KLAS RESEARCH | Healthcare IT Insights

CENSINET

American Hospital Association™
Advancing Health in America

Health-ISAC™
Collaborating for Resilience in Healthcare

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Scottsdale Institute
COLLABORATION | EDUCATION | NETWORKING

Partnered Report

Healthcare Cybersecurity Benchmarking Study 2025

Strengthening Healthcare Cybersecurity Resiliency Through Industry Best Practices & Cybersecurity Frameworks

April 2025

Healthcare Cybersecurity Benchmarking Study 2025

Strengthening Healthcare Cybersecurity Resiliency Through Industry Best Practices & Cybersecurity Frameworks

The 2024 Change Healthcare cybersecurity breach had detrimental and unprecedented ripple effects across the healthcare industry. The breach alerted many to how interwoven—and often fragile—the connections are between health systems, payers, and third-party vendors. A major disruption at any point in the ecosystem can directly impact care operations, financial stability, and patient safety across the entire industry. To address ongoing and evolving cybersecurity threats, many organizations are adopting and implementing cybersecurity frameworks and best practices, such as 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). High coverage of these frameworks and best practices is a strong indicator of an organization's cybersecurity maturity and preparedness.

Providing an update to previous research, this Healthcare Cybersecurity Benchmarking Study examines organizations' self-reported coverage within the frameworks and best practices listed above. In particular, it looks at the gaps that persist around third-party risk management and asset management. In addition, key metrics from participating organizations regarding cybersecurity insurance premiums, IT and cybersecurity spending/staffing, and other data was analyzed for correlations. Data in the report comes from 69 healthcare and payer organizations who were surveyed September–December 2024.

This research is a collaboration between the following organizations:

KLAS RESEARCH

CENSINET

American Hospital Association™ Advancing Health in America

Health-ISAC™ Collaborating for Resilience in Healthcare

Healthcare & Public Health Sector Coordinating Councils PUBLIC PRIVATE PARTNERSHIP

Scottsdale Institute COLLABORATION | EDUCATION | NETWORKING

Key Findings

Key insights from the study are outlined below. Further insights for each framework or set of guidelines are examined in the sections that follow.

NIST CSF 2.0

- Healthcare organizations continue to be more reactive than proactive in their approach to cybersecurity
- Like last year, the Respond and Recover functions have the strongest coverage—organizations are preparing for when, not if, they will need to rapidly respond to cybersecurity incidents
- Also like last year, Supply Chain Risk Management (previously a category under the Identify function; now a category under the new Govern function) and Asset Management (under the Identify function) are the areas most in need of improvement, especially as third-party breaches increase
- Those using NIST CSF 2.0 as a primary framework report lower cybersecurity insurance premium increases year-over-year

HPH CPGs

- Analysis of the HPH CPGs shows that, as with NIST CSF 2.0, third-party risk management and asset management are both opportunities for improvement

NIST AI RMF

- Respondent organizations are starting with AI governance as a foundation for AI risk management and are still in the early stages of AI risk remediation
- Although cybersecurity programs see more success when there is high CISO ownership, AI programs see more success with a different approach; to ensure safe and ethical AI use, organizations must implement cross-departmental ownership and involve stakeholders outside of cybersecurity (since AI also presents risks associated with data bias and transparency, clinical workflows, privacy, and ethics)

HICP

- HICP coverage is similar to last year—medical device security continues to be a critical gap

What's Not Included in This Summary Report?

This report summarizes key findings. Participants in the Healthcare Cybersecurity Benchmarking Study receive the full report, which includes:

- A detailed analysis of financial ratios and operational metrics (e.g., percentage of IT budget and workforce allocated to cybersecurity)
- Peer comparisons of IT and cybersecurity organizational structure and functional ownership
- Insight into the root cause drivers of coverage gaps

Participating organizations also gain exclusive benefits, including personalized remediation plans, tailored reports to prioritize cybersecurity investments and facilitate executive and board communications, and enhanced peer group comparisons to fully contextualize their performance.

To participate in next year's Benchmarking Study, please email benchmarks@censinet.com.

