HHS 405(d)
Aligning Health Care
Industry Security Approaches

# The 405(d) Post

## Volume XXI

A Word from the Task Group

# 5 Key Insights from The Healthcare Cybersecurity Benchmarking Study

By Ed Gaudet, 405(d) Task Group member

The Healthcare Cybersecurity Benchmarking Study, co-led by Censinet, KLAS Research, and the American Hospital Association, and sponsored by leading health systems, is the industry's first initiative to establish robust, trusted, and actionable peer benchmarks to help healthcare organizations strengthen cybersecurity maturity and resiliency. The Study produced detailed findings and peer benchmarks across three key areas:

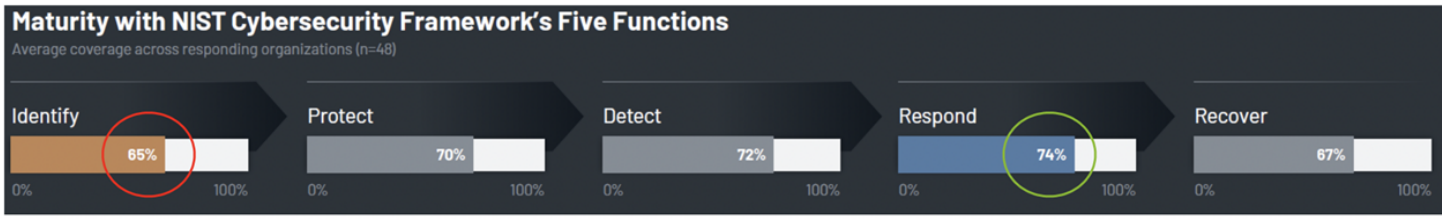
- **Organizational Key Performance Indicators (KPIs)**
- **The NIST Cybersecurity Framework (CSF)**
- **The 405(d) Health Industry Cybersecurity Practices (HICP)**

Findings from this landmark Study also served as one of the primary sources of data included in the recently published HHS Hospital Cyber Resiliency Initiative: Landscape Analysis.

## Here are 5 key insights from the first wave of the Study (which included 48 healthcare delivery organizations):

### 1. Healthcare is Still More Reactive than Proactive in Cybersecurity

Much like the relative infrastructure in place to manage acute care episodes versus preventing chronic disease at health systems, the Study found that the healthcare industry currently is better positioned to respond to security incidents versus identifying (and mitigating) cyber threats before they become incidents. The Study found "Identify" ranked lowest in maturity across all 5 NIST CSF Functions while "Respond" ranked highest.



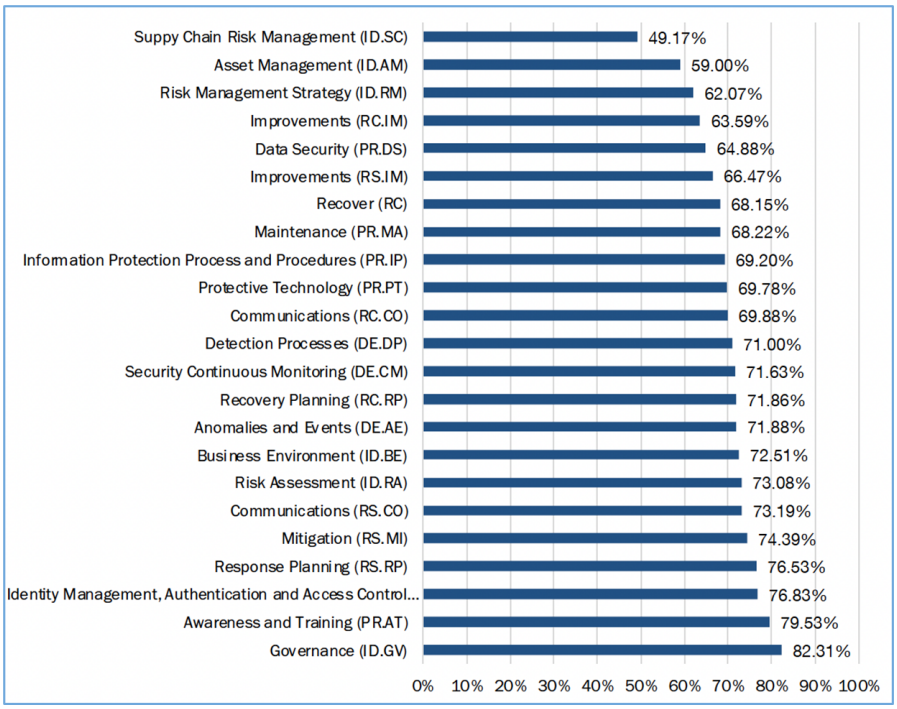

## NIST CSF Function Coverage

### 2. "Supply Chain Risk Management" Ranks Last in NIST CSF Maturity

Digging deeper into the key drivers of Insight #1 above, the Study found "Supply Chain Risk Management" ranks last in relative HDO maturity across all 23 NIST CSF Categories. Despite best intentions, managing third-party risk still faces significant headwinds as it remains a highly-manual and time-consuming process. Moreover, just as the attack surfaces and the threat landscape keep growing, CISOs find themselves facing one of the most acute cybersecurity workforce shortages in modern history.

