HealthManagement.org

LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES VOLUME 24 • ISSUE 3 • € 22

Virtual and Retail Healthcare

ACCESS - HOME CARE - EQUITY- EXPERIENCE - EFFICIENCY - CASES

KLAS 2024 Cybersecurity Benchmark in Healthcare

The latest updated and comprehensive study by Censinet, KLAS Research, and the AHA highlights significant cybersecurity challenges in healthcare. It reveals that organisations remain better prepared for incident response than for identification. They are reactive in risk management, especially in supply chain and medical device security. The study underscores the need for proactive measures and clear cybersecurity leadership to enhance protection and reduce financial impacts.

KLAS RESEARCH

Information Technology & Services | Utah, USA

key points

- Healthcare organisations does better in incident response than in proactive risk management, especially in supply chain and asset management.
- Organisations are strong in the NIST Respond function but struggle with the Identify function, particularly in supply chain risk management.
- Email systems have high protection, while medical device security is weak, with coverage barely above 50%.
- Clear infosec leadership improves network and medical device security, highlighting the importance of assigning responsibility.
- NIST CSF adoption: Most organisations use NIST CSF, which is correlated with lower cybersecurity insurance premiums.

The digital transformation of the healthcare sector has brought remarkable benefits, including enhanced patient care, streamlined operations, and improved data management. However, this shift has also introduced significant cybersecurity challenges. To address these concerns, Censinet, KLAS Research, and the American Hospital Association (AHA) have published reports in 2023 and 2024 to establish collaborative cybersecurity benchmarks for the healthcare industry. The 2023 study included 48 healthcare organisations; the 2024 study evaluated 54 healthcare organisations—ranging from small critical access hospitals to large academic medical centres and including several payers and IT vendors—to assess their adherence to the NIST Cybersecurity Framework (NIST CSF) and Health Industry Cybersecurity Practices (HICP).

This article explores the study's key findings (KLAS, 2024), focusing on the maturity of healthcare organisations in managing cybersecurity risks, their alignment with HICP guidelines, and their cybersecurity investments.

NIST Maturity: Reactive Versus Proactive Approaches

The study reveals that healthcare organisation practices remained similar from 2023 to 2024, with organisations predominantly adopting a reactive rather than proactive stance when it comes to cybersecurity, especially in identifying and managing risks. Across the NIST CSF's five functions—Identify, Protect, Detect, Respond, and Recover—organisations exhibited the highest average coverage in the Respond function. This is mainly due

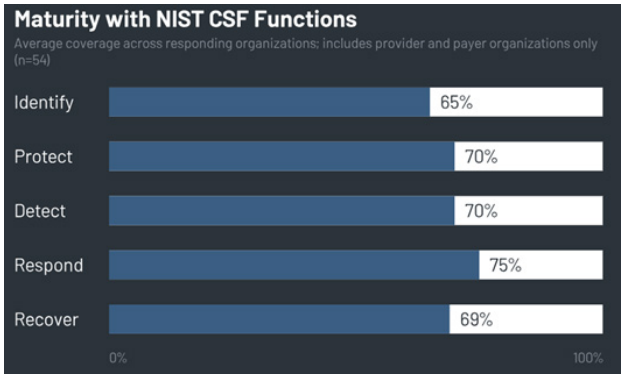

Figure 1. Maturity with NIST Guidelines.

to maturity in the Analysis category, which involves investigation, forensics, categorisation, analysis, and understanding of cybersecurity incidents. Almost all organisations reported robust investigation practices following detection system notifications, with a majority demonstrating at least 70% coverage in this area.

Conversely, the Identify function showed significant gaps, particularly in the Supply Chain Risk Management, Asset Management, and Risk Management subcategories. In the 2023 study, over 40% of organisations were non-compliant in conducting response and recovery planning with suppliers and third-party providers. Supply Chain Risk Management emerged as the subcategory with the lowest coverage across all five NIST functions. The challenge of coordinating cybersecurity testing with third-party suppliers and managing those processes appears to exceed the maturity level of many healthcare organisations. Despite these challenges, the data indicates that organisations with better supply chain risk management report lower year-to-year increases in cybersecurity insurance premiums, suggesting a potential benefit to improvement.

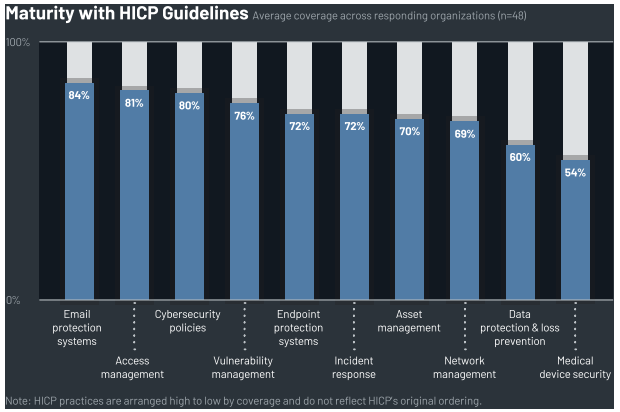

Figure 2. Maturity with HICP Guidelines.

