

HHS 405(d) Program

Cyber Safety is Patient Safety

How HHS is providing the healthcare & public health (HPH) sector with impactful resources, products, and tools to raise awareness and strengthen the sector's cybersecurity posture against cyber threats.



In this Presentation

Here's what we'll cover:

Why You Should Care About Cybersecurity

[A Brief History of](#) the 405(d) Program

Where Do you Stand [Hospital Resiliency Landscape Analysis](#)

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

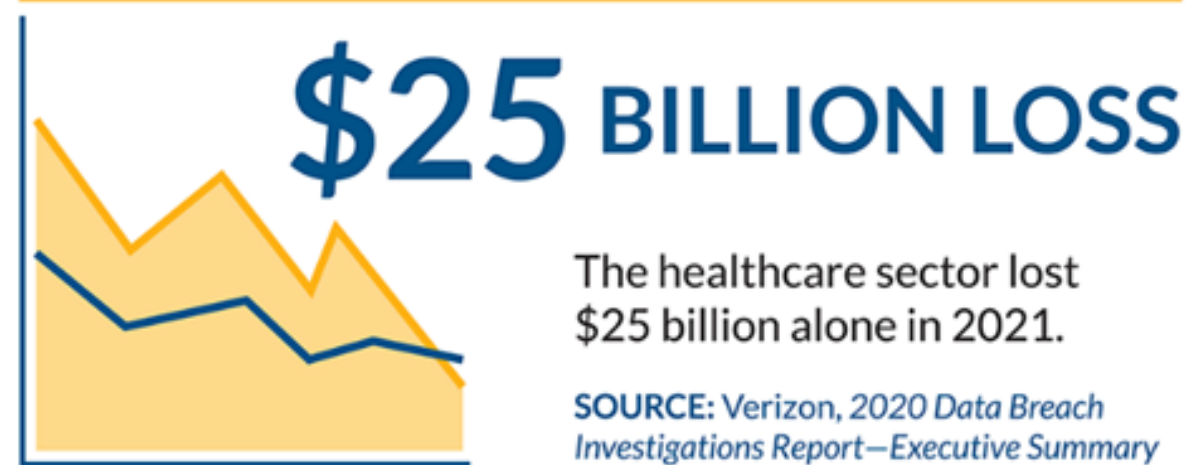
How We Can Help You

Regulatory Incentive to Implement Cybersecurity within Your Organization

Questions

In July 2021, there were **52** reported hacking/IT incidents in which the protected health information of **5,393,331** individuals was potentially compromised.

SOURCE: HIPAAJournal.com, July 2021 Healthcare Data Breach Report



\$65 BILLION

The healthcare industry is expected to spend around **\$65 billion** on cybersecurity between 2017 and 2021.
SOURCE: Herjavec Group, *The 2020 Healthcare Cybersecurity Report*

In July 2021, there were **70** reported data breaches of **500** or more records.

SOURCE: HIPAAJournal.com, July 2021 Healthcare Data Breach Report

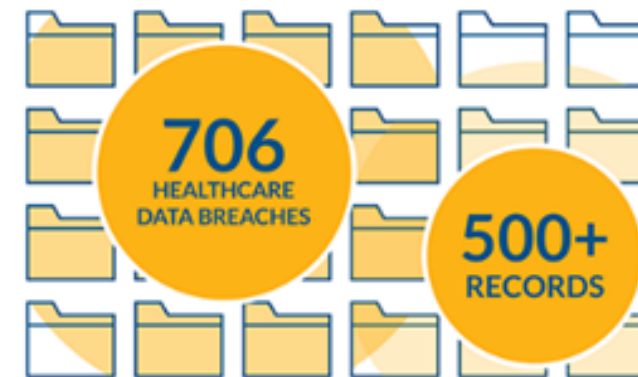


July 2021 was the **5th consecutive month** where data breaches in the healthcare sector have been reported at a rate of **2 or more per day**.

SOURCE: HIPAAJournal.com, July 2021 Healthcare Data Breach Report

From the start of August 2020 to the end of July 2021, the healthcare data of **44,369,781** individuals has been exposed or compromised.

SOURCE: HIPAAJournal.com, July 2021 Healthcare Data Breach Report



From the start of August 2020 to the end of July 2021, there have been **706 reported healthcare data breaches** of **500 or more records**.