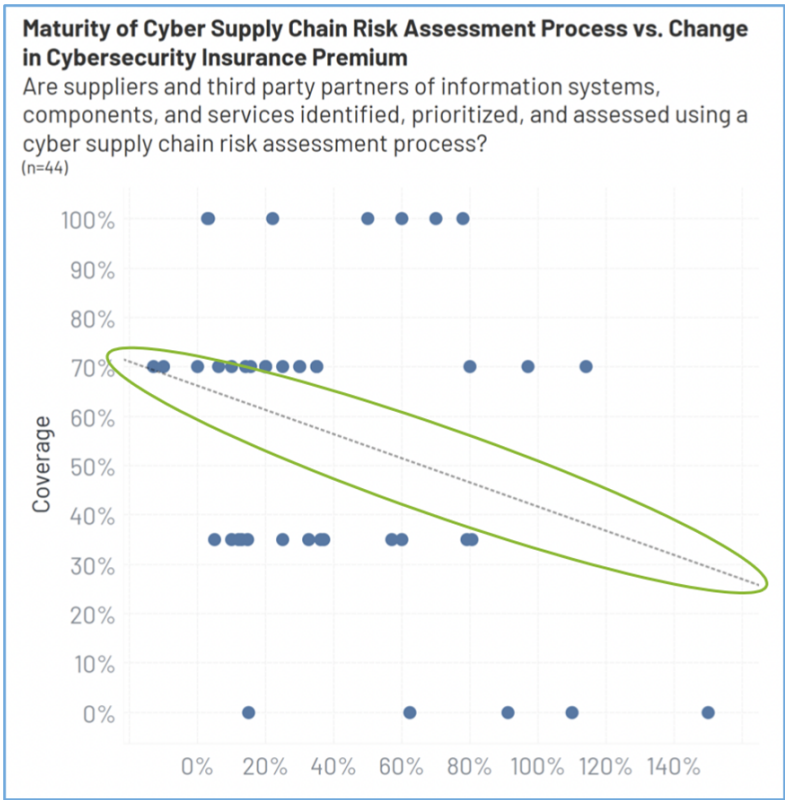
Adding fuel to the fire, it should be noted that the largest healthcare breach in 2022 did not occur at a top Health IT company – it was a hacking incident at a printing & mailing vendor, affecting 2.7 million individuals across 37 different HDOs.

## NIST CSF Category Coverage



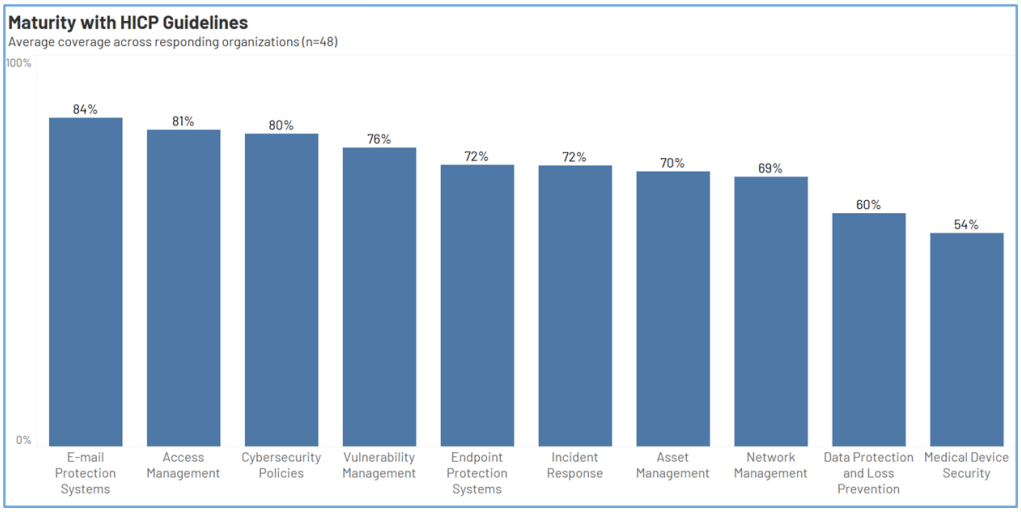

## 3. Higher Third-Party Risk Coverage Correlated with Lower Cyber Insurance Premium Growth

The Study found statistically-significant correlation between higher third-party risk assessment maturity and lower annual increases in cyber insurance premiums. The Study also found significant challenges acquiring and keeping cyber insurance coverage as well as extraordinary annual growth in premium costs: large-sized organizations saw an average increase of 46% in premium cost last year, while medium-sized organizations saw 50% growth, on average. Anecdotal interviews with hospitals and health systems found increasing policy exclusions, shrinking policy coverage amounts, and even instances of cyber insurers refusing to pay out on claims after a security incident.



