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

Partnered Report

Healthcare Cybersecurity Benchmarking Study 2024

Improving Cybersecurity Preparedness through NIST CSF & HICP Best Practices

February 2024

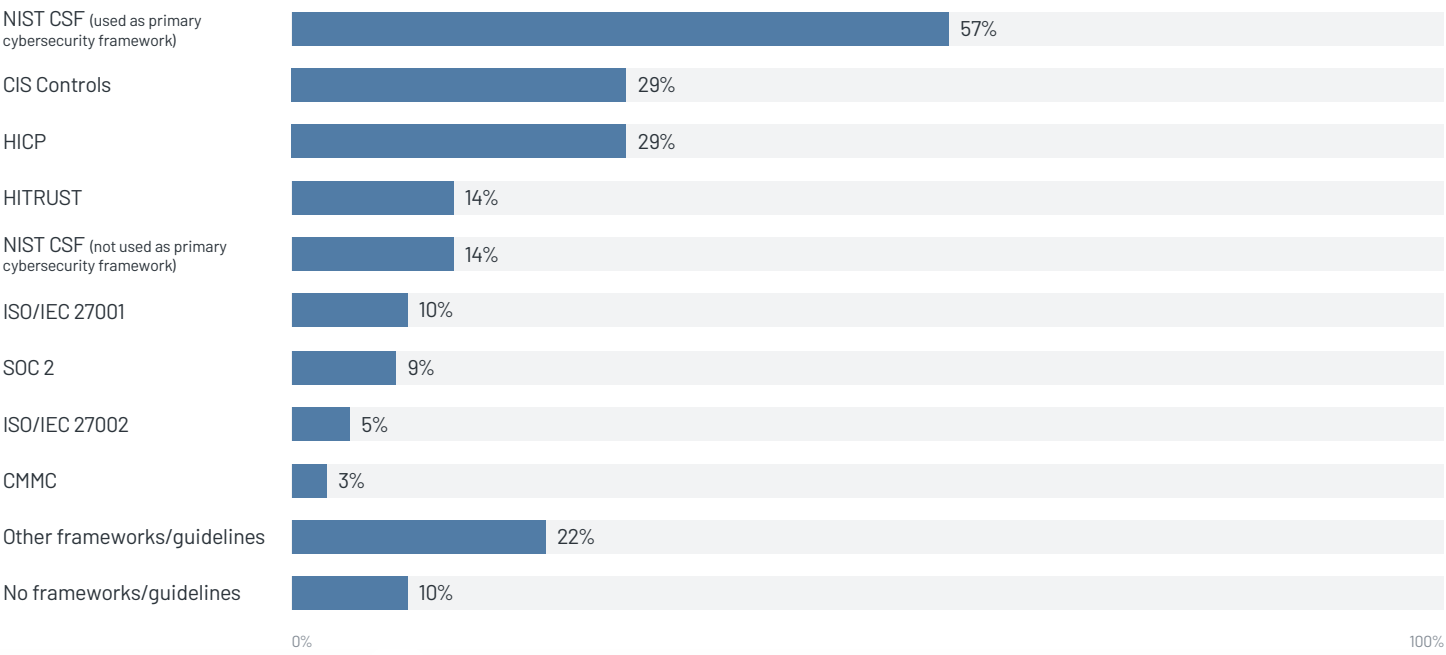
Healthcare Cybersecurity Benchmarking Study 2024

Improving Cybersecurity Preparedness through NIST CSF & HICP Best Practices

With cyberattacks on the rise, having a strong cybersecurity strategy is a must for healthcare organizations, especially as they face post-pandemic resource constraints and staffing shortages. Many are protecting their data by adopting and implementing cybersecurity frameworks and best practices, such as the NIST Cybersecurity Framework (NIST CSF) and the Health Industry Cybersecurity Practices (HICP). NIST CSF and HICP are accessible resources for healthcare organizations, and high NIST CSF and HICP coverage is a strong indication of cybersecurity preparedness. This report—a collaboration between Censinet, KLAS, the American Hospital Association, Health-ISAC, and the Healthcare and Public Health Sector Coordinating Council—provides an update to previous research on the status of healthcare cybersecurity preparedness. It also examines the effect of governance and resource investment on cybersecurity preparedness and insurance premiums. Data for this report comes from 58 respondents (54 payer or provider organizations and 4 healthcare vendors) who were interviewed September–December 2023.