NIST CSF 2.0

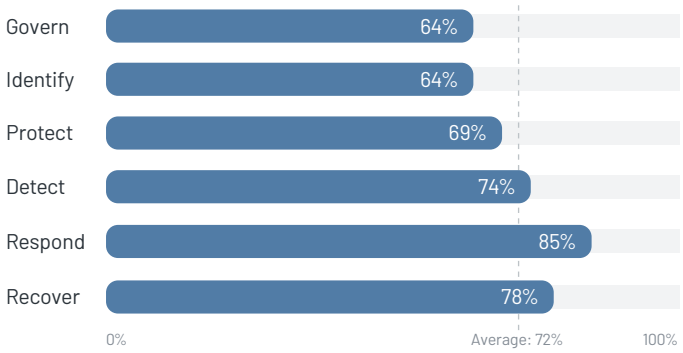
Cross-industry cybersecurity framework consisting of six functions (previous versions of the framework had five functions); recommended by the HHS 405(d) Program and by government entities like OCR for HIPAA compliance

Organizations Continue to Be More Reactive Than Proactive in Their Approach to Cybersecurity

Coverage of the NIST CSF 2.0 functions is similar to that of the NIST CSF 1.1 functions reported on in previous years. There are two notable insights. First, the Govern function (a new addition to NIST CSF 2.0) and Identify function tie for the lowest coverage—this marks the third consecutive year that the Identify function has had the lowest coverage. Second, the coverage disparity between the Respond function and the other functions has become more pronounced. As the likelihood of cybersecurity breaches increases for both healthcare organizations and their third-party vendors, many are preparing for when, not if, they will need to employ incident response, disaster recovery, and business continuity strategies.

Coverage of NIST CSF 2.0 Functions

Average coverage across responding organizations (n=69)



Supply Chain Risk Management & Asset Management Remain the NIST CSF 2.0 Categories with Lowest Coverage

For the third consecutive year, Supply Chain Risk Management (previously a category under the Identify function; now a category under the Govern function) and Asset Management (a category under the Identify function) have the lowest coverage, with coverage at an average of just over 50% across respondents. The low coverage for Supply Chain Risk Management is

Coverage of Supply Chain Risk Management & Asset Management

Average coverage across responding organizations (n=69)

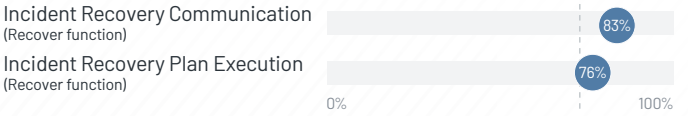
especially concerning, as the number of third-party breaches in the healthcare industry has continued to increase year-over-year. Asset management, which is closely linked to third-party and supply chain management, requires organizations to maintain a detailed inventory and understanding of all assets, including third-party hardware, software, data, and storage systems. This knowledge allows organizations to identify and address vulnerabilities in third-party products and services and mitigate potential risks.

Respond & Recover Are NIST CSF 2.0 Functions with Highest Coverage; Organizations Are Prepared to Quickly Respond to Cybersecurity Incidents but Can Further Enhance Long-Term Resiliency

The Respond function has the highest coverage; respondent organizations report having well-defined incident response procedures, including strong incident mitigation tactics and clear communication protocols. However, many organizations have more mature processes for immediate responses compared to processes for long-term recovery and business continuity. While organizations generally excel at internal and external communication during recovery efforts—thus ensuring that stakeholders are informed about status and progress—recovery plan execution is an area for improvement. Organizations could strengthen their coordination of various teams, resources, and activities as they work to fully restore operations. As organizations increase their coverage of supply chain management, it is likely they will gain a more complete understanding of the areas in which they need to recover.

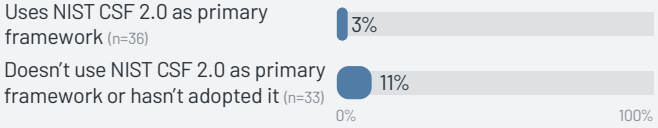
Coverage of Incident Recovery Communication & Incident Recovery Plan Execution

Average coverage across responding organizations (n=69)



Average Annual Change in Cybersecurity Insurance Premiums—by NIST CSF 2.0 Adoption

Average percentage change across responding organizations



Primary Adoption of NIST CSF 2.0 Is Connected to Lower Cybersecurity Insurance Premium Growth

Organizations that invest in higher cybersecurity preparedness see tangible benefits. In this study, those who have adopted NIST CSF 2.0 as their primary cybersecurity framework see lower year-over-year increases to their cybersecurity insurance premiums. The 2024 study showed similar results (for those who adopted NIST CSF 1.1 as their primary framework), underscoring that robust cybersecurity preparedness can translate into tangible benefits.