SOURCE: HIPAAJournal.com, July 2021 Healthcare Data Breach Report

Under Attack

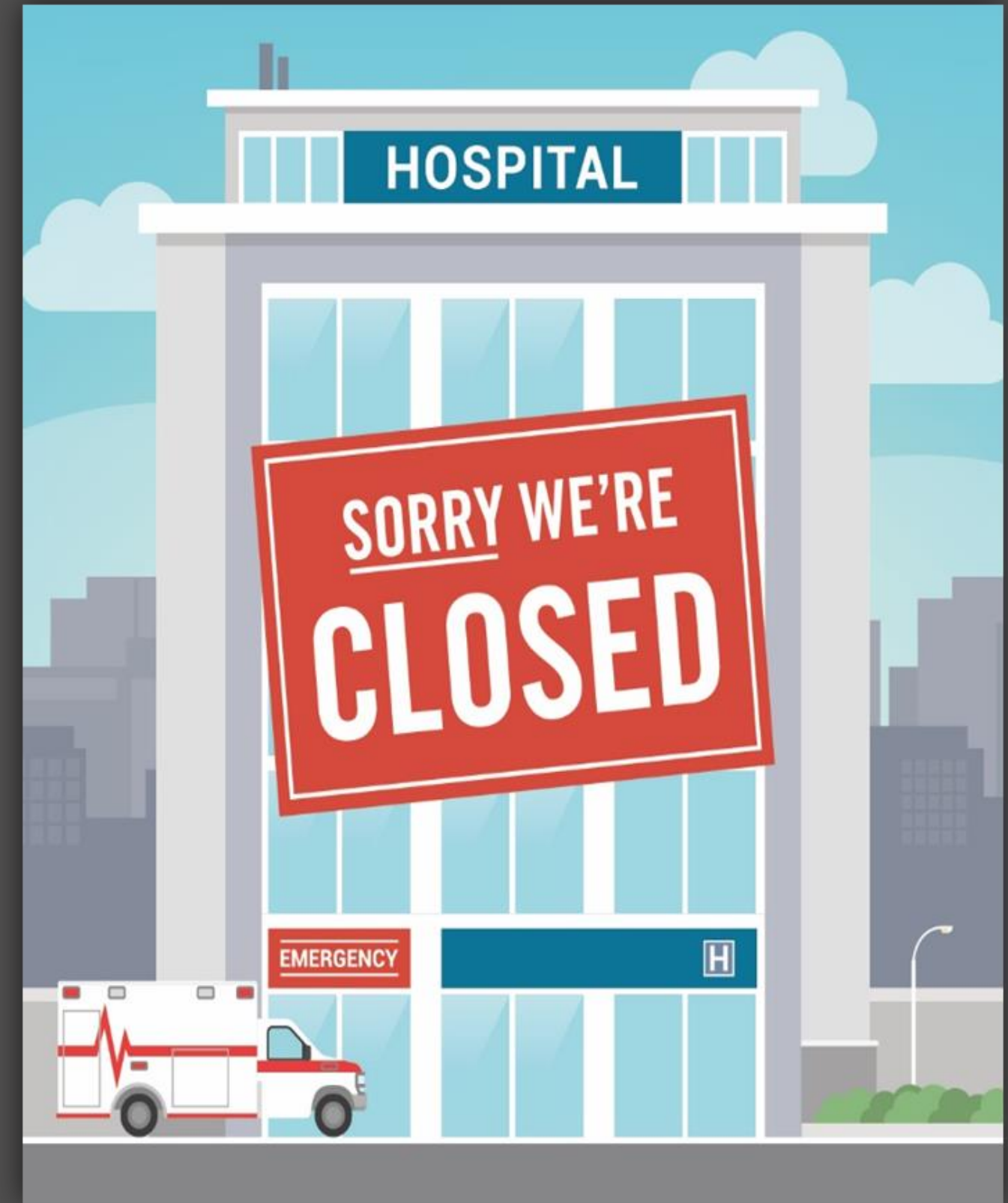
Cyber attacks are an increasing threat to the Health and Public Health (HPH) sector. As seen with delayed procedures, diagnostic imaging and laboratory system shutdowns, patient diversions, and more, these attacks can directly compromise patient safety



Cyber Safety = Patient Safety

Cyber attacks in healthcare affect every aspect of an organization but most importantly they affect patient safety.

A single cyber attack has the potential to shut down care facilities, erase important patient health history, and put your patient's health and identity at risk.



A brief history of



HHS 405(d) Aligning Health Care Industry Security Approaches

2015	Cybersecurity Act of 2015 (CSA) calls upon HHS to work with industry to Align Health Care Industry Security Approaches
2017	HHS in partnership with the Health Sector Coordinating Council establish the 405(d) Task Group. The Task Group begins to develop a "best practices" publication
2018	After significant analysis of the current cybersecurity issues facing the HPH Sector, the Task Group developed and released the <i>Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients</i>
2019	HHS builds a federal program around the 405(d) Task Group, with a focus on HPH cyber outreach and engagement
2023	405(d) Releases HICP 2023, Landscape Analysis and the Knowledge on Demand Platform

What We Do

As the leading collaboration center of the Office of the Chief Information Officer/Office of Information Security, the 405(d) Program is focused on providing the HPH sector with useful and impactful resources, products, and tools that help raise awareness and provide vetted cybersecurity practices, which drive behavioral change and move towards consistency in mitigating the most relevant cybersecurity threats to the sector.