Adoption of Cybersecurity Frameworks & Guidelines

Percentage of respondents who report using framework/guideline; respondents could choose multiple options (n=58)



Note: Other frameworks/guidelines include GLBA, MITRE ATT&CK, and PCI-DSS.

What Are NIST CSF & HICP?

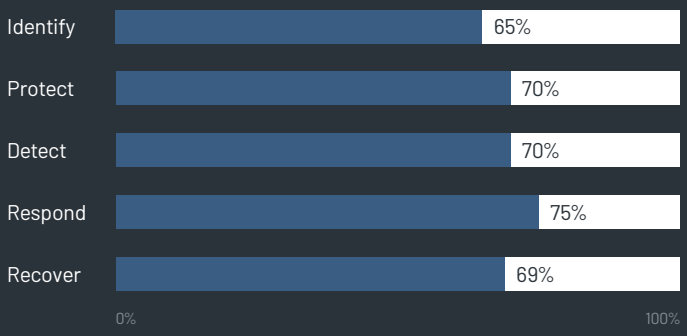
When this report refers to cybersecurity coverage, it is specifically talking about coverage of NIST CSF and HICP. NIST CSF 1.1 is a cross-industry cybersecurity framework consisting of five functions. HICP is a set of ten healthcare-specific cybersecurity mitigating practices based on the top threats to healthcare cybersecurity. Both NIST CSF and HICP are recommended by the HHS 405(d) Program; recently published Healthcare and Public Health Sector Cybersecurity Performance Goals from the Department of Health and Human Services are also based on NIST CSF and HICP. In this report sample, most respondents have adopted NIST CSF and use it as their primary cybersecurity framework.

Healthcare Provider & Payer Cybersecurity Preparedness at a Similar Level Compared to 2023 Benchmarking Study; Repeat Respondents See Increased Coverage across Measurements

Based on NIST CSF and HICP metrics, healthcare cybersecurity coverage is at a similar level as it was in 2023. Average coverage across the five NIST CSF functions shows that organizations are generally more reactive than proactive in their approach to cybersecurity, with the Identify function having the lowest coverage and the Respond function having the highest. This year's HICP coverage is also similar to last year's, confirming that most organizations have Email Protection Systems in place but have a long way to go with Medical Device Security and Data Protection and Loss Prevention.

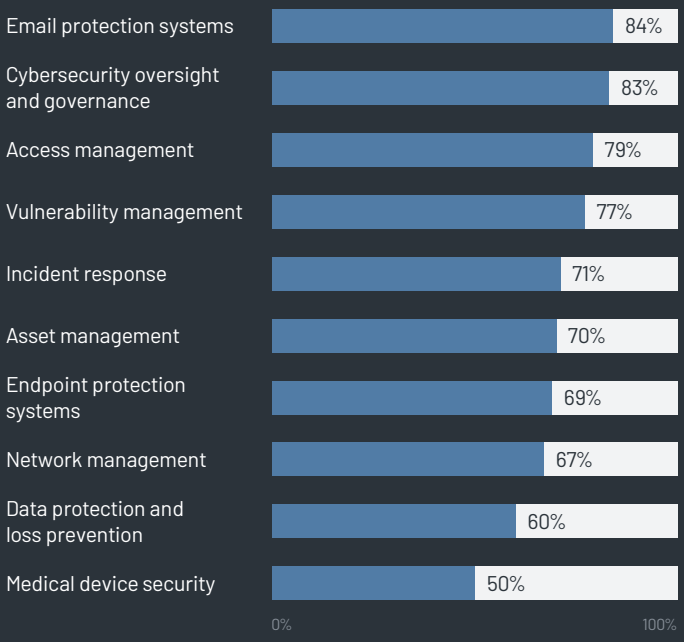
Maturity with NIST CSF Functions

Average coverage across responding organizations; includes provider and payer organizations only (n=54)



Maturity with HICP

Average coverage across responding organizations; includes provider and payer organizations only (n=54)

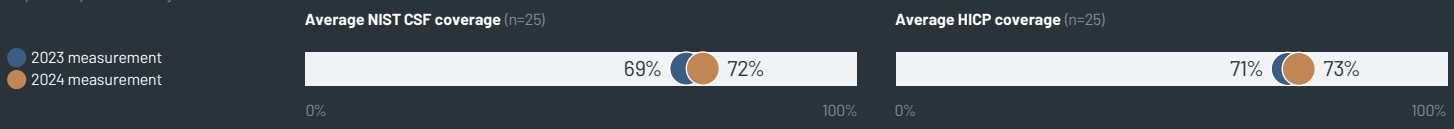


Note: In 2023, HICP updated their best practices; note that Cybersecurity Oversight and Governance was previously called Cybersecurity Policies.

