405(d) Spotlight Webinar! Healthcare Benchmarking Study

Ed Gaudet- 405(d) Task Group Member, CEO& Founder Censinet

Ruirui Sun- Manager of KLAS Research

Message from the 405(d) Team

The 405(d) Aligning Health Care Industry Security Practices initiative, along with the *Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients* publication and this engagement, are in partnership with the Healthcare & Public Health Sector Coordinating Council (HSCC).

"This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches. The topics chosen are developed by a different 405(d) Task Group Member each iteration and do not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute to this webinar series. This webinar is 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."

- This Webinar is being recorded and will be available for future viewing
- A note for media: While this event is open to the public, we would like to direct any media representatives to contact the public affairs office of whichever representative you have questions for to receive an official statement on behalf of the organization and refrain from quoting panelists during this event directly.

405(d) Events and Announcements

August
- 405(d) Post
- Poster release

September
- 405(d) Spotlight Webinar

For more information or to see all our products, visit our website at https://405d.hhs.gov

Email: CISA405d@hhs.gov

Social Media: @Ask405d LinkedIn, Twitter, Facebook, Instagram

Agenda

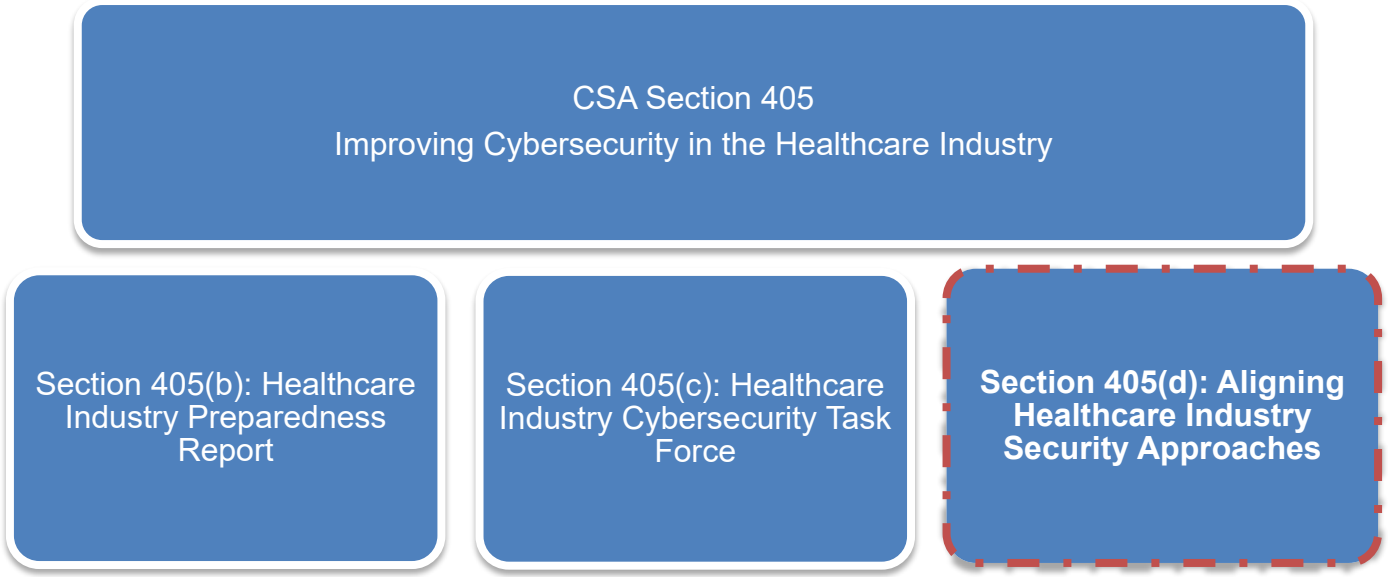
Time	Topic	Speaker
10 minutes	Opening Remarks and Introductions	Julie Chua- HHS GRC Director and 405(d) Federal Co-Lead
60 Minutes	Hospital Cybersecurity Benchmarking Study	Ed Gaudet- 405(d) Task Group Member CEO & Founder Censinet Ruirui Sun – Manager KLAS research
25 Minutes	Questions	All
5 Minutes	Closing	405(d) Team

Cybersecurity Act of 2015: Legislative Basis

Under the auspices of the Cybersecurity Act of 2015 (CSA), Section 405(d), the U.S. Department of Health and Human Services (HHS) convened the CSA 405(d) public-private task group to enhance cybersecurity and align industry security practices.

The purpose of the 405(d) Spotlight Webinar is to continue the 405(d) mission and vision of "Aligning Health Industry Security Approaches" by discussing a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations.

This webinar series aims to align industry security practices by providing an information sharing platform for our public-private partnership. For more information on the 405(d) Program please email us at CISA405d@hhs.gov !



405(d) Outreach & Program Resources

Below you can find examples of products from 405(d) and the corresponding category the items fall under.

HHS/405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! Since 2018 the program has released more than 60 awareness products which organizations across the HPH sector can leverage.

405(d) Outreach

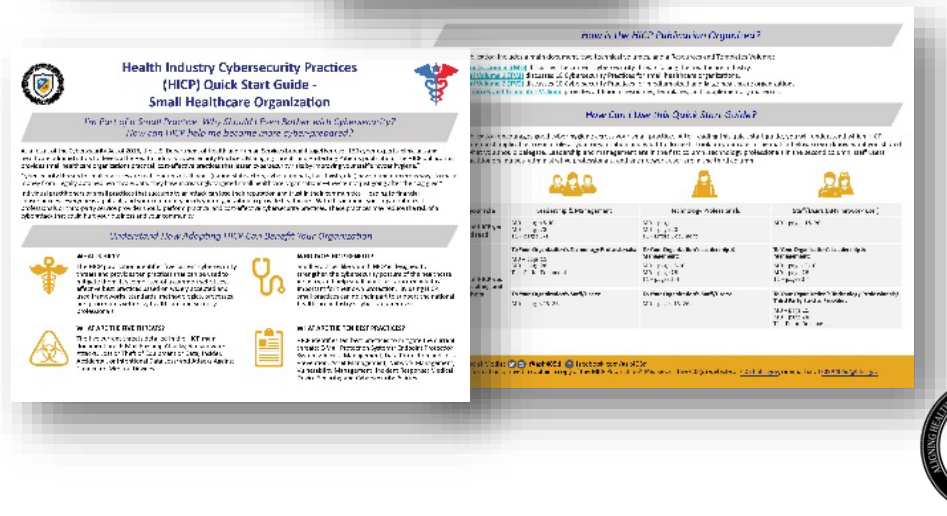
The 405(d) Program produces Bi-monthly Newsletters, SBARs, and Spotlight Webinars to increase cybersecurity awareness and present new and emerging cybersecurity news and topics, as well highlight the HICP Publication!