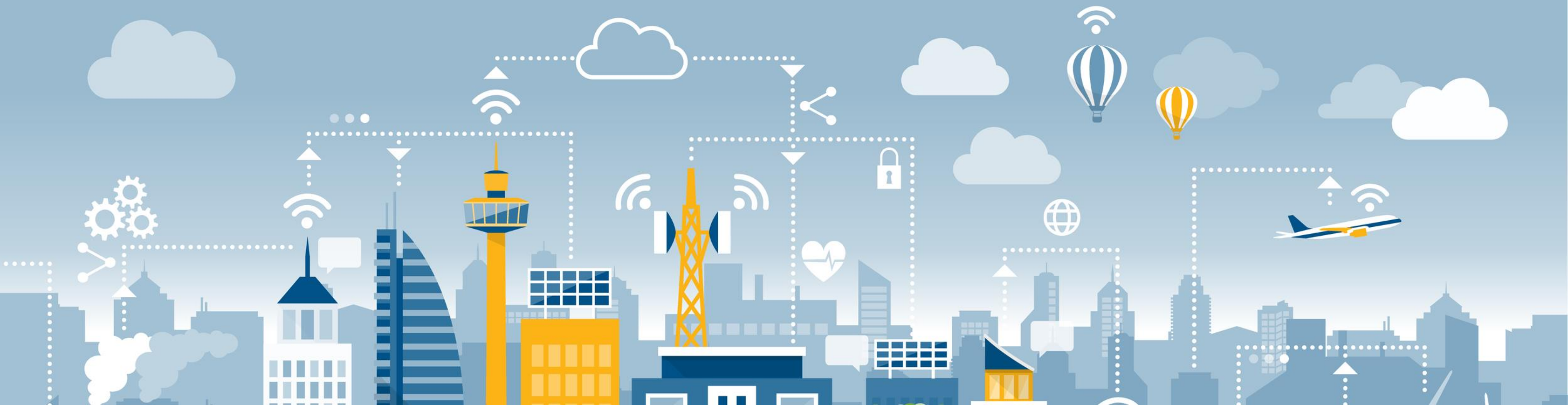


Who We Are

The 405(d) Program is a collaborative effort between industry and the federal government to align healthcare industry security practices to develop consensus-based guidelines, practices, and methodologies to strengthen the healthcare and public health (HPH) sector's cybersecurity posture against cyber threats.

Hospital Resiliency Landscape Analysis

Released April 16, 2023



Document Overview

What to expect and What we covered



Executive Summary		Threat Analysis		Capabilities and Performance Assessment	Adoption of HICP Practices
Overview of key observations, HICP Practice Adoption and a note on Data sources		Overview of the evolving threat of ransomware and links between threats and mitigations		Covers staff analysis, cyber expense, coverage to NIST and HICP	Covers practices in HICP that have significant progress, need improvement, and need additional research, and non urgent items

Key Observations



Directly targeted ransomware attacks aimed to disrupt clinical operations are an outsized and growing cyber threat to hospitals

Variable adoption of critical security features and processes, coupled with a continually evolving threat landscape can expose hospitals to more cyber-attacks

Hospitals report measurable success in implementing email protections, which is a key attack vector

Supply chain risk is pervasive for hospitals. Only 49% of hospitals state they have adequate coverage in managing risks to supply chain risk management

Medical devices have not typically been exploited to disrupt clinical operations in hospitals.

Key Observations



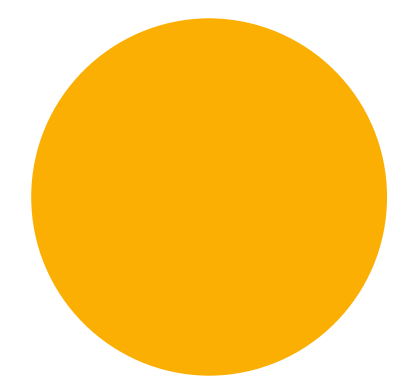
There is significant variation in cybersecurity resiliency among hospitals

The use of antiquated hardware, systems, and software by hospitals is concerning

Cybersecurity insurance premiums continue to rise

Securing cyber talent with requisite skills and experience is challenging

Adopting HICP improves cyber resiliency



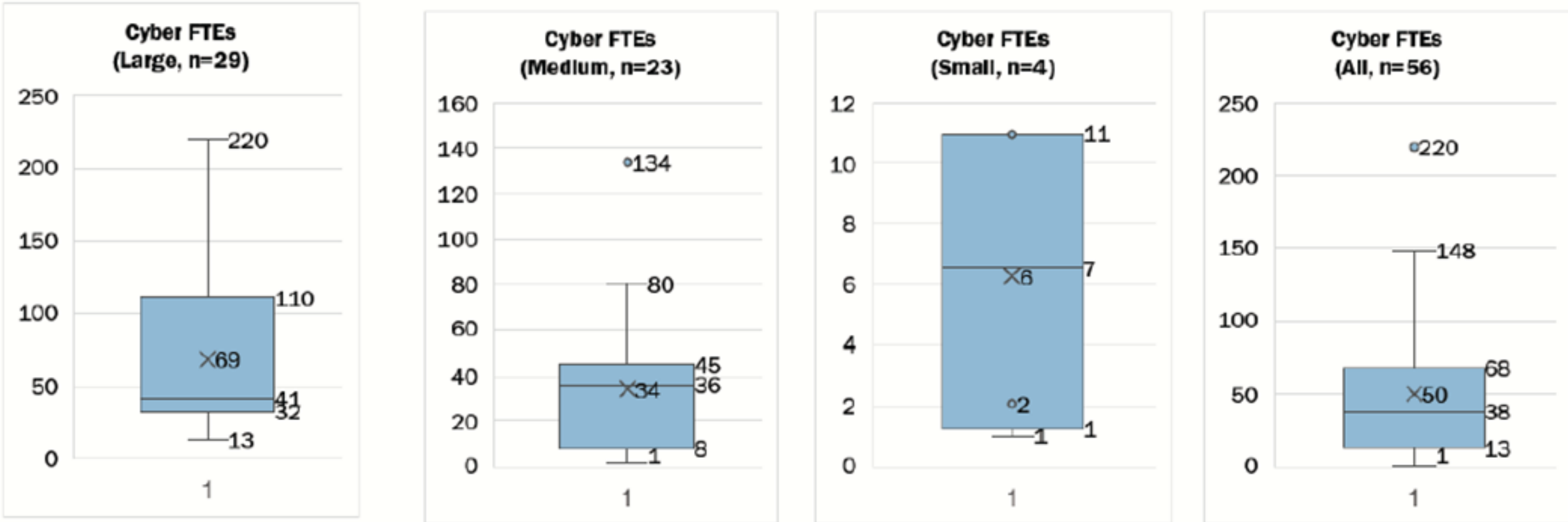
Insights. How Do You Compare?



Staffing Analysis

On average, organizations employed or contracted 50 cybersecurity full-time employees (FTEs), though the median was 38. This number varied by the size of the organization, based on HICP size analysis.