HPH CPGs

Comprised of a set of essential and a set of enhanced cybersecurity performance goals developed by HHS, in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA) and industry partners

A First Look Reveals Similar Gaps in Third-Party Risk Management & Asset Management

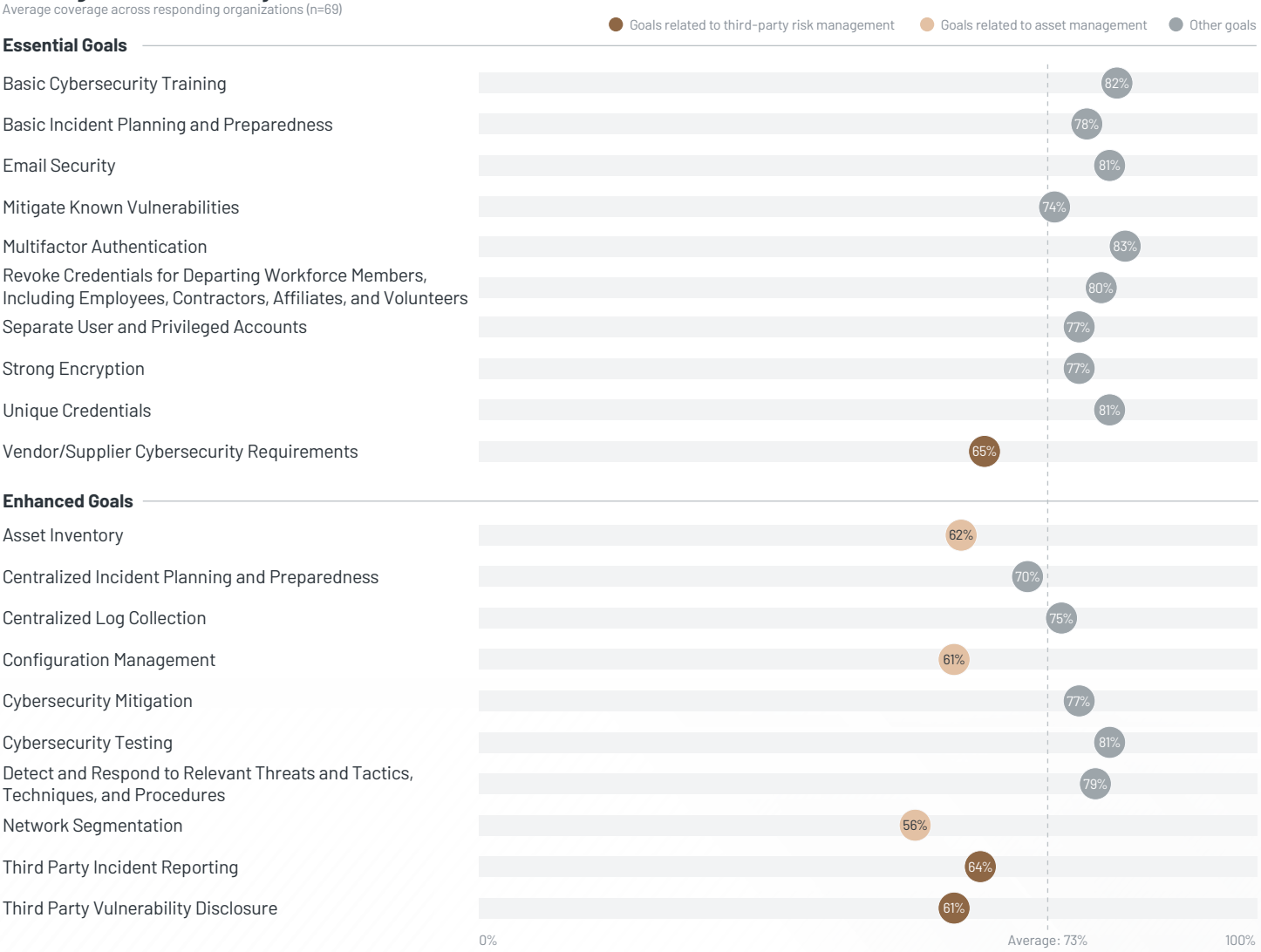
This 2025 report marks the first time the Healthcare Cybersecurity Benchmarking Study has looked at coverage of the HPH CPGs, and analysis shows that—as with NIST CSF 2.0—third-party risk management and asset management are opportunities for improvement. The Essential Goals have higher coverage overall, with the exception being Vendor/Supplier Cybersecurity Requirements, which is well below average. The Enhanced Goals, which include several outcomes related to third-party risk management and asset management, also have coverage that falls well below average. Network Segmentation, one of the Enhanced Goals, has the lowest coverage across both goal types. Network segmentation can be very complex, requiring significant investments in infrastructure; however, it can compensate for, and mitigate, asset vulnerabilities. For example, segmenting medical or legacy devices that no longer receive security patches helps restrict the devices' access to the internet and other critical systems, thus lowering risk.