Knowledge on Demand

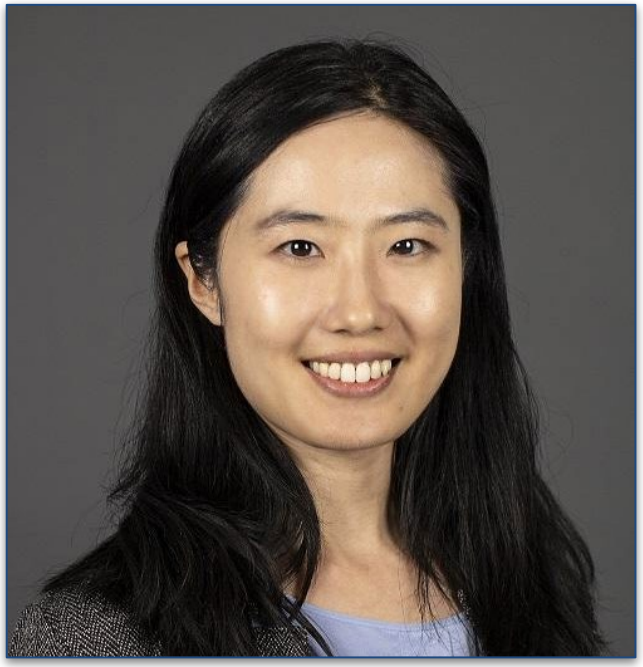
The 405(d) Program, recently launched a new cybersecurity training platform on its website—405d.hhs.gov.This new cybersecurity education platform will include multiple delivery methodologies to reach the varied size health care facilities across the country. The platform will include five cybersecurity awareness trainings that align with the landmark 405(d) publication: HICP and its accompanying two volumes.

Official Task Group Products

These resources are official products produced by the 405(d) Task Group. Examples include the HICP Publication, Quick Start Guides, New Cyber ERM Publication, and 5 threat flyers.



Presenters



RUIRUI SUN, PhD

Insights Manager

KLAS Research

ED GAUDET

CEO and Founder

Censinet

Agenda

1. Study Overview & Timeline
2. Value of Peer Benchmarking
3. Findings from the Study

Study Overview & Timeline

THE HEALTHCARE CYBERSECURITY BENCHMARKING STUDY

Advanced Cyber Threats Require Community Collaboration

$10.1M

Average Cost of a Breach in Healthcare*

79%

Increase in Cyber Insurance Premiums in Q2 2022

CommonSpirit Takes a **$150M** Hit (So Far) From Ransomware Attack in Q4 2022…

Ransomware Attack on UVM Health Network Estimated to Cost **$63M** in Lost Business…

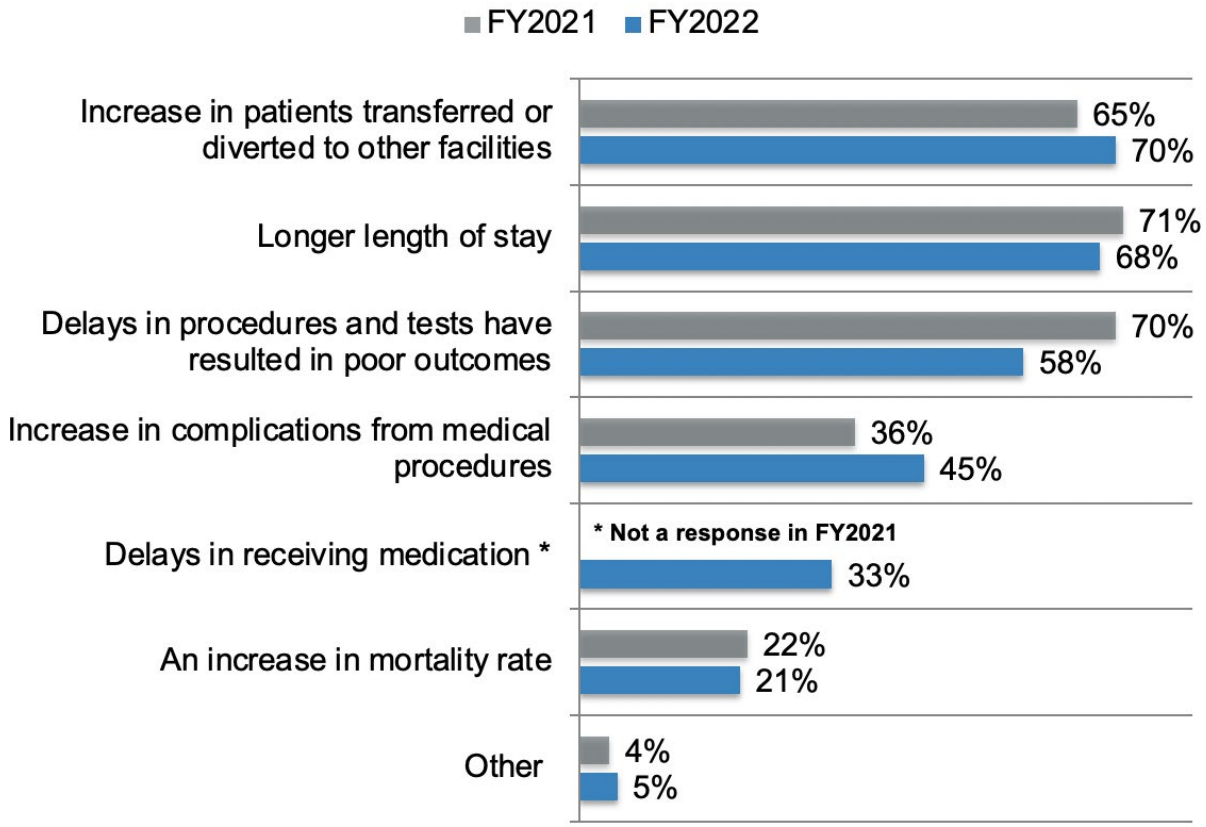
Baton Rouge General **Switches to Paper-Based** Operations After Cyberattack on EHR…

**Does not include HHS penalties of $1.2M on average per case*

Ponemon INSTITUTE

What impact did the ransomware attack at your organization have on patient care?

N = 579 IT/Security Professionals at Healthcare Delivery Organizations (multiple responses permitted)



Why Benchmarking?

Protect Patient Safety

Increasing ransomware attacks elevating cyber risk to top enterprise risk priority.

Prioritize Investments

Where and how do I invest and allocate scarce resources to maximize effectiveness?

Close Critical Gaps

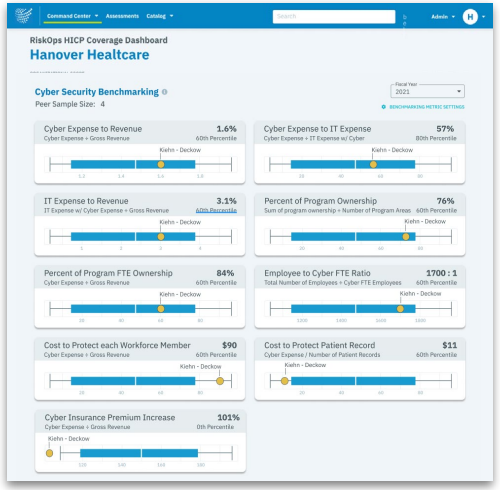
Do we have critical gaps in our security program that need immediate attention?