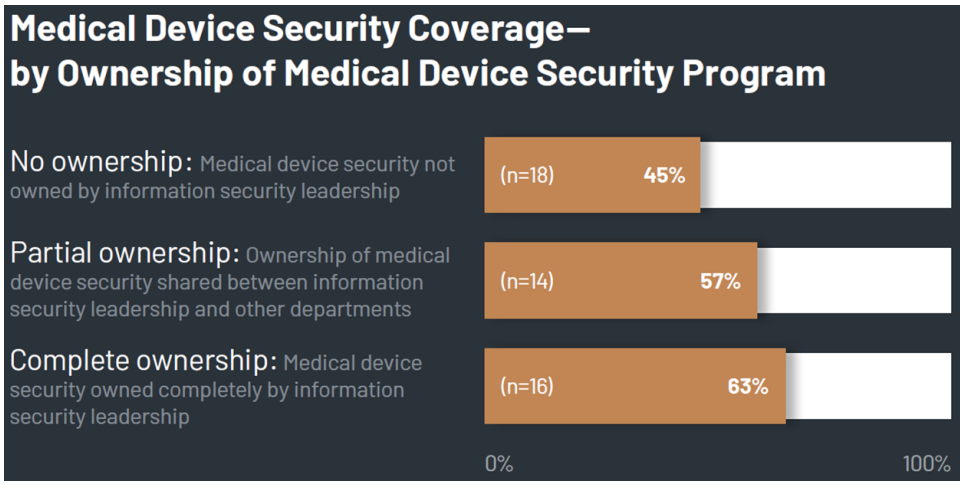
## 4. While Email Protections Are Largely In Place, There's Still A Long Way to Go on Medical Device Security

The Study found wide disparity in the Health Industry Cybersecurity Practices Publication (HICP) adoption across the ten best practice areas, with email protections ranking highest in adoption and medical device security ranking last in coverage across HDOs with just over 50% coverage. With 10 -15 network connected medical devices per bed, and the market for Internet-of-Medical-Things (IoMT) growing rapidly, this will certainly be a key focus area for both BioMed leaders and CISOs – especially with ransomware groups now directly threatening patient care and safety.




## 5. Higher CISO Program Ownership Correlates with Higher HICP Coverage for Medical Device Security

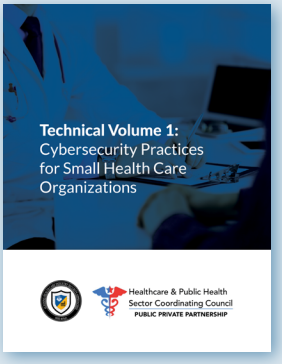
Looking into implications for programmatic changes and their effect on security, the Study also found an interesting, statistically-significant correlation between CISO program ownership and HICP adoption for medical device security. Specifically, when the CISO's office owned responsibility for medical device security, HDOs saw an 18 percentage point increase in HICP coverage – from 45% with no ownership to 63% with complete ownership.




## Conclusion:

As ransomware increasingly shuts down care operations at hospitals across the country, healthcare organizations are now forced to manage cyber risk as patient safety risk. These organizations are seeking out solutions to help them understand the risks they face and fight back against these emerging threats. Peer benchmarking is an invaluable tool for identifying, assessing, and, ultimately, mitigating cyber risk across the enterprise. By comparing cybersecurity program performance and maturity to peer organizations, IT/Security teams can identify where critical gaps in security exist today, prioritize allocation of scarce resources, and help justify future investment in cybersecurity to their Boards to make the overall enterprise more resilient -- and safer for patients.