25 of the healthcare delivery organizations in the research sample also participated in last year's benchmarking study. Year over year, these repeat organizations on average have seen improved coverage in all NIST CSF functions as well as HICP best practices, and their average NIST CSF and HICP coverage is higher than that of other participating provider and payer organizations. Repeat organizations saw the largest increase in the following NIST CSF categories: Response Improvement, Recovery Improvement, Business Environment, and Recovery Planning. Improved coverage in HICP areas was slightly lower in magnitude and largely seen in Data Protection and Loss Prevention, Vulnerability Management, and Incident Response.

Maturity with NIST CSF & HICP—Year-over-Year Comparison

Repeat respondents only

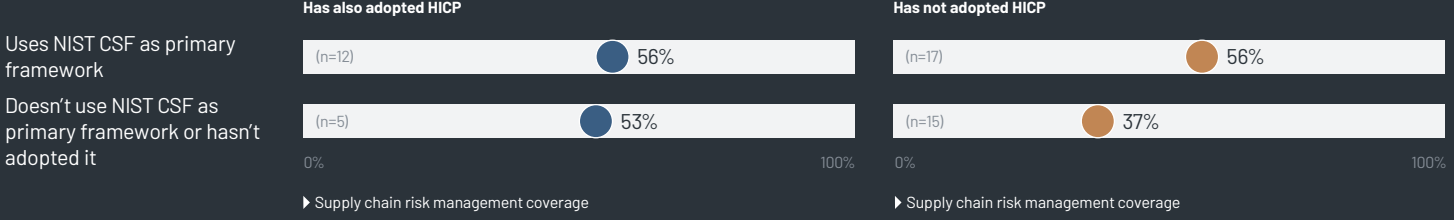


Supply Chain Risk Management Remains NIST CSF Category with Lowest Coverage

Of the many categories within the NIST CSF framework, Supply Chain Risk Management (a component of the Identify function) remains the one with the lowest coverage. The lack of adoption of this category is particularly alarming given that the healthcare industry is more likely than other industries to be victimized by third-party data breaches. Additionally, higher coverage of Supply Chain Risk Management is associated with smaller increases in cybersecurity insurance premiums. The HICP best practices have limited impact on Supply Chain Risk Management coverage when organizations use NIST CSF as their primary framework, but HICP does increase coverage for organizations that don't use NIST CSF as their primary framework.

Supply Chain Risk Management Coverage—by NIST CSF & HICP Adoption

Average coverage across responding organizations

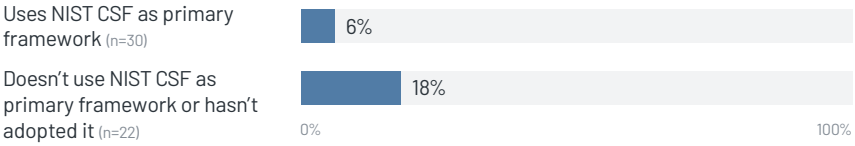


Higher Cybersecurity Preparedness & Resiliency Strongly Correlated with Lower Insurance Premium Growth

On average, respondent organizations who adopt NIST CSF have lower year-over-year increases to their cybersecurity insurance premiums. In particular, those using NIST CSF as their primary cybersecurity framework report premium increases one-third the percentage reported by non-NIST CSF organizations. Higher coverage within the NIST CSF categories related to cyber resiliency is especially correlated with lower increases in cybersecurity premiums. Focusing on these areas helps organizations mitigate the impact of breaches on patient care and safety and maintain business continuity.