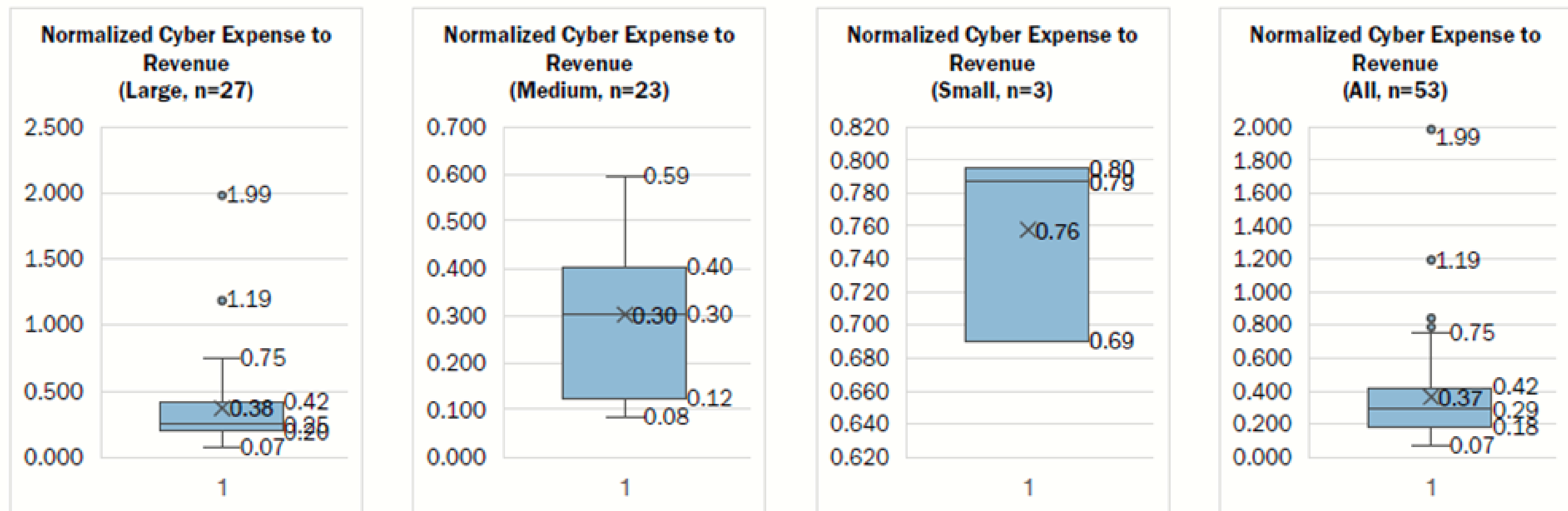
Figure 7 Staffing Analysis of organizations by size



Cyber Expense to Revenue

It was rare that the cybersecurity program underneath the CISO was directly responsible for, and budgeted for, all common components of the cybersecurity program. For example, in some organizations the CISO was not responsible for firewall management or identity and access management. However, these programmatic elements are still important for determining cybersecurity capability and they still introduce cost.

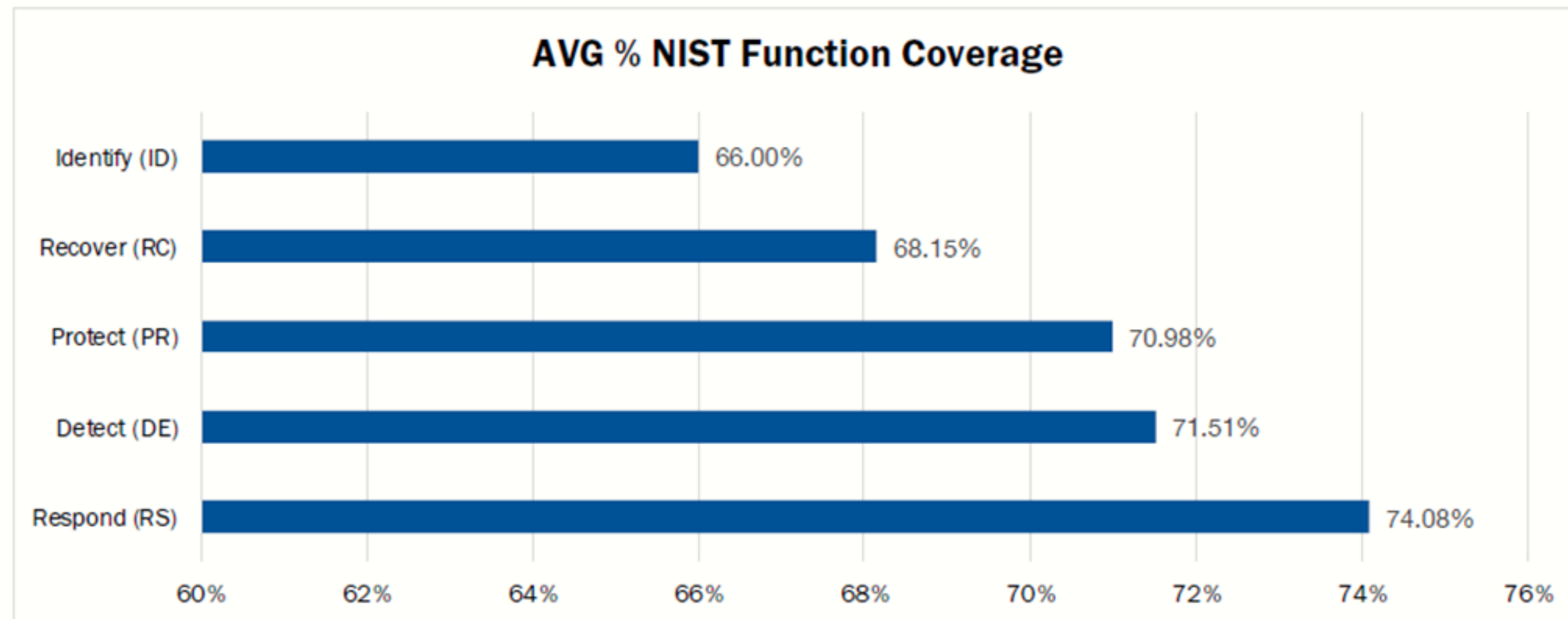
Figure 8 Normalized Cyber expense to revenue