Make Meaningful Decisions

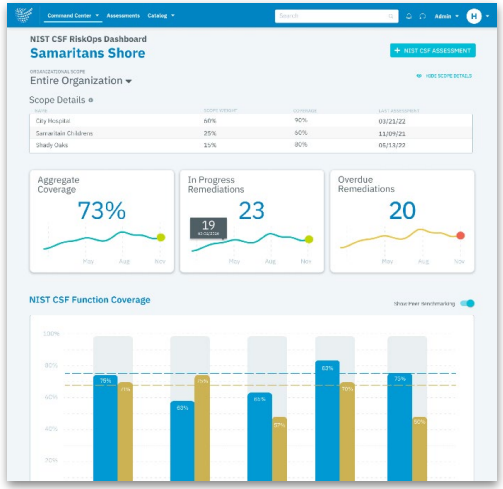
How do we enable decision making across cyber teams, investment committees & Boards?

Comprehensive, Actionable Visibility into Cybersecurity Program Maturity and Performance

Organizational Benchmarks



NIST CSF 1.1 Benchmarks



HICP Benchmarks

Stronger Together - Driving Community Collaboration

Co-Led by:

CENSINET

KLAS RESEARCH

American Hospital Association™

MISSION

To protect patient safety against cyber threats like ransomware, Censinet, KLAS Research, and the American Hospital Association conducted a landmark study in collaboration with leading health systems to establish robust, insightful, and actionable cybersecurity benchmarks.

The Healthcare Cybersecurity Benchmarking Study is the first initiative to combine (1) organizational metrics, (2) NIST Cybersecurity Framework, and (3) Health Industry Cybersecurity Practices (HICP) for comprehensive assessment.

Provided in Partnership with the Following Provider Sponsors:

Intermountain Health

Mass General Brigham

Cedars Sinai

Fairview Health Services

Baptist Health

Hartford HealthCare

dayton children's

Censinet Cyber Peer Benchmarking Scope

Censinet Cyber Peer Benchmarking

Standard offering for organizations looking to drive improvement in cybersecurity program maturity, resiliency, and coverage of recognized security practices.

- ✓ Complete access to all three peer benchmarking modules: NIST CSF 1.1, HICP, and Organizational Benchmarking
- ✓ Each module includes all standard Censinet assessment features to drive targeted improvement, including: enterprise assessment, automated action plans with tracking, built-in evidence and documentation capture, auto-generated summary reporting, risk ratings, workflow review, and organizational scopes with enterprise roll-up
- ✓ Currently supports HICP 2023
- ✓ NIST enterprise assessment includes out-the-box, curated questionnaires for 5 Functions, 23 Categories, and 108 Sub-Categories with automated action plans
- ✓ NIST peer benchmarks for 5 Functions and 23 Categories
- ✓ HICP peer benchmarks for 10 Practices Areas
- ✓ Organizational Benchmarking includes cyber program cost, productivity, and ownership KPIs

Category	Scope
NIST CSF 1.1 Peer Benchmarking	☑
Enterprise Assessment	☑
Built-In Evidence & Documentation Capture	☑
Risk Ratings	☑
Automated Action Plan Generation	☑
Auto-Generated Summary Reporting for Board	☑
Organizational Scopes with Enterprise Roll-Up	☑
Coverage Support for P.L. 116-321	☑
HICP Peer Benchmarking	☑
All Standard Censinet Assessment Features Above	☑
Support for HICP 2023	☑
Organizational Peer Benchmarking	☑

Prioritize and Communicate HICP Progress and Performance

Peer Benchmarking Reporting

- Identify critical gaps and immediate priorities with internal team
- Prioritize budget and allocate resources and workforce to goals
- Justify targeted cybersecurity investment with executives and Board
- Track live view of progress and relative performance against peers
- Show Enterprise-level views, or drill down into sub-categories or practices
- Audit reporting, demonstrate coverage per P.L. 116-321

Drive Proactive Remediations

- Surface findings based on NIST / HICP self-assessment responses
- Generate Corrective Action Plan (CAP) and recommended remediations
- Track remediations for disposition, mitigation, and closure
- Assign to SMEs internally, set priority, and track progress

Track/Trend HICP Performance

- Annual survey enables trend analysis of risk coverage, program performance
- Set goals and track progress live, quarterly, or year-over-year
- Demonstrate increasing program coverage and maturity to Board (or auditors, if necessary)

Study Key Findings

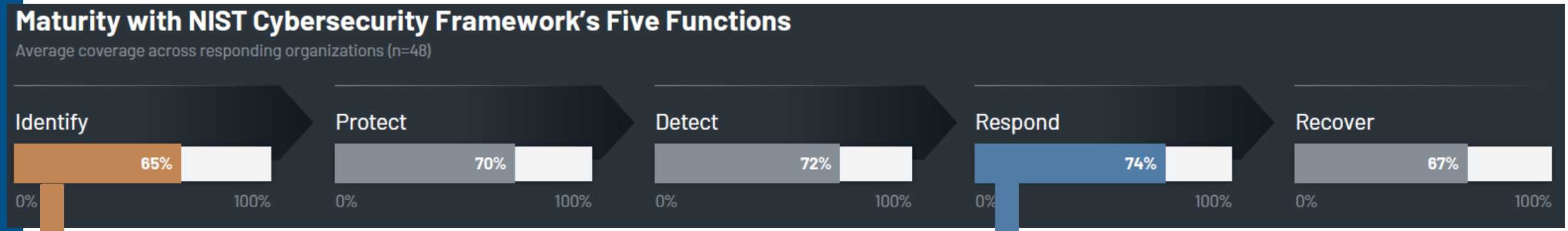
THE HEALTHCARE CYBERSECURITY BENCHMARKING STUDY

Key Findings

- ✓ Much like care delivery, healthcare cybersecurity better positioned to be reactive rather than proactive
- ✓ Risk Management Strategy requires greater transparency, especially around enterprise risk tolerance
- ✓ Many organizations lack complete, comprehensive inventory for both digital & non-digital assets
- ✓ Poor coverage across supply chain risk management persists, compounding enterprise risk exposure
- ✓ Higher third-party risk assessment coverage correlates with lower growth in cyber insurance costs
- ✓ Large organizations still under-covered across many Large-Only HICP practice areas
- ✓ While Email Protections are largely in place, still room for improvement in Medical Device Security
- ✓ CISO program ownership correlated with higher coverage in Medical Device Security, Network Management

Cybersecurity Mirrors Care Delivery in Relative Preparedness

Among all five NIST Functions, **Identify ranks lowest in maturity**. Akin to care delivery, Study shows stronger relative infrastructure in place to manage “acute episodes” in healthcare cybersecurity (aka, security incidents), rather than in managing prevention.