Coverage of HPH CPGs

Average coverage across responding organizations (n=69)

Coverage of HPH CPGs—by Individual Essential & Enhanced Goals

Average coverage across responding organizations (n=69)



NIST AI RMF

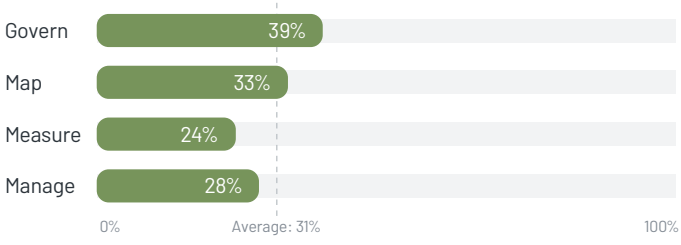
Cross-industry framework consisting of four functions designed to help organizations assess and manage AI-specific risks and ensure responsible, trustworthy, and secure AI adoption

Organizations Are in Early Stages of AI Risk Management; Broad Ownership from Multiple Stakeholders Is Critical for Safe, Secure & Ethical AI Use

This report is also the first Healthcare Cybersecurity Benchmarking Study to look at coverage of NIST AI RMF. The 13 organizations that opted to respond are in the early stages of AI risk management, and many face challenges with risk remediation due to uncertainties surrounding AI. Although AI presents unprecedented opportunities to benefit healthcare organizations, it also introduces unique cybersecurity risks. Respondent organizations have started implementing governance around the use, development, and deployment of AI, a process that aligns with the Govern function of NIST AI RMF. As AI programs grow and mature, organizations should establish cross-departmental ownership that includes a broad set of stakeholders in order to achieve safe, secure, and ethical use of AI. This recommendation contrasts with traditional cybersecurity risk management, where high program ownership is typically maintained by the CISO.

Coverage of NIST AI RMF Functions

Average coverage across responding organizations (n=13)



Managing AI Risk: Emerging Best Practices from Censinet

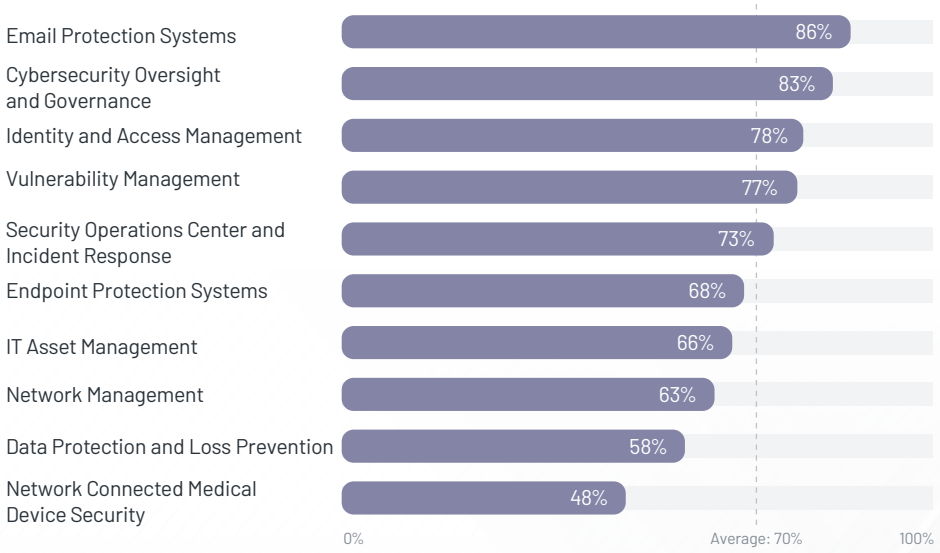
- Establish a dedicated AI governance committee with broad stakeholder representation across business functions
- Determine which vendors have AI capabilities that require additional diligence
- Identify which subject matter experts need to review which AI risks, and create a streamlined process for subject matter expert review
- Maintain a central repository of vendors and products that use AI; also track diligence efforts and risk findings in a central repository
- Perform reassessments on AI vendors based on criticality and/or upon change in functionality