Industry Coverage to NIST CSF

Based on the Censinet/AHA/KLAS Study, the participating hospitals claim that they provided 70.7% of coverage to the NIST CSF. Based on the NIST Function level, the lowest coverage was Identify (66.0%) and the highest coverage was Respond (74.1%)

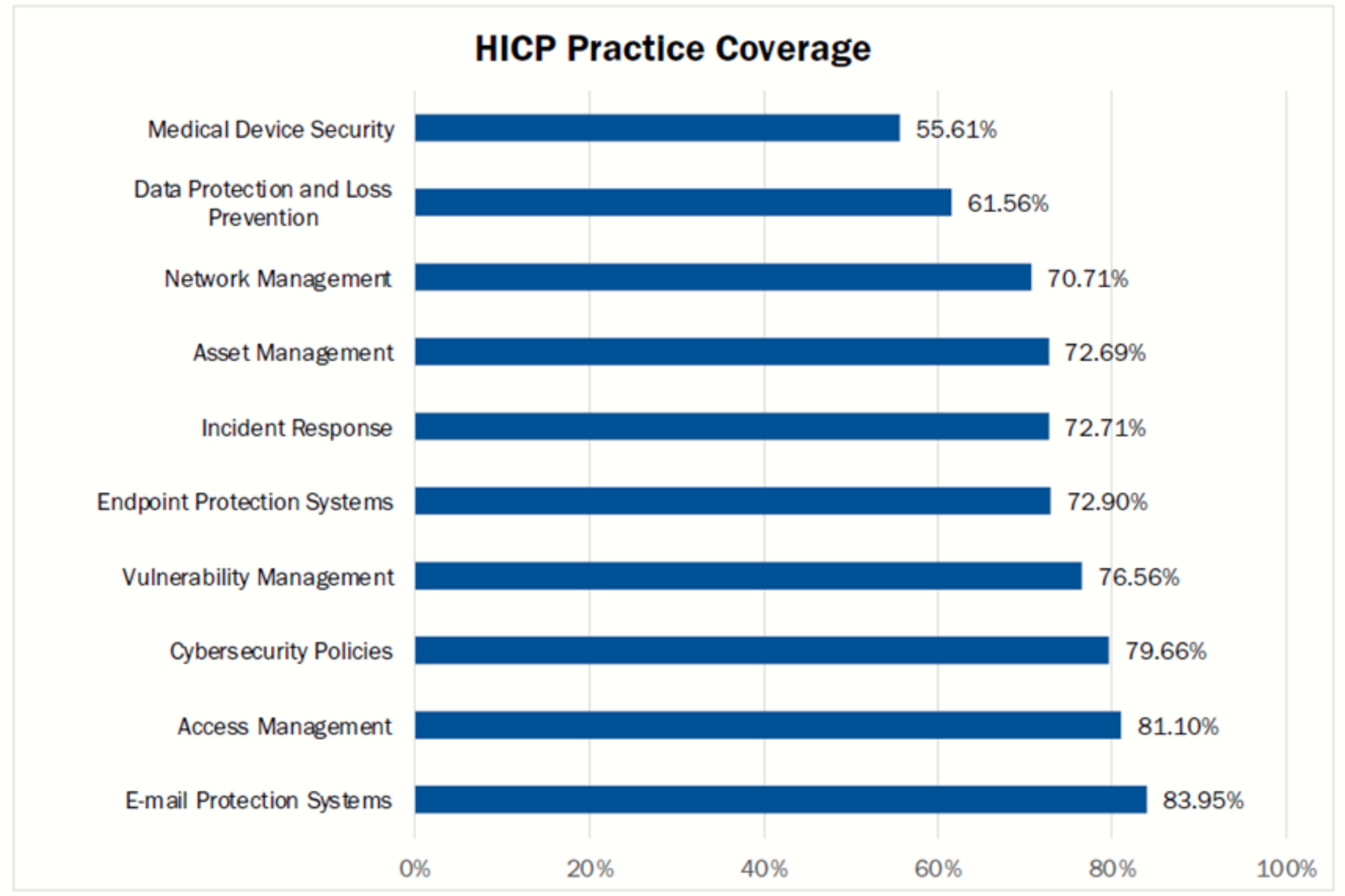
Figure 9 NIST Category level percent of coverage



Industry Coverage to HICP

Based on the Censinet/AHA/KLAS Study of 2023, on average, hospitals claim to have 72.05% of the HICP practices covered, with email protection being the highest amount of coverage and medical device security being the lowest.