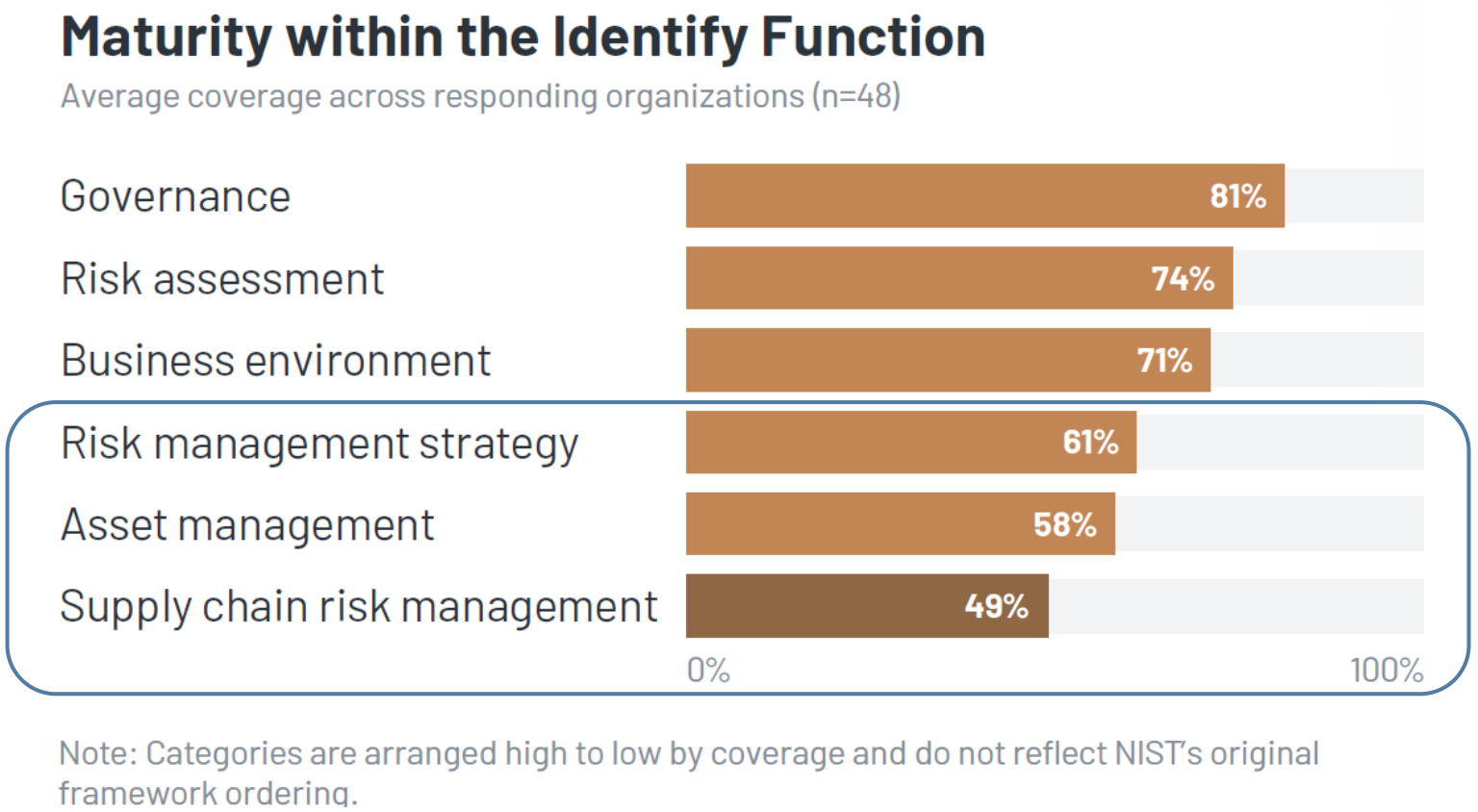


Driven by low coverage in Risk Strategy, Asset Management, and Supply Chain Risk Mgmt.

Driven by high relative coverage in incident response & analysis

Still Relatively Immature Across Three Critical Risk Categories

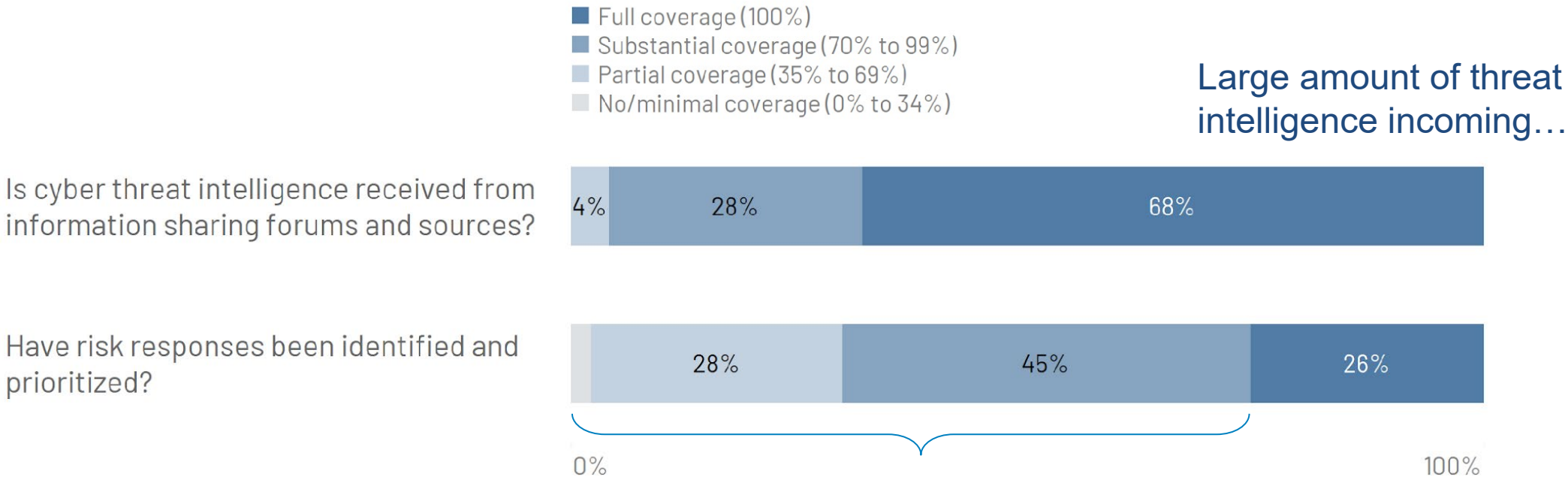
Within NIST Function Identify, Study shows current **low relative maturity** and room for improvement across Risk Management Strategy, Asset Management, and Supply Chain Risk



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

Challenging to Separate 'Signal' from 'Noise' in Risk Assessments

Within Risk Assessment category, Study shows meaningful divergence between the amount of cyber risk intelligence received vs. the ability to prioritize into actionable risk insights

