventories, enforcing supplier security standards and implementing role-based access controls. In the AI space, recommended practices include establishing governance committees with multi-disciplinary representation, maintaining central repositories for AI vendor data and instituting routine reassessments of risk based on evolving capabilities.

The 2025 Healthcare Cybersecurity Benchmarking Study reflects an industry at a pivotal moment. While improvements in incident response and communications demonstrate growing maturity, persistent gaps in asset and third-party risk management expose healthcare organisations to unnecessary risk. The study affirms that adopting recognised frameworks like NIST CSF 2.0 and the HPH CPGs can lead to measurable improvements—not only in operational resilience but also in financial outcomes. Moving forward, broader stakeholder engagement, especially in managing AI risks, will be essential to ensure that cybersecurity strategies evolve in parallel with emerging technologies. By closing these gaps and embedding cybersecurity into all facets of operations, healthcare organisations can better protect patients, data and the integrity of care delivery.

Source: KLAS

Image Credit: iStock

Published on : Thu, 24 Apr 2025