Figure 11 HICP average percent coverage by practice



Adoption of HICP Practices

The analysis of the data sources shows that hospitals' adoption of HICP practices fall into the following four categories:



No Action Required – Significant Progress Made

- Email protection systems

Urgent Improvement Needed

- Endpoint protection systems
- Access management
- Network management
- Vulnerability management
- Incident response

Additional Research Required

- Asset management
- Medical device security
- Cybersecurity policies

Further Attention Recommended - Not Urgent

- Data protection and loss prevention

NEW 405(d) RELEASE

HICP 2023

Health Industry Cybersecurity
Practices: Managing Threats and
Protecting Patients



HICP 2023

405(d)'s Cornerstone Publication

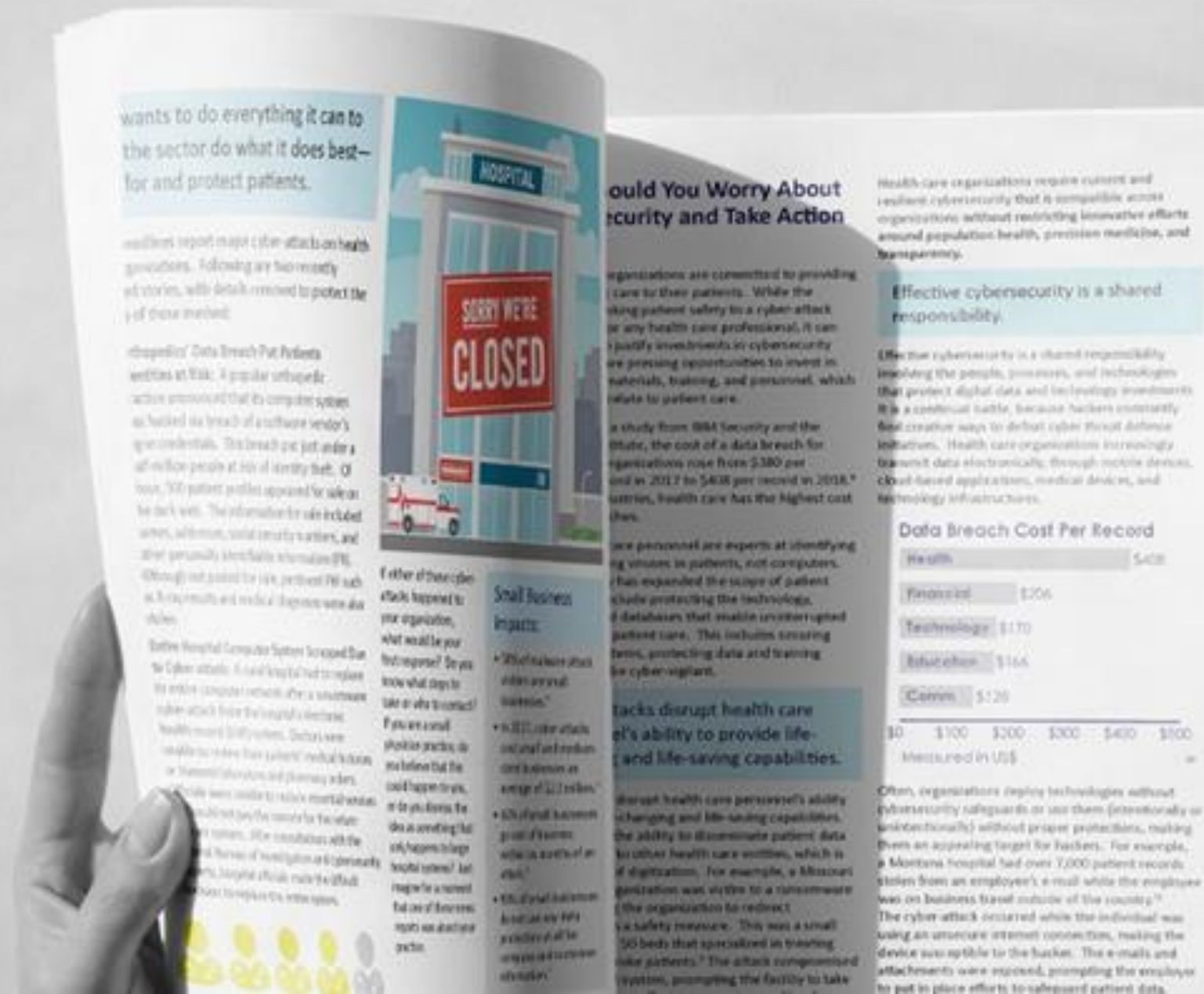
Cybersecurity threats evolve each year and with them comes new mitigating practices. The HICP 2023 Edition has been updated by industry and government professionals to include the most relevant and cost-effective ways to mitigate the current cybersecurity threats the HPH sector is facing. After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group agreed on the development of three HICP components—a main document and two technical volumes, and a robust appendix of resources and templates.

The Main Document

examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.

Technical Volume 1 discusses these ten cybersecurity practices for small healthcare organizations.

Technical Volume 2 discusses these ten cybersecurity practices for medium and large healthcare organizations.








What's New in HICP 2023

The 405(d) Task Group has been working over the past 2 years to update HICP to ensure that the publication stays relevant and provides the sector with the most up-to-date best practices.