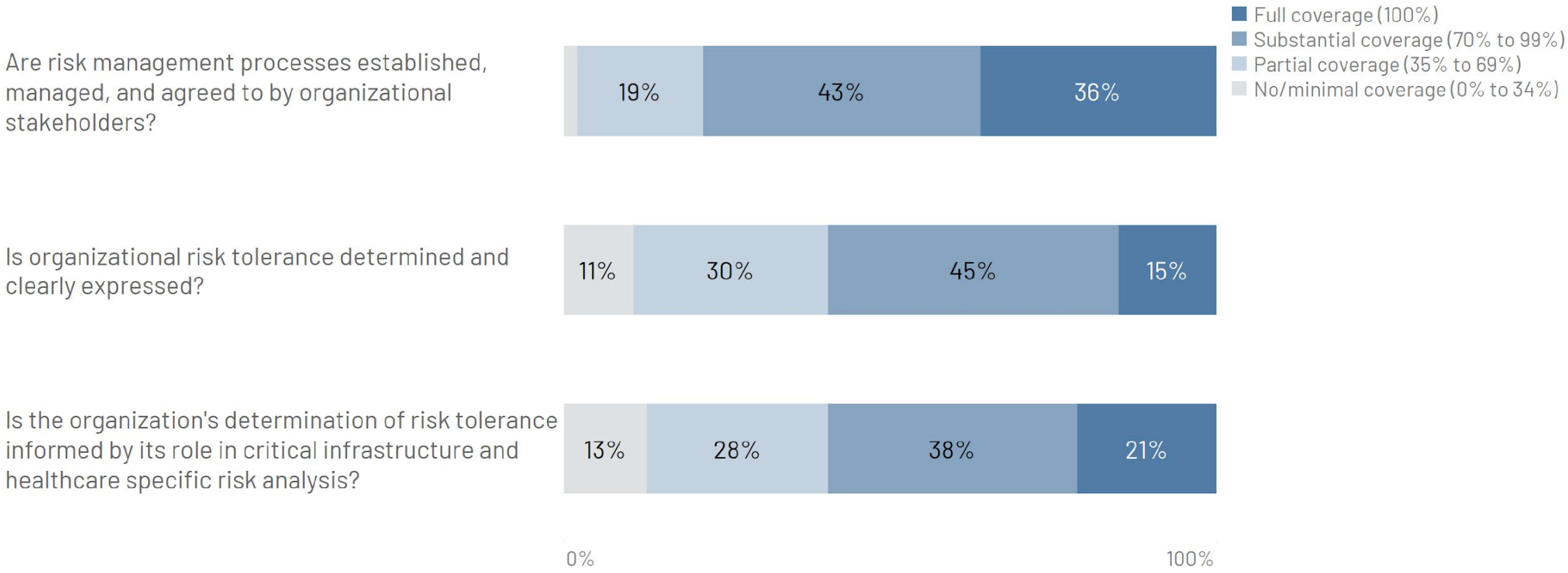


Large amount of threat intelligence incoming…

…but not always sure what's most critical, how to prioritize

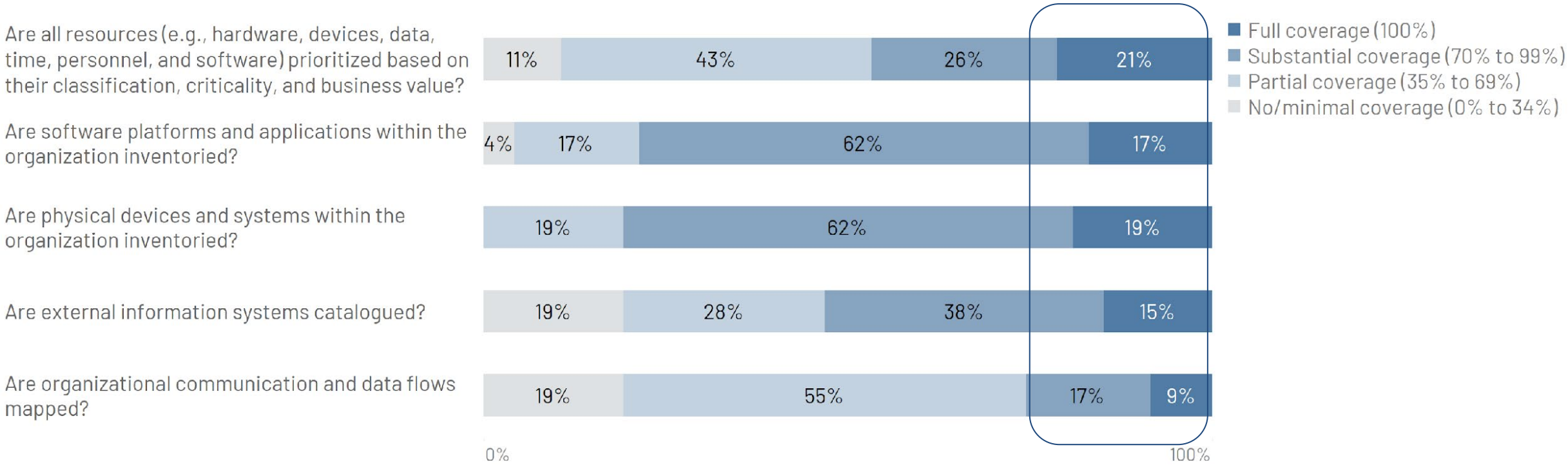
Risk Management Strategy Still Lacks Meaningful Transparency

While there is relative agreement across organizational stakeholders on risk processes, enterprise **risk tolerances remain largely non-transparent**, nor informed by broader dependencies like role in critical infrastructure or healthcare-specific inputs/analysis



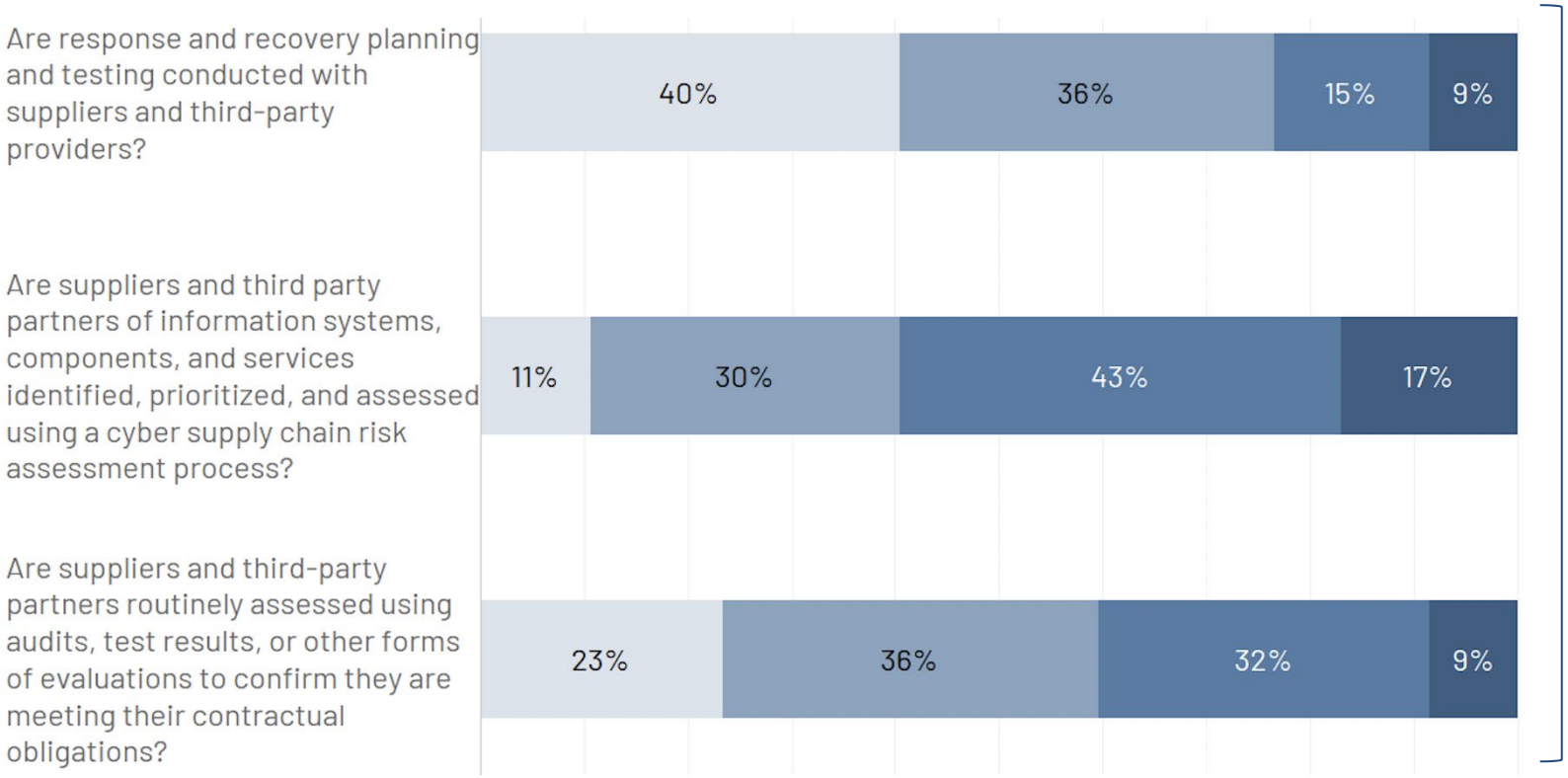
Asset Management Hindered by Incomplete Inventories, Poor Visibility