> "The disparity between email protection and medical device security underscores the need for focused improvements in the latter area, with average coverage for medical device security barely exceeding 50%."

Steady But Unbalanced Alignment with HICP Guidelines

Healthcare organisations' alignment with HICP guidance also remained steady from 2023 to 2024. Coverage is mixed, with organisations demonstrating substantial strengths in email system protection but significant vulnerabilities in medical device security. The 2023 study showed that organisations of all sizes reported high coverage for email protection—in most metrics, over 50% of organisations achieved 100% coverage. However, the landscape for medical device security was far more concerning. Average coverage for medical device security barely exceeded 50%, highlighting a critical vulnerability within the industry.

While almost all organisations ensure medical devices are wiped of data when decommissioned, less than two-thirds configure medical devices to allow only known processes and executables to run, and this configuration is often applied selectively. The disparity between email protection and medical device security underscores the need for focused improvements in the latter area. Interestingly, the study found that organisations with full information security ownership of network management and medical device security report significantly higher coverage in these areas. This correlation suggests that granting clear responsibility and ownership to information security leadership can enhance cybersecurity practices.

Cybersecurity Investments and Resource Allocation

Over the past few years, healthcare organisations have seen significantly more investment in

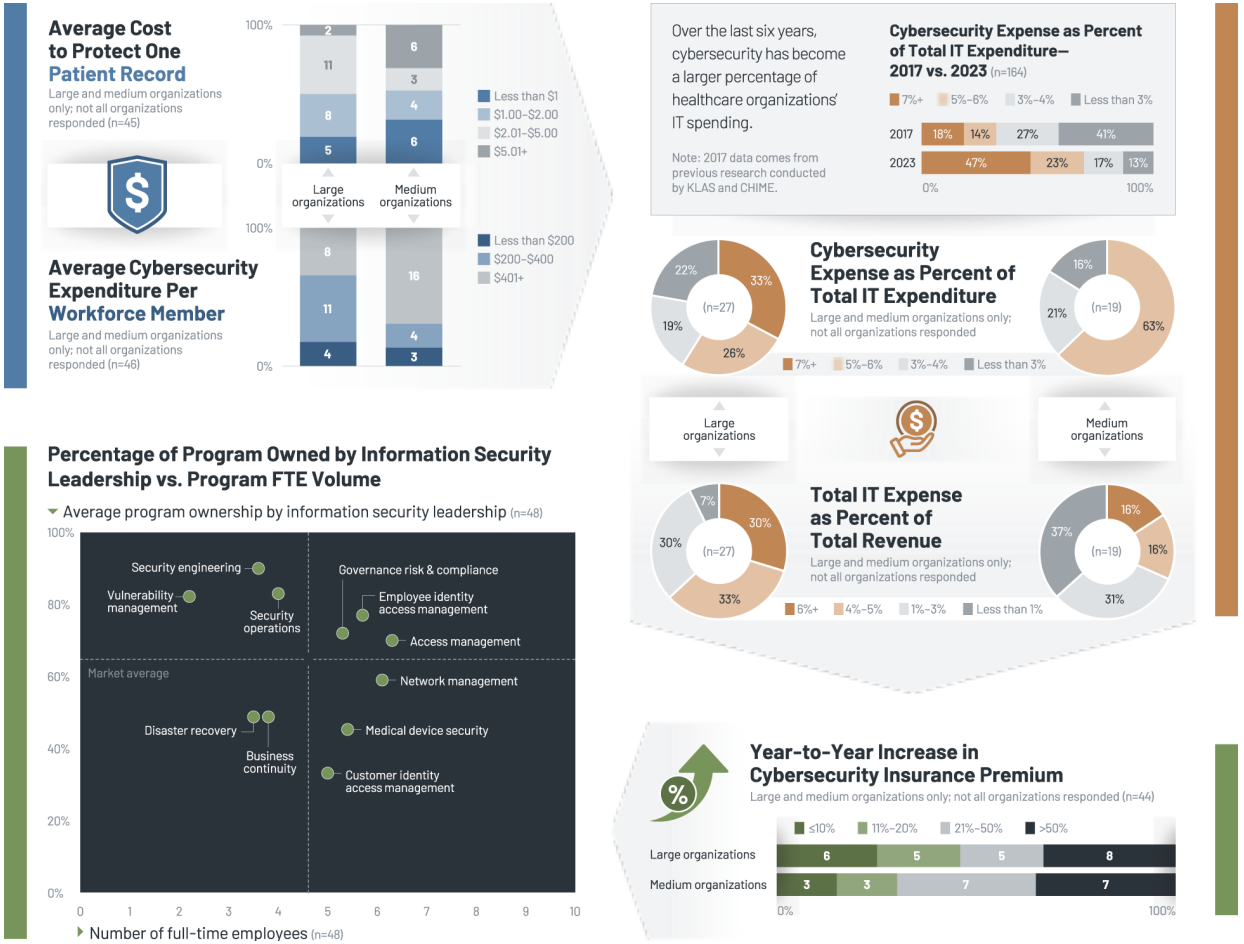

Figure 3: Snapshot of Cybersecurity Expense, 2023 data.