Main Document Updates	Top Ten Practices Updates	Additional NEW Sub-Practices
<p>The HICP Main Document has been updated to renew our call to action to maintain patient safety and includes new cybersecurity strategies such as Zero Trust and Defense in Depth.</p> <p>Email Phishing is now Social Engineering</p>	<p>Cybersecurity Practice #9 on Network Connected Medical Devices has been fully updated</p> <p>Cyber Practice #10 is now Cybersecurity Oversight and Governances</p>	<p>Cyber insurance</p> <p>Cybersecurity Risk Assessment and Management</p> <p>Attack Simulations</p> <p>Medical Devices (Major Updates)</p>

Top 5 Threats

-  **Social Engineering**
-  Ransomware
-  Loss or Theft of Equipment or Data
-  Insider Accidental or Malicious Data Loss
-  **Attacks Against Network Connected Medical Devices**

Top 10 Practices covered in HICP

- Email Protection Systems
- Endpoint Protection Systems
- Access Management
- Data Protection and Loss Prevention
- Asset management
- Network Management
- Vulnerability Management
- Incident Response
- Medical Device Security
- Cybersecurity Oversight and Governance

Cybersecurity Practice #9 Network Connected Medical Devices

A new executive summary was added to this practice in Technical Volume 2 detailing how to secure network connected medical devices plus the below additions:

- Added unique IoT considerations and other unique challenges specific to medical devices.
- Added Goals of Risk Mitigation for Medical devices.
- Added guidance for applying other practices already covered in HICP toward medical devices.
- Moved Asset Management to the first sub-practice of Cybersecurity Practice #9 and added graphics to illustrate the need for Asset Discovery and Security tools.
- Added Zero-Trust model to discussion of Endpoint Protections.
- Added steps for implementing and maintaining Identity and Access Management, including further explanation of Remote Access.
- Added a section on micro-segmentation under Network Management.

Areas of Impact

PHI

Medium Sub-Practices

9.M.A Asset Management

9.M.B Endpoint Protections

9.M.C Identity and Access Management

9.M.D Network Management

9.M.E Vulnerability Management

9.M.F Contacting the FDA

Large Sub-Practices

9.L.A Security Operations and Incident Response

9.L.B Procurement and Security Evaluations

Key Threats Addressed

Attacks against network connected medical devices that can affect patient safety

405(d) Resources

Prescription Poster: Network Connected Medical Devices

Sub Practice: Cybersecurity Insurance (10.S.D and 10.L.A)

Cyber insurance is one option that can help protect your business against losses resulting from a cyber-attack. 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.

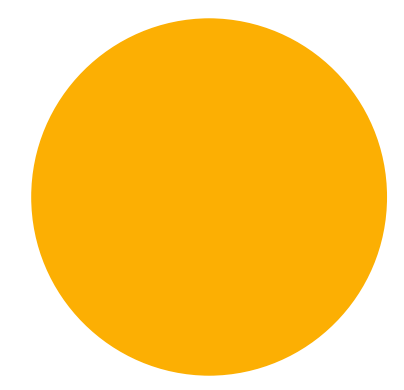
Key Information in New Sub-Practice:

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

Information on: What your cyber insurer provider will do in the event of a cyber attack



How We Can Help You



405(d) Outreach & Program Resources

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

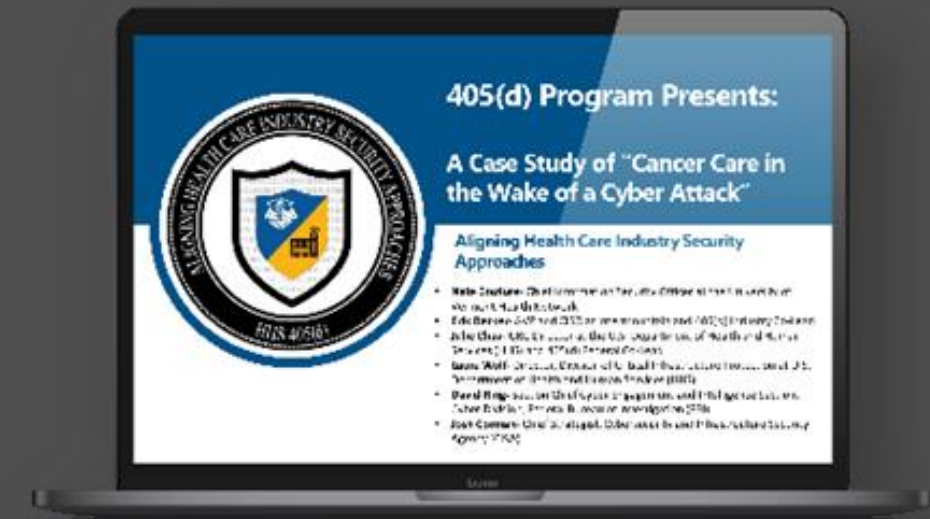
The 405(d) Program produces Bi-monthly Newsletters, SBARs, and Spotlight Webinars to increase cybersecurity awareness and present new and emerging cybersecurity news and topics, as well highlight the HICP Publication

Knolwedge on Demand

The 405(d) Program, is launching 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.





HHS 405(d) Knowledge on Demand

The 405(d) Program, in collaboration with industry, launched new cybersecurity training platform on its website—405d.hhs.gov—titled Knowledge on Demand (KOD).

The delivery methodologies for Knowledge on Demand include:



Job Aids

These are single documents with key tips related to the topic. This format is meant to be used as an "on-the-job" resource tool. They can provide instructional steps if necessary to meet the training objectives.

Key Benefits: Job aids are useful since an employee can reference one throughout the day-to-day operations. They can also act as reminders about topics covered in more formal trainings.



Learning Management System (LMS) File

Content intended for an LMS will be similar in look and experience as the previously discussed Interactive Training video. Content will be exported and saved to a file type compatible for import to an organization's LMS platform.

Key Benefits: This delivery method will allow larger organizations that already have an LMS platform and want to add our content directly to their system. This will be especially useful if they do not already have cybersecurity training courses.



Interactive Training Videos

These videos are launched from the 405(d) KOD webpage but can also be downloaded by the end user. They include recorded audio to take the trainee through the video along with interactive content to include knowledge checks and animations.

Key Benefits: This interactive delivery method provides end users flexibility to access each threat topic at their own time due to the easy of access from the website.