Asset Management suffers from **low coverage across several subcategories**, including lack of risk tiering, comprehensive inventory (digital & non-digital), and visibility into enterprise data flows



Poor Third-Party Risk Management Compounds Enterprise Risk Exposure

Very low coverage **(many with little-to-no coverage at all)** for key controls within Supply Chain Risk Management, including lack of risk assessment, routine reassessment, or response & recovery planning with suppliers and third-party vendors



Not Always IT / Digital Health
Non-Technical Suppliers Driving Largest Breaches in Recent Past…

Largest breach in 2022 caused by a printing and mailing vendor; 2.7M records

Largest breach in 2023 so far by a third-party administrator for health plans; 4.2M records

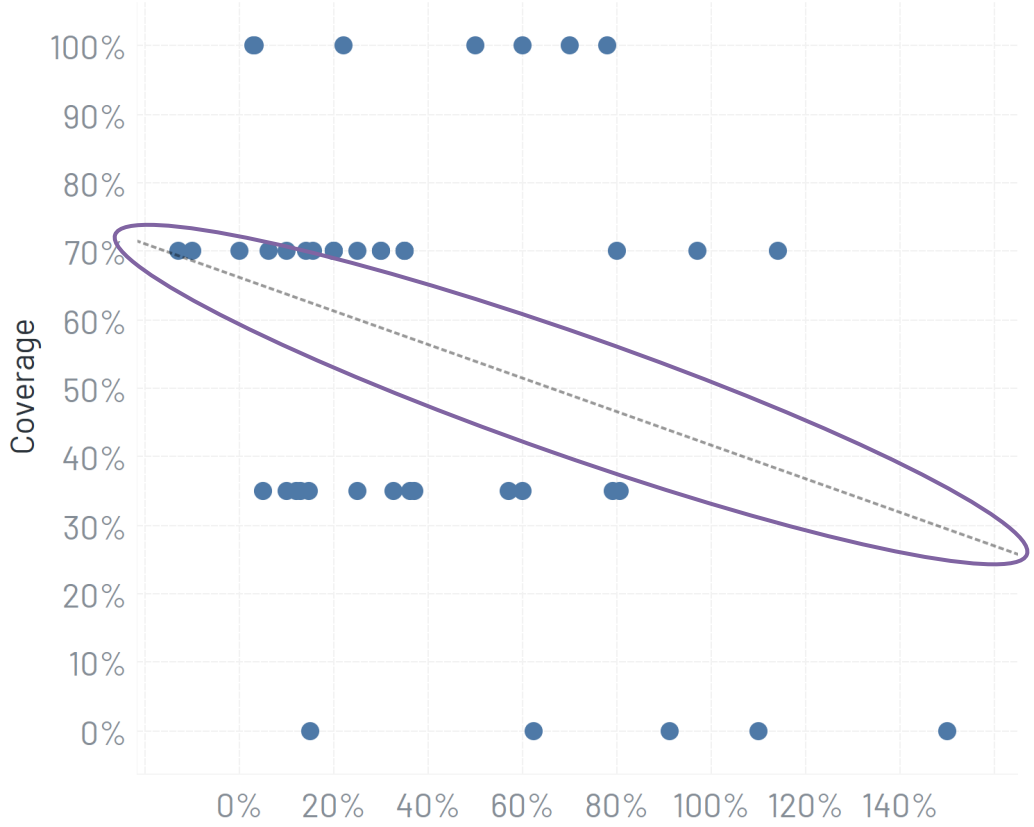
Third-Party Coverage Correlated With Lower Premium Cost Growth

Study shows **correlation between higher supplier and third-party risk assessment coverage and lower cyber insurance premium growth** year-over-year.