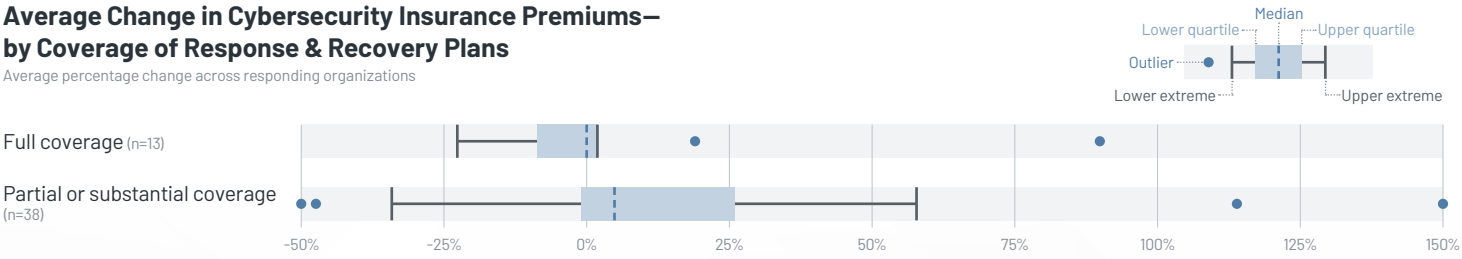
Average Change in Cybersecurity Insurance Premiums—by NIST CSF Adoption

Average percentage change across responding organizations



Average Change in Cybersecurity Insurance Premiums—by Coverage of Response & Recovery Plans

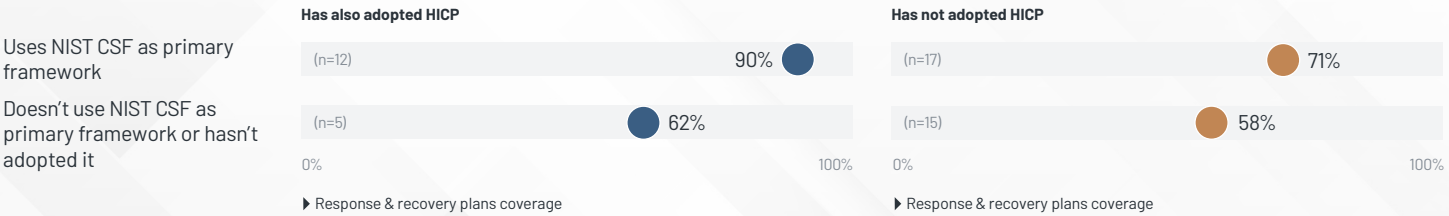
Average percentage change across responding organizations



Note: Coverage of response and recovery plans is measured by organizations' responses to the following subcategory within the Protect function: Are response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) in place and managed?

Coverage of Response & Recovery Plans—by NIST CSF & HICP Adoption

Average coverage across responding organizations



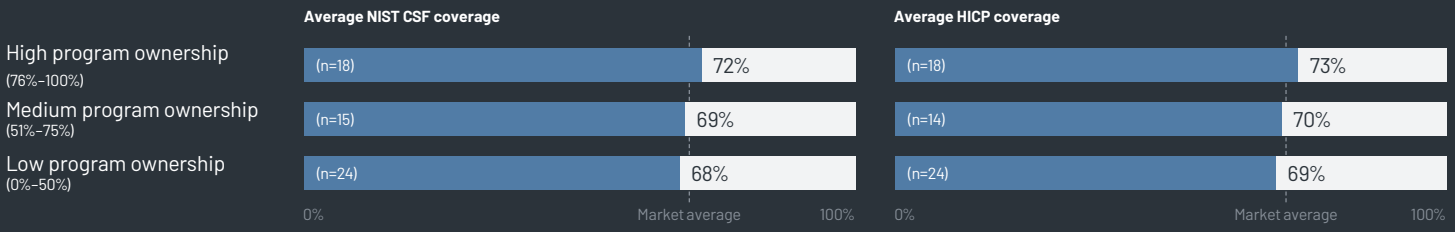
Note: Coverage of response and recovery plans is measured by organizations' responses to the following subcategory within the Protect function: Are response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) in place and managed?

High Program Ownership by Information Security Leaders Continues to Contribute to Higher Coverage

As discussed in last year's benchmarking study, organizations whose information security leaders have greater ownership of cybersecurity-related areas more often achieve higher cybersecurity coverage. KLAS used a linear regression analysis to determine the impact of several variables on cybersecurity coverage. The level of cybersecurity program ownership by information security leaders continues to be significantly correlated with high coverage. While the industry average for NIST CSF and HICP coverage is 70%–71%, organizations that assign information security leaders higher percentages of program ownership achieve above-average cybersecurity coverage. In particular, higher program ownership is correlated with significantly higher coverage in the HICP areas of Endpoint Protection Systems and Data Protection and Loss Prevention. Among organizations that participated in both the 2023 and 2024 studies, those that increased cybersecurity program ownership under their CISO almost always saw increased coverage. The NIST CSF categories that these organizations invested in include Access Management, Network Management, and Disaster Recovery Programs.