HICP | Set of 10 healthcare-specific cybersecurity mitigating practices based on the top threats to healthcare cybersecurity; recommended by HHS 405(d) Program to improve cybersecurity preparedness

Organizations Continue to Have Strong Email Protection Systems but Have Significant Gaps Around Medical Device Security

The HICP-assessment portion of the Healthcare Cybersecurity Benchmarking Survey was optional, resulting in a lower sample size. Coverage of HICP is close to the levels reported in past years, with most organizations having email protection systems in place but room for improvement with medical device security. Coverage for the latter has lagged the other mitigating practices for three consecutive years and supports findings from NIST CSF 2.0 and the HPH CPGs that third-party risk management and asset management still lag behind in industry coverage.

Coverage of HICP Average coverage across responding organizations (n=32)



Report Information

About This Report

The 2025 Healthcare Cybersecurity Benchmarking Study is co-sponsored by Censinet, KLAS Research, the American Hospital Association, the Health Information Sharing and Analysis Center, the Healthcare and Public Health Sector Coordinating Council, and the Scottsdale Institute. This study is the industry's first and only collaborative initiative to establish robust, objective, and actionable peer benchmarks to strengthen cybersecurity maturity and resiliency across the healthcare sector.

Study Sponsors

KLAS RESEARCH

CENSINET

American Hospital Association™
Advancing Health in America

Health-ISAC™
Collaborating for Resilience in Healthcare

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Scottsdale Institute
COLLABORATION | EDUCATION | NETWORKING

About

KLAS RESEARCH

Driven by a mission to improve the world's healthcare, KLAS is a healthcare-focused research firm whose data helps provider, payer, and employer organizations make informed software and services decisions. Powered by insights and experiences discovered in the 25,000+ interviews with healthcare organization leaders and end users that KLAS conducts each year, KLAS' work creates transparency in the healthcare market and acts as a catalyst for software vendors and services firms to improve their offerings.

CO-AUTHOR
Chloe Jensen
chloe.jensen@KLASresearch.com

CO-AUTHOR
Steven Low
steven.low@KLASresearch.com

CO-AUTHOR
Ciera Black Walker
ciera.walker@KLASresearch.com

WRITER
Sarah Brown

DESIGNER
Nikki Christensen

Our Mission

Improving the world's healthcare through collaboration, insights, and transparency.

365 S. Garden Grove Lane, Suite 300
Pleasant Grove, UT 84062

Ph: (800) 920-4109

For more information about KLAS, please visit our website: **engage.KLASresearch.com**

Cover image:
© K.Mongkol / Adobe Stock

About

CENSINET

Censinet®, based in Boston, MA, takes the risk out of healthcare with Censinet RiskOps, the industry's first and only cloud-based risk exchange of healthcare organizations working together to manage and mitigate cyber risk. Purpose-built for healthcare, Censinet RiskOps™ delivers total automation across all third party and enterprise risk management workflows and best practices. Censinet transforms cyber risk management by leveraging network scale and efficiencies, providing actionable insight, and improving overall operational effectiveness while eliminating risks to patient safety, data, and care delivery. Censinet is an American Hospital Association (AHA) Preferred Cybersecurity Provider. Find out more about Censinet and its RiskOps platform at censinet.com.

CEO & FOUNDER
Ed Gaudet
egaudet@censinet.com

CHIEF PRODUCT OFFICER
Paul Russell
prussell@censinet.com

CHIEF INFORMATION SECURITY OFFICER
David Woska, PhD
dwoska@censinet.com