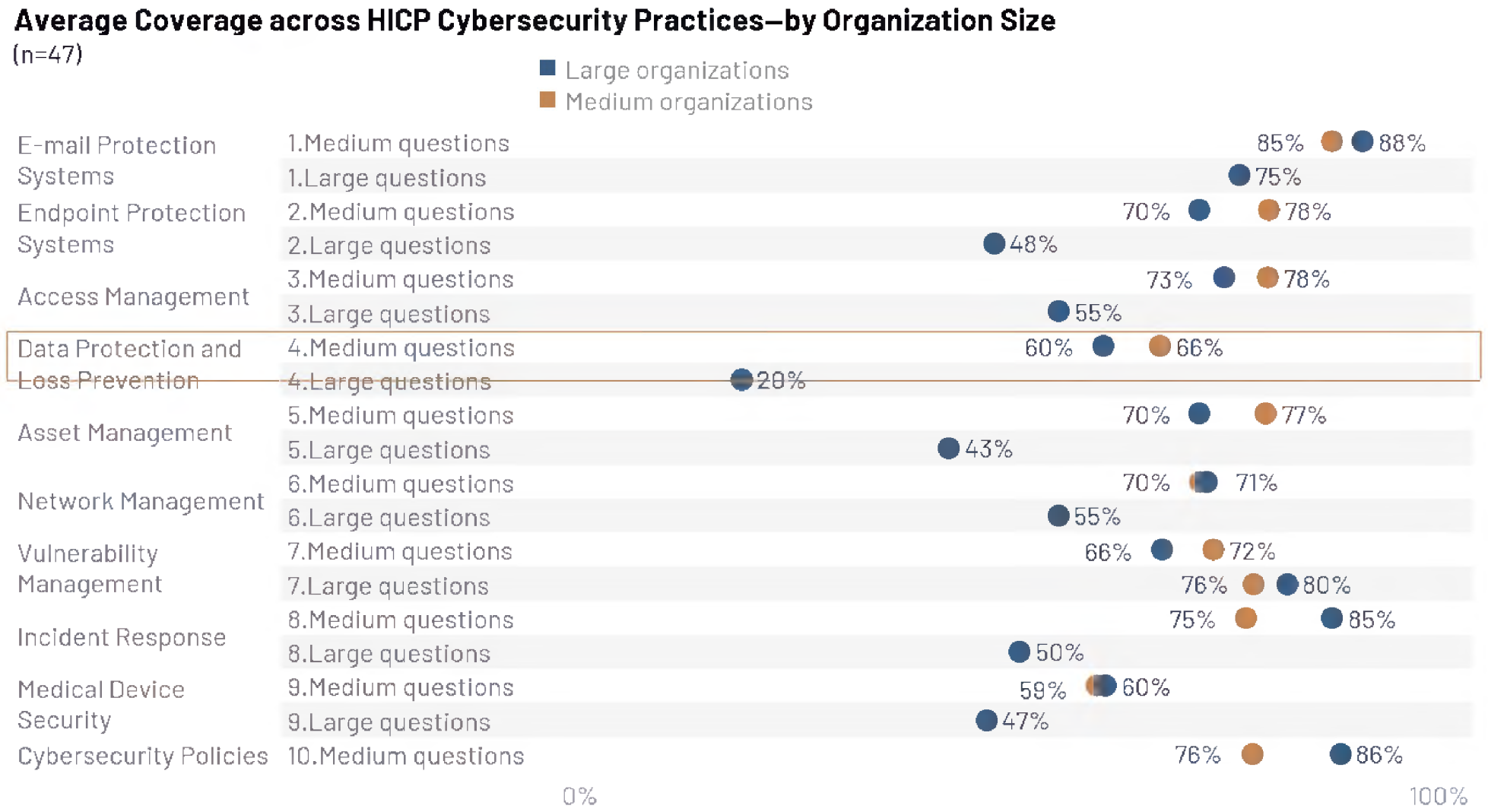
Maturity of Cyber Supply Chain Risk Assessment Process vs. Change in Cybersecurity Insurance Premium

Are suppliers and third party partners of information systems, components, and services identified, prioritized, and assessed using a cyber supply chain risk assessment process?

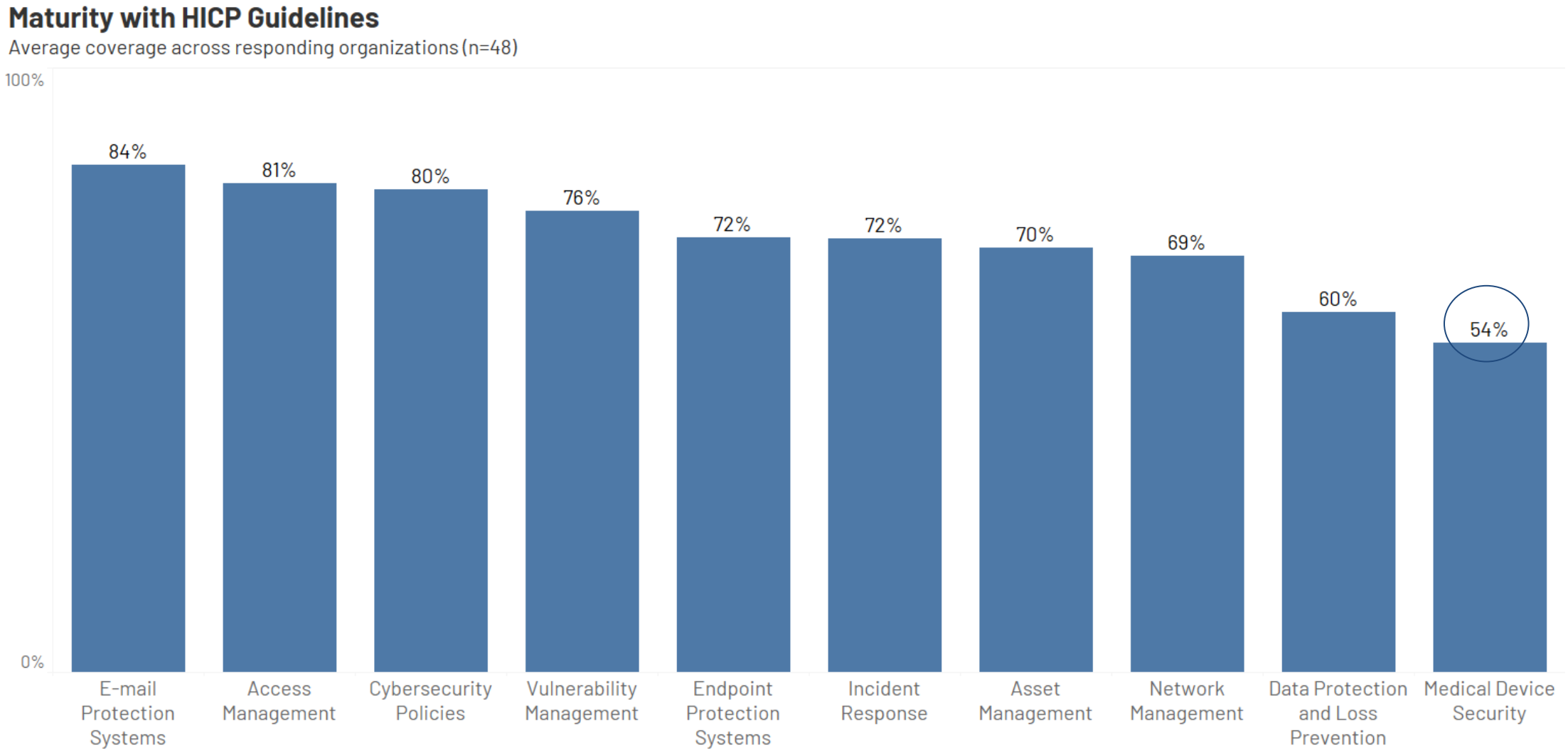
(n=44)