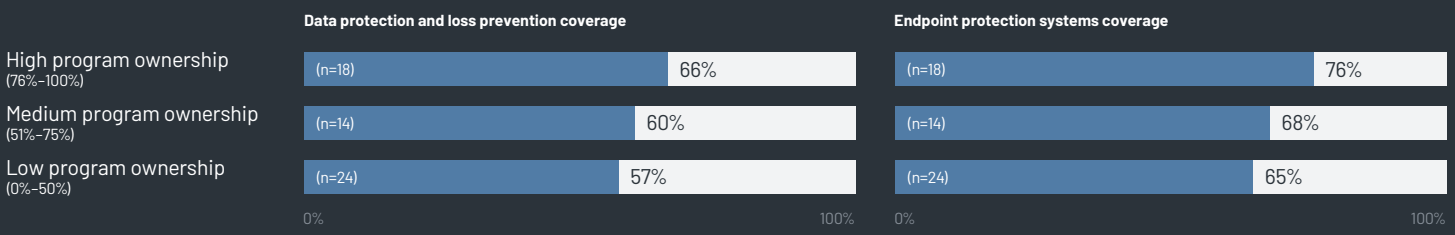
Maturity with NIST CSF & HICP—by Information Security Leaders' Ownership of Cybersecurity Programs

Average coverage across responding organizations



Maturity in Select HICP Areas—by Information Security Leaders' Ownership of Cybersecurity Programs

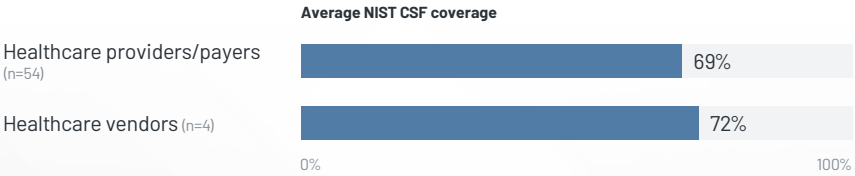
Average coverage across responding organizations



Vendors Take a More Preventive Approach to Cybersecurity Preparedness

Maturity with NIST CSF—Vendors vs. Healthcare Providers/Payers

Average coverage across responding organizations



Vendors play an integral role in healthcare cybersecurity; if critical third-party systems and devices used for care delivery are compromised, they can negatively impact care quality and patient safety. Four vendors are included in this report sample, all of whom have adopted NIST CSF 1.1. This limited sample shows that on average, vendors have similar NIST CSF coverage to other respondents; however, the level of coverage within the five NIST CSF functions varies between vendors and payer/provider organizations. Payers and providers typically show more coverage for the Respond function than vendors, while vendors show comparatively higher coverage across the Identify and Protect functions.

Report Information

About This Report

The 2024 Healthcare Cybersecurity Benchmarking Study is co-sponsored by Censinet, KLAS Research, the American Hospital Association, the Health Information Sharing and Analysis Center, and the Healthcare and Public Health Sector Coordinating Council. 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. Research for the 2024 study included 58 participating organizations—including healthcare delivery organizations and healthcare vendors—and analyzes coverage across the NIST Cybersecurity Framework and the Health Industry Cybersecurity Practices as well as key organizational and cybersecurity program performance metrics.

Study Sponsors

CENSINET

KLAS RESEARCH

American Hospital Association™
Advancing Health in America

Health-ISAC™
Collaborating for Resilience in Healthcare

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

About

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
Ruirui Sun
ruirui.sun@KLASresearch.com

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

CO-AUTHOR
Dan Czech
dan.czech@KLASresearch.com

WRITER
Natalie Hopkins

DESIGNER
Jess Wallace-Simpson

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:
www.KLASresearch.com

About

Censinet®, based in Boston, MA, enables healthcare organizations to take the risk out of their business with Censinet RiskOps™, the first and only cloud-based risk exchange that integrates and consolidates enterprise risk management and operations capabilities across critical clinical and business areas. RiskOps builds upon the company's foundational success with third-party risk management (TPRM) for healthcare. Censinet transforms healthcare risk by increasing productivity and operational effectiveness while eliminating risks to care delivery, data privacy, and patient safety. 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

VP OF MARKETING
Briana McGann
bmcgann@censinet.com