Censinet, KLAS, and American Hospital Association Publish the 2025 Healthcare Cybersecurity Benchmarking Study

Co-Led by Censinet, KLAS, AHA, Health-ISAC, HSCC, and The Scottsdale Institute, 2025 Benchmarking Study Details State of Healthcare Cyber Maturity, Preparedness

BOSTON, MA, UNITED STATES, April 14, 2025 /EINPresswire.com/ -- Censinet, the leading provider of healthcare risk management solutions, and KLAS Research, healthcare's leading research and insights firm, today announced the publication of the Executive Summary from the 2025 Healthcare Cybersecurity Benchmarking Study. Co-sponsored by Censinet, KLAS Research, the American Hospital Association (AHA), Health Information Sharing and Analysis Center (Health-ISAC), the Health Sector Coordinating Council (HSCC), and The Scottsdale Institute, The Healthcare Cybersecurity Benchmarking Study is the industry's only collaborative initiative to establish robust, objective, and actionable peer benchmarks to strengthen the health sector's cyber preparedness, maturity, and resiliency. The Executive Summary for the 2025 Benchmarking Study can be downloaded now on the Censinet website here.

> "As the industry navigates growing complexity, these benchmarks serve as a clear, impartial compass for strategic investment in cybersecurity and risk management."
>
> *Steve Low, President of KLAS Research*

"Censinet is honored to deliver findings from the 2025 Healthcare Cybersecurity Benchmarking Study in partnership with our esteemed co-sponsors," said Ed Gaudet, CEO and Founder of Censinet. "We deeply thank the nearly 200 healthcare organizations that have participated in the Benchmarking Study since 2023, and we applaud their dedication to protect patient safety from cyber threats. The Benchmarking Study is a testament to the industry's shared dedication and commitment to strengthening the sector's cyber resiliency—we are truly Stronger Together."
With 69 healthcare delivery organizations (HDOs) participating in the third annual Healthcare Cybersecurity Benchmarking Study, the 2025 Study findings expand upon the comprehensive set of peer benchmarks established in the landmark 2023 and 2024 Benchmarking Studies. This year's study also includes updated industry coverage and insights across the NIST Cybersecurity Framework 2.0 (CSF 2.0), the HHS Healthcare and Public Health Cybersecurity Performance Goals (HPH CPGs), the NIST AI Risk Management Framework (AI RMF), Health Industry Cybersecurity Practices 2023 (HICP 2023), and key Organizational Metrics.

“KLAS is honored to once again co-lead this industry-defining initiative with Censinet and our partners,” said Steve Low, President of KLAS Research. “The 2025 Benchmarking Study not only sheds light on the evolving threat landscape and the state of our collective preparedness, but also equips healthcare organizations with critical, data-driven insights to drive targeted, continuous improvement in cyber resiliency. As the industry navigates growing complexity, these benchmarks serve as a clear, impartial compass for strategic investment in cybersecurity and risk management.”

Key findings from the 2025 Benchmarking Study include:

 For the third year in a row, healthcare cybersecurity is still better positioned to be reactive rather than proactive, as Govern and Identify coverage lagged behind all other NIST CSF 2.0 Functions.
 Supply Chain Risk Management still ranks last in coverage across all NIST CSF 2.0 Categories, a worrying trend in light of the record-breaking number of healthcare third-party breaches, including the Change Healthcare cyberattack in Feb. 2024.
 A first look at HPH CPG coverage reveals similar gaps in supply chain / third-party risk management as well as low coverage in Asset Management and Network Segmentation.
 Organizations using NIST CSF as their primary security framework continue to report lower year-over-year cyber insurance premium cost growth.
 Low adoption of the new NIST AI RMF indicates that healthcare organizations are still in the early phases of AI adoption, with current efforts focused more on policy development and governance than on proactive risk management.

“The Healthcare Cybersecurity Benchmarking Study plays a critical role in uniting the healthcare sector against a growing surge of cyber threats, enabling U.S. hospitals and health systems to better anticipate, withstand, and recover from cyberattacks through collaboration and data-driven insight,” said John Riggi, National Advisor for Cybersecurity and Risk, the American Hospital Association. “Today’s cyber adversaries are increasingly targeting the sector’s most mission critical direct and third-party assets—these are not just digital crimes: they represent a direct threat to patient care and people’s lives. The Benchmarking Study helps equip the health sector with the knowledge and collective strength needed to safeguard healthcare operations, and, most importantly, protect the patients and communities we serve.”

Participation in the Benchmarking Study entitles healthcare organizations to exclusive benefits available free of charge, including:

 Enterprise assessments and peer benchmarks for NIST CSF 2.0, HPH CPGs, NIST AI RMF, HICP 2023, and Operational Metrics (e.g. cyber spend % of total IT spend).
 Board-ready reporting to help prioritize, plan, and justify cybersecurity resources and investment.
 Risk remediation plans tailored to each organization to identify and close critical gaps in

security controls, policies, and procedures.
 Access to both the Executive Summary and Full Reports, published annually.

“Health-ISAC is proud to support the Benchmarking Study, which offers unparalleled visibility into the cybersecurity practices and posture shaping the health sector landscape,” said Errol Weiss, Chief Security Officer of Health-ISAC. “By aligning benchmarking to both recognized security frameworks and emerging models like the NIST AI RMF, the study delivers timely, actionable insights our members can use to adapt to accelerating trends—such as AI adoption—and better prepare for the dynamic threat environment. This level of insight is essential for strengthening the ability to detect, respond to, and recover from attacks that could compromise patient care delivery.”

Participation in the Benchmarking Study is open to a broad set of organizational types across the health sector, including: Healthcare Delivery Organizations (HDOs), Payers, Healthcare Technology Vendors, Pharmaceutical and Lab Companies, Public Health Organizations, Medical Device Manufacturers, Mass Fatality Management Services, and Federal Response & Program Offices.

“As our industry faces mounting cybersecurity requirements and increasingly aggressive threat actors, the 2025 Benchmarking Study offers timely guidance for healthcare organizations to navigate the challenges ahead,” said Greg Garcia, Executive Director of the Health Sector Coordinating Council Cybersecurity Working Group. “The Study provides a clear view into how the sector is progressing against shared cybersecurity priorities and helps organizations align more effectively with best practices—all while informing the long-term investments needed to protect our healthcare infrastructure from disruption.”

“The Scottsdale Institute is honored to support the 2025 Benchmarking Study as part of our ongoing commitment to advancing healthcare’s digital future,” said Janet Guptill, President and CEO of the Scottsdale Institute. “Cybersecurity is no longer a technical issue—it’s a business issue, and a fundamental enabler of trust, safety, and equity in care. Through participation in this Study, our members are gaining the insights and peer collaboration needed to address cyber risk head-on and elevate cybersecurity as a core element of organizational performance.”

To learn more, or to participate in the Benchmarking Study at any time, please contact: benchmarks@censinet.com.

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 RiskOpsTM 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.

# # #

Justyn Thompson
Censinet
+1 617-221-6875
email us here
Visit us on social media:
Facebook
X
LinkedIn
