KLAS RESEARCH | CENSINET | American Hospital Association™ Advancing Health in America

White Paper

Healthcare Cybersecurity Benchmarking Study

How Aligned Is the Industry to NIST and HICP Best Practices?

April 2023

Healthcare Cybersecurity Benchmarking Study

How Aligned Is the Industry to NIST and HICP Best Practices?

The digitalization of healthcare has come with many benefits but also some challenges, cybersecurity being among the most significant. As healthcare organizations introduce new technology into their environments, questions often arise as to how and where to allocate resources in order to best reduce cyber risk. This report—a collaboration between Censinet, KLAS, and the American Hospital Association (AHA)—is intended to provide high-level insights into the current state of cybersecurity preparedness in healthcare and thus highlight potential areas of focus.

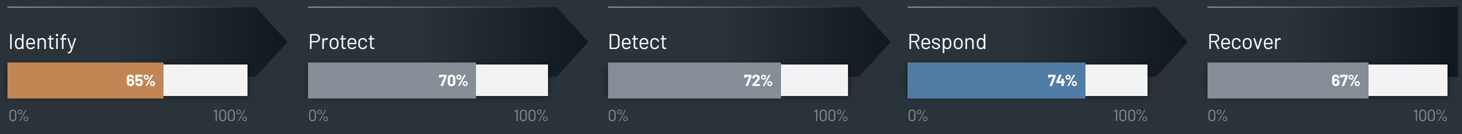
The findings in this report are based on evaluations completed by 48 healthcare organizations, ranging from small critical access hospitals to large multispecialty practices and large academic medical centers. The questions were designed to measure adherence to the guidelines recommended by the NIST Cybersecurity Framework (NIST CSF) and Health Industry Cybersecurity Practices (HICP), with additional questions added to gain insight into organizations' cybersecurity investments and resources and the span of control given to information security leadership.

Maturity with NIST Five Functions

Organizations Are More Reactive than Proactive, Especially in Identifying Asset and Supply Chain Risk

Maturity with NIST Cybersecurity Framework's Five Functions

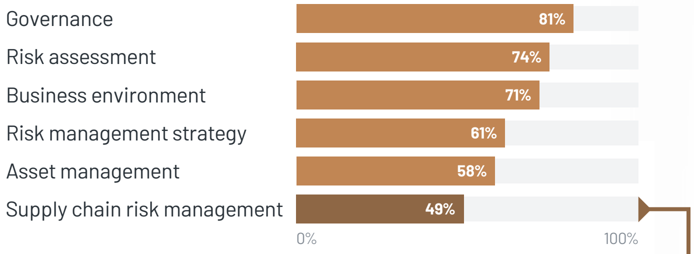
Average coverage across responding organizations (n=48)



Survey results indicate that healthcare organizations are still mostly reactive rather than proactive when it comes to cybersecurity, especially when it comes to identifying cybersecurity risks. Of the six categories within the **Identify** function, organizations have particularly low coverage in Supply Chain Risk Management, Asset Management, and Risk Management. More than 40% of organizations are not compliant with conducting response and recovery planning with suppliers and third-party providers.

Maturity within the Identify Function

Average coverage across responding organizations (n=48)

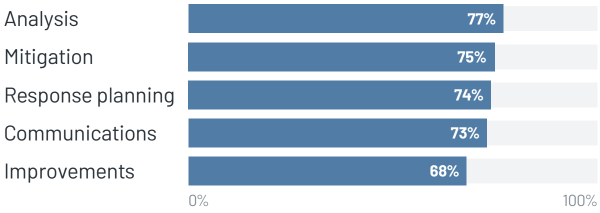


Note: Categories are arranged high to low by coverage and do not reflect NIST's original framework ordering.

Of the five functions in the NIST cybersecurity framework, organizations report the highest average coverage in the **Respond** function. This is driven largely by maturity in the Analysis category, which measures an organization's investigation, forensics, categorization, analysis, and understanding of cybersecurity incidents. All organizations report investigating notifications from detection systems, with the vast majority reporting coverage in this area of at least 70%.