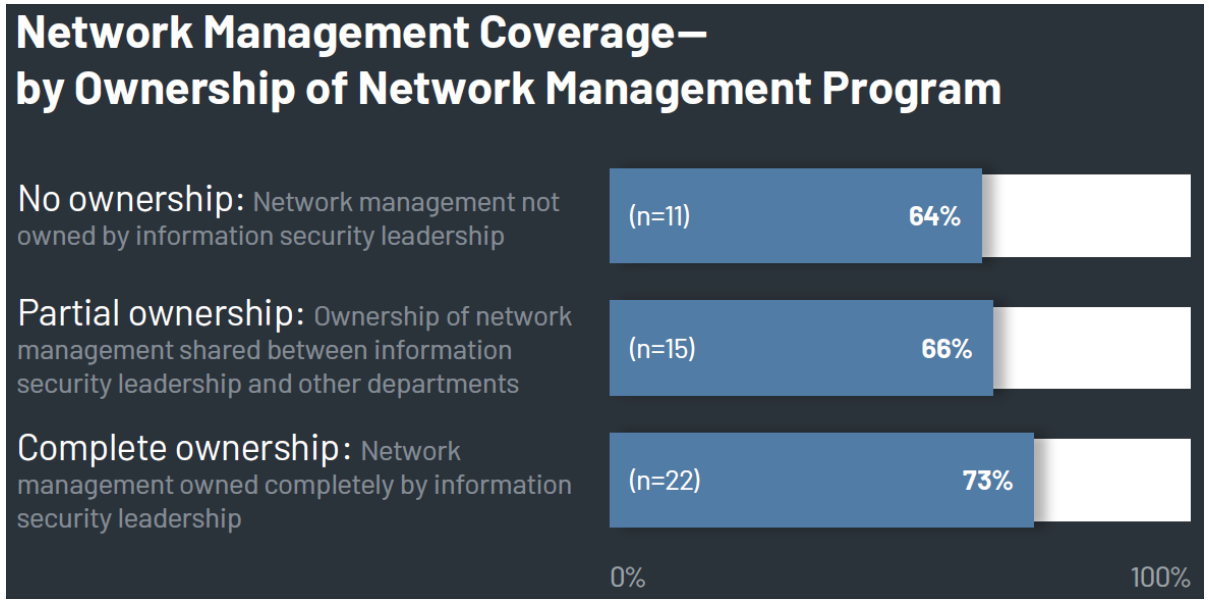
Still Challenging for Large Organizations to Cover Extended HICP Practice Set

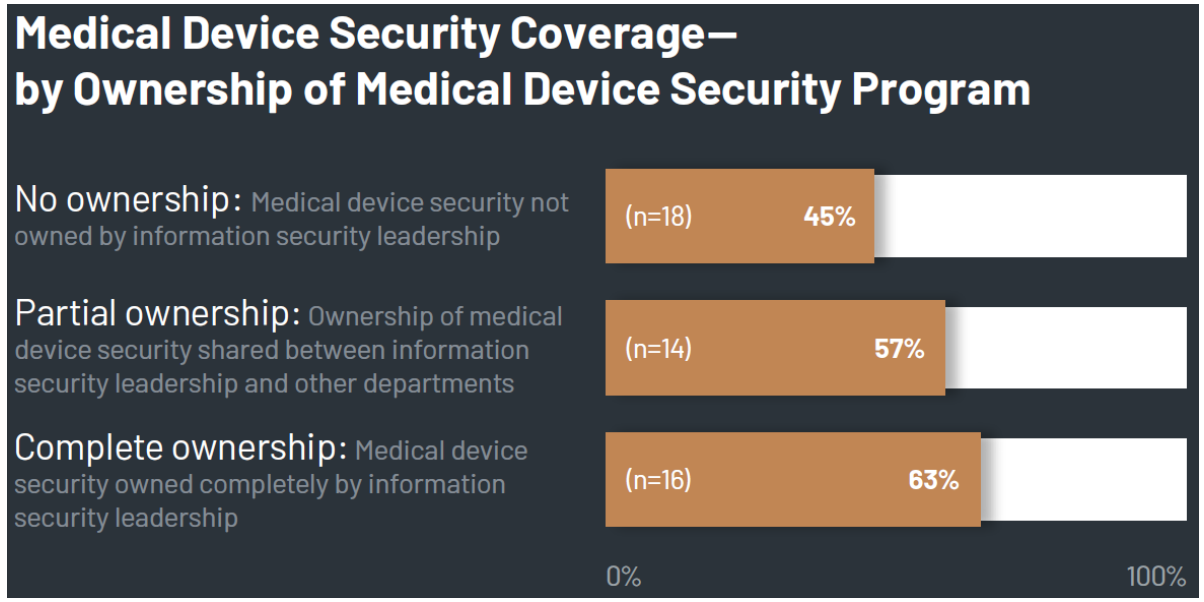


Email Protections in Place; Still Long Way to Go on Medical Devices



CISO Ownership Correlated with Higher Medical Device, Network Coverage





Organizations report **14% (9 percentage points) more coverage** in Network Management when security leader fully owns the program vs. with no security leader ownership.

Organizations report **40% (18 percentage points) more coverage** in Medical Device Security when security leader fully owns the program vs. with no security leader ownership.

Opportunities to Improve Across People, Processes, and Technology

- Areas where organizations have opportunities to improve include:
  - Inter-department coordination on cyber risk (e.g., asset inventory)
  - External communication with third parties and suppliers
  - Governance structure for cybersecurity leadership

- See Executive Summary and full report for more details

Summary and Next Steps

THE HEALTHCARE CYBERSECURITY BENCHMARKING STUDY

Enduring Value of Cyber Peer Benchmarking

Study in Brief

Censinet, KLAS Research, and the American Hospital Association conducted a landmark study in collaboration with leading health systems to establish actionable cybersecurity benchmarks.

The Healthcare Cybersecurity Benchmarking Study is the first initiative to combine benchmarks across three key categories for comprehensive cybersecurity program improvement:

(1) Organization cost, productivity, ownership KPIs
(2) NIST Cybersecurity Framework (NIST CSF)
(3) Health Industry Cybersecurity Practices (HICP)

Value of Cyber Peer Benchmarking

- ✓ **Drive continuous improvement** in cybersecurity program maturity, resilience, and best-practice coverage
- ✓ Keep program **consistent with most recent standards** and frameworks (e.g., HICP 2023)
- ✓ **Identify and close critical security gaps** & prioritize/justify future cyber investment with the Board and internal stakeholders
- ✓ Demonstrate continuous use (with evidence) of **'recognized security practices'** for P.L. 116-321

Drive Immediate Improvement in Cyber Hygiene with HICP

- Conduct enterprise assessment and peer benchmarking across the HICP 10 Practice Areas
- Capture evidence and documentation capture
- Generate an action plan
- Summary coverage reporting for Board and HHS Office for Civil Rights / P.L. 116-321
- Support HICP 2023 Edition

✓ Email Protection	✓ Network Management
✓ Endpoint Protection	✓ Vulnerability Management
✓ Access Management	✓ Incident Response
✓ Data Protection	✓ Medical Device Security
✓ Asset Management	✓ Cybersecurity Oversight and Governance

Webinar Participants Receive Exec Summary

- ✓ Visit https://klasresearch.com and search for “Benchmarking Study”

Questions

Do you follow us on Social Media?
Check us out at **@ask405d**

Linkedin.com/company/hhs-ask405d

https://405d.hhs.gov

Closing

For more cybersecurity information and best practices, be sure to check out the 405(d) publication:

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) 2023 Edition

The publication details the top five threats facing the healthcare industry and the ten practices to mitigate them. Read the entire publication on our website: https://405d.hhs.gov