# HICP in the Spotlight




## Cybersecurity Insurance- Technical Volume 1 (Small Organizations)

*Cyber insurance is one option that can help protect your business against losses resulting from a cyberattack. If you are thinking about cyber insurance, discuss which policy would best fit your company's needs with your insurance agent. This should include whether you should go with first-party coverage, third-party coverage, or both. Be advised that many policies require you have a minimum level of security controls in place. You should not secure a cyber insurance policy in lieu of implementing the cybersecurity practices outlined in this document.*

## What Should Your Cyber Insurance Policy Cover?

Be sure your policy includes coverage for:

- ***Data breaches (like incidents involving theft of personal information)***
- ***Cyber-attacks on your data held by vendors and other third parties.***
- ***Cyber-attacks (breaches of your network)***
- ***Cyber-attacks that occur anywhere in the world (not just in the United States)***
- ***Cyber-attacks determined to be nation-state attackers***
- ***Cyber-attacks aided by insiders both intentional and unintentional***
- ***Cyber-attacks that lead to extortion (ransomware attacks)***
- ***Terrorist acts***
- ***Cyber warfare***

Also, consider whether your cyber insurance provider will:

- ***Defend you in a lawsuit or regulatory investigation (called a "duty to defend")***
- ***Provide coverage in excess of any other applicable insurance you have***
- ***Offer a breach hotline that's available every day of the year at-all-times***
- ***Provide access to third-party breach specialists, including forensics, independent legal counsel working on your behalf, not the cyber insurance provider, and incident remediation firms***
- ***Require you to use specific vendors for IR***
- ***Provide coverage for notification costs including printing, mailing, phone centers, and PR assistance***
- ***Loss of business coverage or revenue***

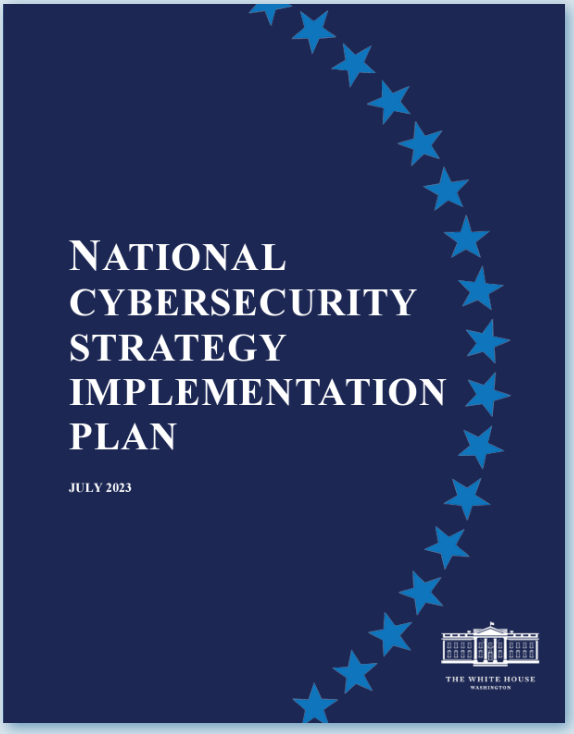
*Review your application closely and answer any questions about your business to the best of your ability. Seek the advice of your insurance broker or legal counsel for assistance with questions about the scope or meaning of the questions and how they relate to your cybersecurity practices.*

# A note from the 405(d) Program

The White House released a new National Cybersecurity Strategy Implementation Plan

The HHS 405(d) Program is encouraged by the new White House National Cybersecurity Strategy Implementation Plan released on July 13, 2023. The White House is taking the novel step of publishing the National Cybersecurity Strategy Implementation Plan (NCSIP) to ensure transparency and a continued path for coordination. This plan details more than 65 high-impact Federal initiatives, from protecting American jobs by combatting cybercrimes to building a skilled cyber workforce equipped to excel in our increasingly digital economy. The NCSIP, along with the Bipartisan Infrastructure Law, CHIPS and Science Act, Inflation Reduction Act, and other major Administration initiatives, will protect our investments in rebuilding America's infrastructure, developing our clean energy sector, and re-shoring America's technology and manufacturing base.

We encourage all of our healthcare stakeholders to read the full implementation plan here!




# Other HHS Resources

## CISA

CISA provides organizations with a remote access software overview, including the malicious use of remote access software, detection methods, and recommendations for all organizations.

## HC3

Artificial Intelligence, Cybersecurity and the Health Sector

## OCR

HHS Office for Civil Rights and the Federal Trade Commission Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies.

HHS Office for Civil Rights Settles HIPAA Investigation with iHealth Solutions Regarding Disclosure of Protected Health Information on an Unsecured Server for $75,000

### About The 405(d) Post

*This newsletter is for information purposes only and aims to broaden awareness and align healthcare security approaches. The "A Word from the Task Group" and the "405(d) Chronicles" is written by a different 405(d) Task Group Member each issue and does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute to this newsletter. The news articles are not an endorsement of any product/viewpoint/entity. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations.*

**Need To Contact Us?** Email us at cisa405d@hhs.gov

## Follow us!

Facebook
X
Instagram
LinkedIn

Visit our website at 405d.hhs.gov!