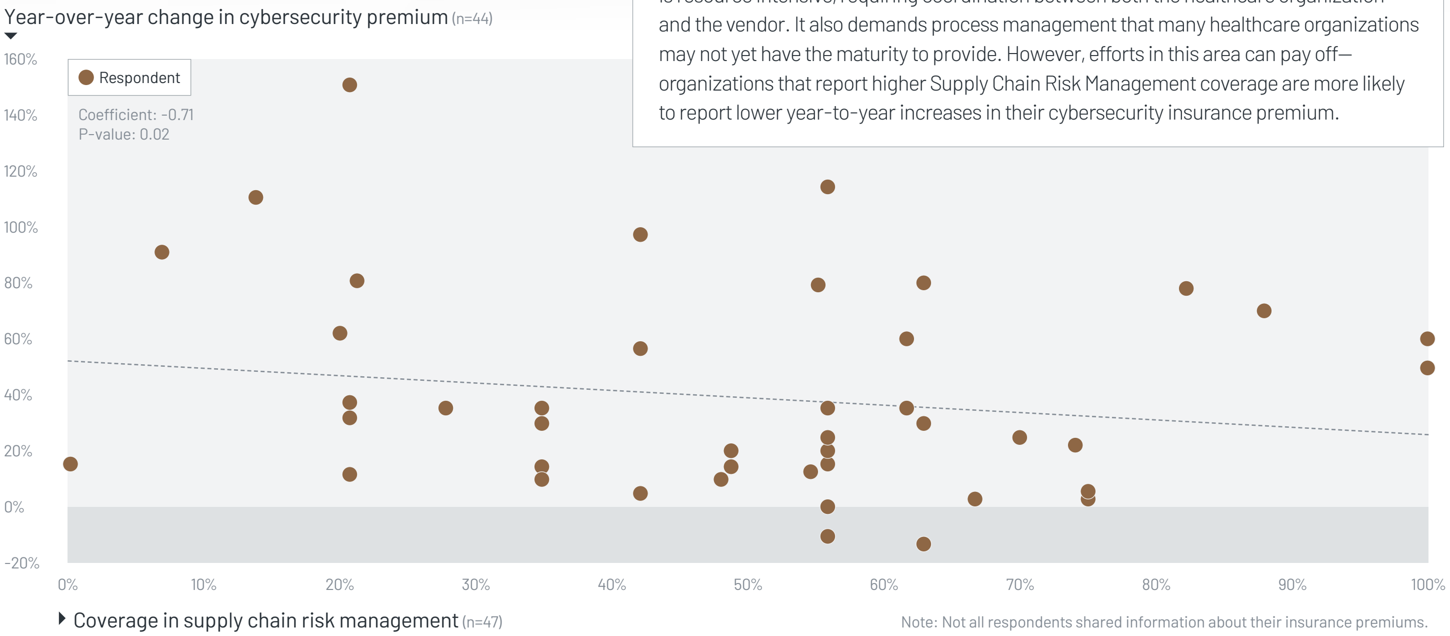
Maturity within the Respond Function

Average coverage across responding organizations (n=48)



Note: Categories are arranged high to low by coverage and do not reflect NIST's original framework ordering.

Coverage in Supply Chain Risk Management vs. Change in Cybersecurity Insurance Premium