cybersecurity programmes. The 2023 study examined cybersecurity spending compared to 2017 data, and more than 40% of organisations are now spending more than 7% of their IT budget on cybersecurity, compared to less than 3% six years ago. Not surprisingly, larger organisations have more resources to spend than others.

Different cybersecurity programmes also receive different FTE volumes, with access management having more resources than areas like vulnerability management.

Cybersecurity Ownership Is Crucial to Preparedness

Data from both years shows that organisations that have security leaders overseeing cybersecurity programmes tend to have more coverage when measured against NIST and HICP metrics. While the industry average for NIST CSF and HICP coverage is about 70%, organisations that assign information security leaders higher percentages of programme ownership achieve above-average cybersecurity coverage. In particular, higher programme ownership is correlated with significantly higher coverage in the HICP areas of Endpoint Protection Systems and Data Protection and Loss Prevention. Among organisations that participated in both the 2023 and 2024 studies, those that increased cybersecurity programme ownership under their CISO almost always saw increased coverage.

Most organisations use NIST as their primary cybersecurity framework (with many using more than one framework), and they report lower year-over-year increases to their cybersecurity insurance premiums than those not using NIST. In other words, the insurance cost for organisations using primarily NIST is growing slower than for organisations not using NIST.

Conclusion

The collaborative studies by Censinet, KLAS Research, and the AHA provide crucial insights into the current state of cybersecurity in the healthcare sector. While healthcare organisations demonstrate maturity in incident response, particularly in analysis and investigation, they remain largely reactive rather than proactive in risk management, especially

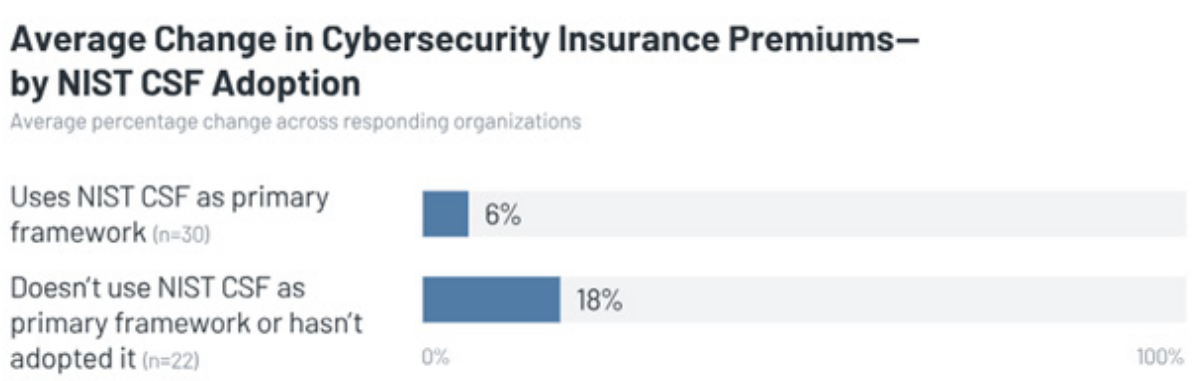

Figure 4: Cybersecurity Insurance Premium Increase by NIST CSF Adoption

concerning supply chain and asset management. Email protection is robust across the board, but medical device security is a critical area requiring substantial improvement. The studies underscore the importance of clear ownership and governance in enhancing cybersecurity practices. By aligning cybersecurity responsibilities with information security leadership and investing in proactive risk management, healthcare organisations can better safeguard their digital infrastructure and reduce the financial impacts of cybersecurity threats.

Conflicts of Interest

None.

references

KLAS Research (2024) Healthcare Cybersecurity Benchmarking Study. Available at: https://klasresearch.com/report/healthcare-cybersecurity-benchmarking-study-2024-improving-cybersecurity-preparedness-through-nist-csf-and-hicp-best-practices/3448

KLAS Research (2023) Healthcare Cybersecurity Benchmarking Study. Available at: https://klasresearch.com/report/healthcare-cybersecurity-benchmarking-study-how-aligned-is-the-industry-to-nist-and-hicp-best-practices/3102


HealthManagement
Promoting Management and Leadership