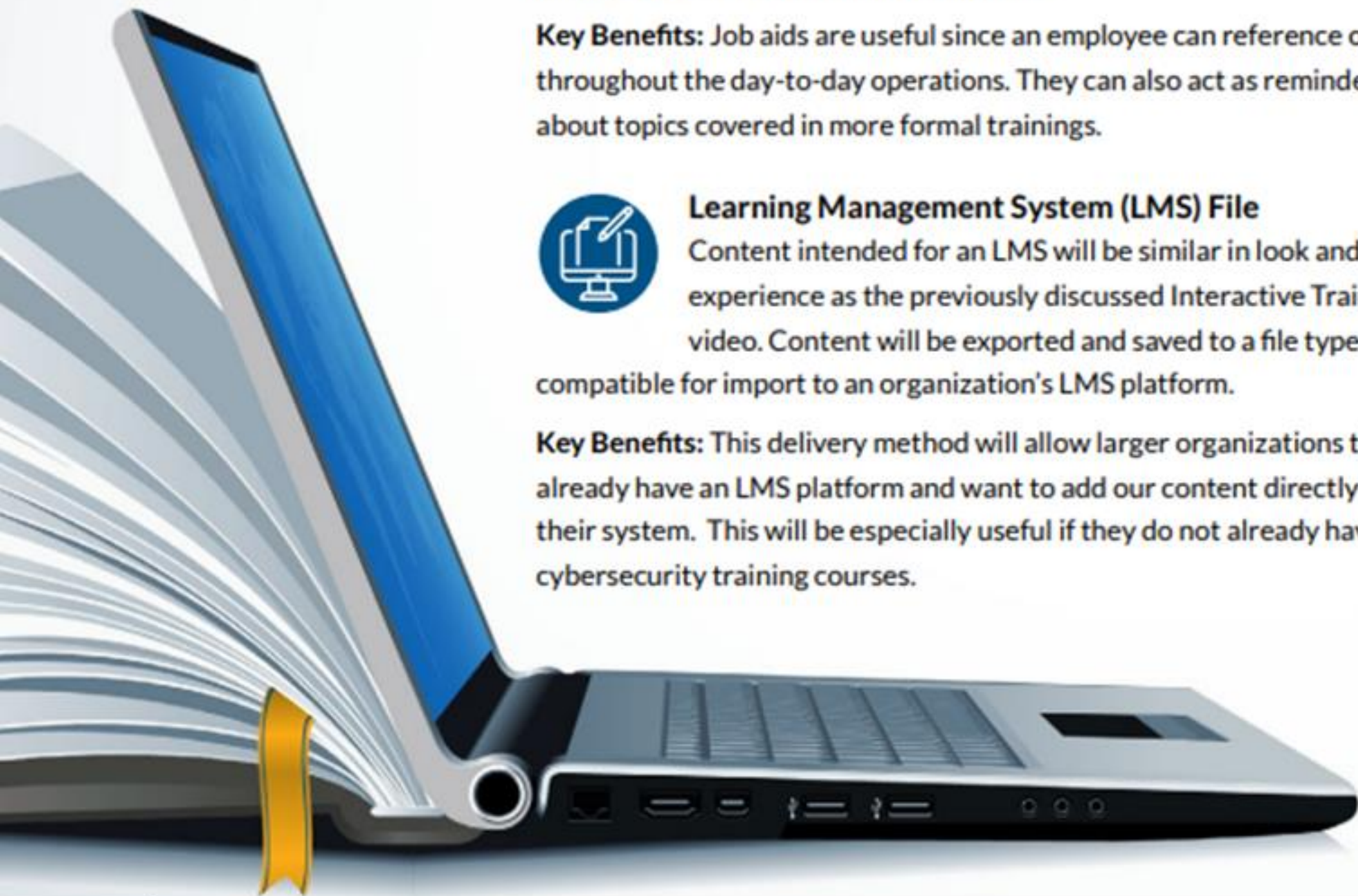


PowerPoint Trainings

These can be leveraged for in person or on-site presentations. These will include facilitator notes with slide specific content and knowledge checks to reinforce learning. Such presentations can be delivered in presentation mode or in a "Lunch n Learn" format at your location.

Key Benefits: PowerPoint presentations are useful tools because they encourage discussion between employees and managers. It also allows the organization to better tailor their training to meet their specific needs.

Visit our website at 405d.hhs.gov/KOD to experience this new learning platform and explore the ways you can integrate this platform into the awareness education for all employees at your healthcare organization.



2021 HITECH Amendment

H.R.7898 — 116th Congress (2019-2020)

To amend the Health Information Technology for Economic and Clinical Health Act (HITECH) to require the Secretary of Health and Human Services (HHS) to consider certain **recognized security practices** of covered entities and business associates when making certain determinations, and for other purposes.

Signed January 5, 2021 | Public Law No: 116-321

What are Recognized Security Practices?

The standards, guidelines, best practices, methodologies, procedures, and processes developed under the:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- HHS 405(d) Program approaches
- Other programs and processes that address cybersecurity and are developed, recognized, or promulgated through regulations under other statutory authorities



What does this new amendment do?

If you can prove you have been following these Recognized Security Practices for the previous 12 months, HHS must consider that when making decisions for things like audits and enforcement.

HHS can take Recognized Security Practices into consideration to:

- Mitigate fines for violations
- Award an early, favorable termination of an audit
- Mitigate conditions proposed for resolution agreements



Questions?



Do you follow us on social media?
Check us out at [@ask405d](#)
Website: [405d.hhs.gov](#)