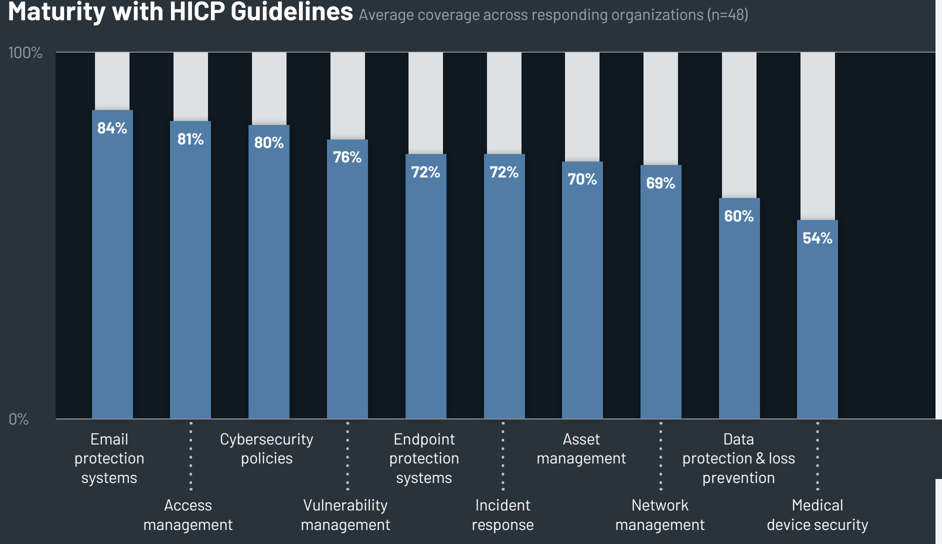
Note: Not all respondents shared information about their insurance premiums.

Supply Chain Risk Management has the lowest coverage of any subcategory across all five NIST functions. A particular challenge is that conducting testing with third-party suppliers is resource intensive, requiring coordination between both the healthcare organization and the vendor. It also demands process management that many healthcare organizations may not yet have the maturity to provide. However, efforts in this area can pay off—organizations that report higher Supply Chain Risk Management coverage are more likely to report lower year-to-year increases in their cybersecurity insurance premium.

Alignment with HICP Guidance

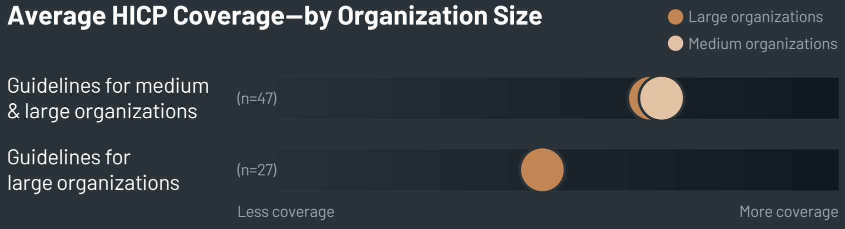
Email System Protections Are in Place; Medical Device Security Has a Long Way to Go

Maturity with HICP Guidelines



Note: HICP practices are arranged high to low by coverage and do not reflect HICP's original ordering.

Average HICP Coverage—by Organization Size

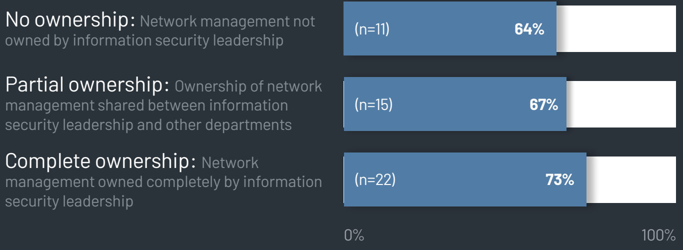


HICP guidance differs based on organization size, and respondents self-selected into one of three groups based on size, complexity, IT capabilities, cybersecurity investment, and other criteria as laid out by HICP. Of the participating organizations, 27 self-selected as large, 20 as medium, and 1 as small.

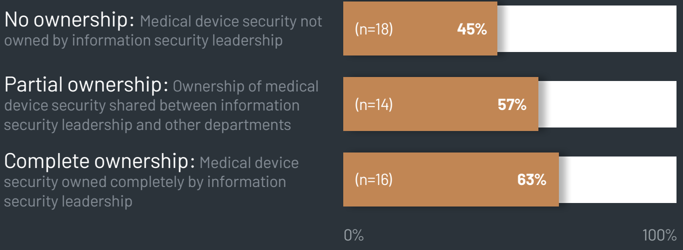
Regardless of size, organizations report the highest coverage for email protection. For most of the metrics that fall under email protection, more than half of organizations report 100% coverage. On the other hand, medical device security is an area of industry-wide vulnerability, with average coverage barely over 50%. Almost all responding organizations ensure medical devices are wiped of all data when decommissioned. However, when such configuration is supported by the manufacturer, less than two-thirds configure medical devices to allow only known processes and executables to run on medical devices, and most of these organizations report doing this for only some devices.

The HICP guidelines for large organizations include all subpractices recommended for medium organizations as well as additional, more advanced subpractices targeted specifically to large organizations. Large organizations are nearly equal with medium organizations in their adoption of the shared recommendations, while their adoption of the large-organization recommendations is much lower, especially in the areas of data protection and loss prevention, endpoint protection systems, and asset management.

Network Management Coverage— by Ownership of Network Management Program



Medical Device Security Coverage— by Ownership of Medical Device Security Program



Two of HICP's cybersecurity practice areas—network management and medical device security—show significant correlation between an organization's coverage in that area and how much of that area is owned by information security leadership. Organizations with full information security ownership of their **network management** program report 64% coverage in this assessment area, an improvement of 9 percentage points over organizations with no information security ownership. Similarly, organizations with full information security ownership of **medical device security report** 63% coverage in this assessment area, which is 18 percentage points more than organizations with no ownership. Organizations wishing to improve coverage in these areas should consider establishing structure and governance that give clear responsibility and ownership to those most suited to manage the risk.

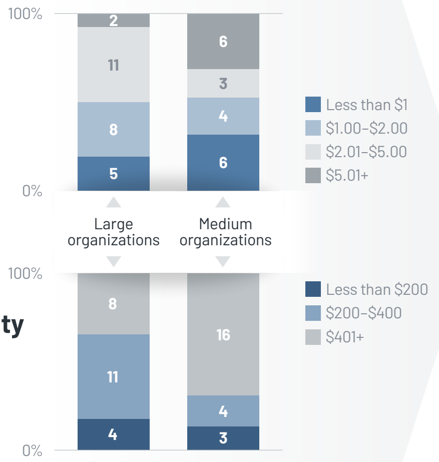
Snapshot of Cybersecurity Expense

Average Cost to Protect One Patient Record

Large and medium organizations only; not all organizations responded (n=45)

Average Cybersecurity Expenditure Per Workforce Member

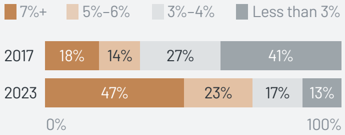
Large and medium organizations only; not all organizations responded (n=46)

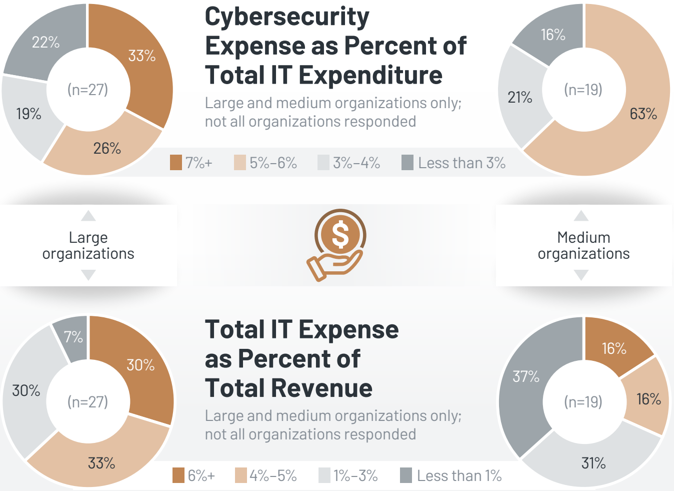


Over the last six years, cybersecurity has become a larger percentage of healthcare organizations' IT spending.

Note: 2017 data comes from previous research conducted by KLAS and CHIME.

Cybersecurity Expense as Percent of Total IT Expenditure— 2017 vs. 2023 (n=164)





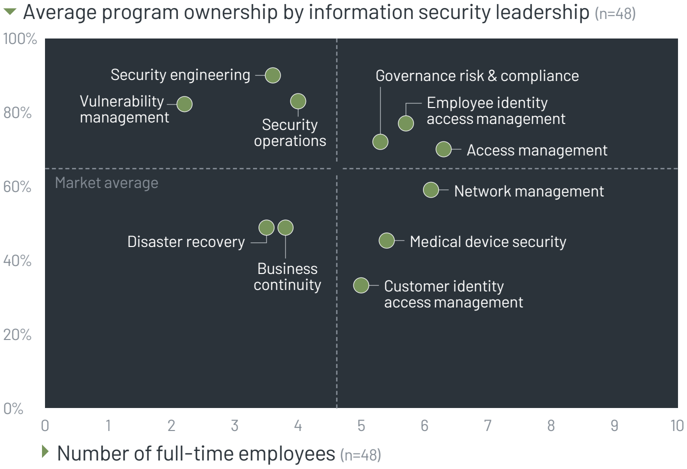
Cybersecurity Expense as Percent of Total IT Expenditure

Large and medium organizations only; not all organizations responded

Total IT Expense as Percent of Total Revenue

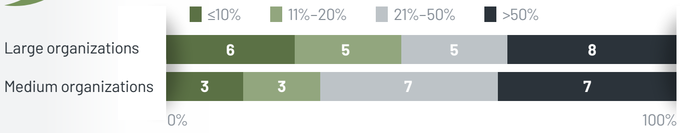
Large and medium organizations only; not all organizations responded

Percentage of Program Owned by Information Security Leadership vs. Program FTE Volume



Year-to-Year Increase in Cybersecurity Insurance Premium

Large and medium organizations only; not all organizations responded (n=44)



Key Findings

Healthcare organizations do well at responding to cybersecurity incidents, particularly when it comes to incident analysis. But the data shows a lack of proactivity in managing third-party products and services.

Organizations that report lower coverage of Supply Chain Risk Management are more likely to report higher year-to-year increases in their cybersecurity insurance premium, indicating that efforts to better assess and identify risk with supply chain providers can pay off.

Most organizations have email protection systems in place that cover a majority of their entities.

Medical device security is a significant vulnerability, but ownership of this area by information security leadership has a significantly positive impact. This correlation suggests that coverage in this area can be improved by aligning ownership under the most appropriate leadership.

Ownership by information security leadership also shows a positive correlation with network management coverage. Organizations wishing to improve coverage in this area should consider giving ownership to those most suited to manage the risk.

Large organizations may lack the resources to meet the HICP guidelines targeted specifically to large organizations. Their coverage in most of these areas is significantly lower than their coverage of the guidelines that they share with medium organizations.

Report Information

About This Report

Conducted by Censinet, KLAS Research, and the American Hospital Association (AHA), this study is intended to establish collaborative cybersecurity benchmarks for the healthcare industry. The findings are based on evaluations completed by 48 healthcare organizations, ranging from small critical access hospitals to large multispecialty practices and large academic medical centers. The study questions were designed to measure adherence to the guidelines recommended by the NIST Cybersecurity Framework (NIST CSF) and Health Industry Cybersecurity Practices (HICP), with additional questions added to gain insight into organizations' cybersecurity investments and resources and the span of control given to information security leadership.

Study participants were given access to additional, more in-depth analysis of the findings. To participate in future benchmarking studies, please contact Censinet at benchmarking@censinet.com.

Study Sponsors

The healthcare cybersecurity benchmarking study is provided in partnership with the following sponsors:

BAPTIST HEALTH

Cedars Sinai

dayton children's

Fairview HEALTH SERVICES

Hartford HealthCare

Intermountain Health

Marshfield Clinic Health System

Mass General Brigham

Special Thank-You

The study authors extend a special thank-you to the following individuals/groups for their guidance and expertise:

John Riggi
National Advisor for Cybersecurity and Risk
AHA

Erik Decker
Vice President & CISO
Intermountain Healthcare

HHS 405(d) Program and Task Group

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.

LEAD AUTHOR
Dan Czech
dan.czech@KLASresearch.com

CO-AUTHOR
Ruirui Sun
ruirui.sun@KLASresearch.com

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

WRITER
Elizabeth Pew

DESIGNER
Natalie Jamison

PROJECT MANAGER
Andrew Wright

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

Cover image: © Anela Ramba/peopleimages.com / Adobe Stock

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 CUSTOMER SUCCESS
Brianna Connolly
bconnolly@censinet.com