Spotlight Webinar! HICP 2023, Hospital Resiliency Landscape Analysis, Knowledge on Demand

Aligning Health Care Industry Security Approaches

- **Erik Decker – VP and CISO Intermountain, 405(d) Industry Co-Lead, Chair, Cybersecurity Working Group of HSCC**
- **Cindi Bassford- Partner Guidehouse, 405(d) Task Group Wave Lead**
- **Douglas Nock, Rob Wood -Centers for Medicare & Medicaid Services**

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 this webinar series.

- 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

- **June**
  - New Cyber Hygiene Posters
  - 405(d) Post
- **July**
  - Spotlight Webinar! Date, Time, Topic TBD

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

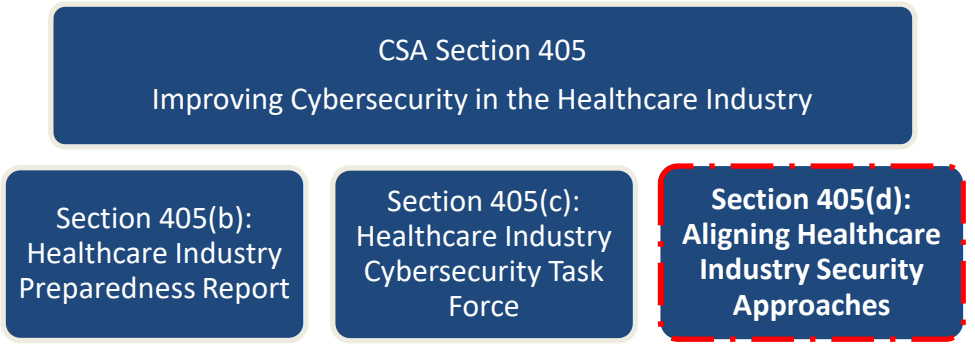
Time	Topic	Speaker
10 minutes	Opening Remarks and Introductions	Julie Chua- HHS Director GRC and 405(d) Federal Co-Lead
25 Minutes	Hospital Cybersecurity Resiliency Landscape Analysis	Erik Decker- Intermountain, 405(d) Industry Co-Lead, Chair, Cybersecurity Working Group of HSCC CMS- Douglas Nock, Rob Wood
25 Minutes	HICP 2023 Overview	Cindi Bassford – Guidehouse, 405(d) Wave Lead
15 Minutes	Knowledge on Demand	Nick Rodriguez, 405(d) Program Manager
10 Minutes	Q&A	405(d) Team
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 !



2021 HITECH Amendment

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

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

405(d) Outreach & Program Resources

Below you can find examples of communication 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

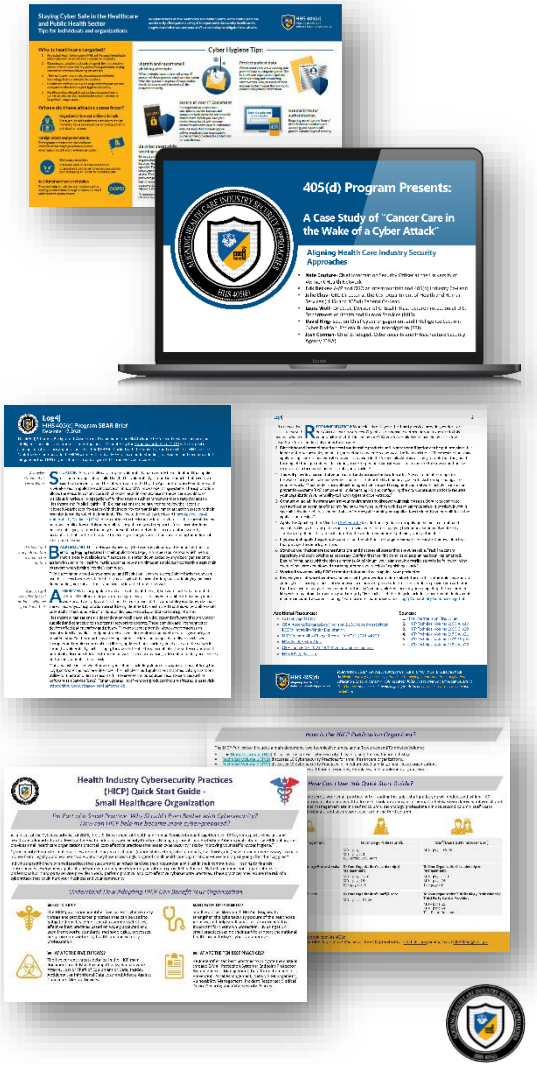
The 405(d) Program produces Bi-monthly Newsletters, SBARs, and Spotlight Webinars to increase cybersecurity awareness and present new and emerging cybersecurity news and topics, as well highlight the HICP Publication!

Knowledge on Demand

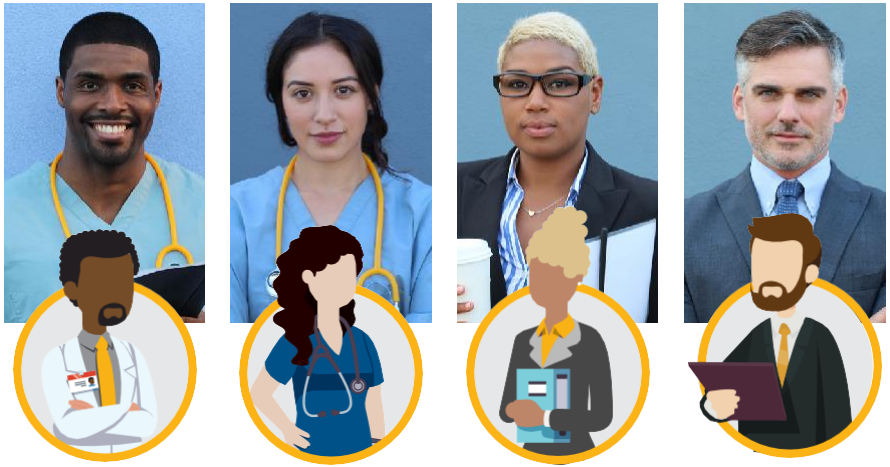
The 405(d) Program, is launching a new cybersecurity training platform on its website—405d.hhs.gov.This new cybersecurity education platform will include multiple delivery methodologies to reach the varied size health care facilities across the country. The platform will include five cybersecurity awareness 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.



405(d) Task Group



The core of the 405(d) program is it's task group members. Convened by HHS in 2017, the 405(d) task group is comprised of over **150 +** information security officers, medical professionals, privacy experts, and industry leaders.

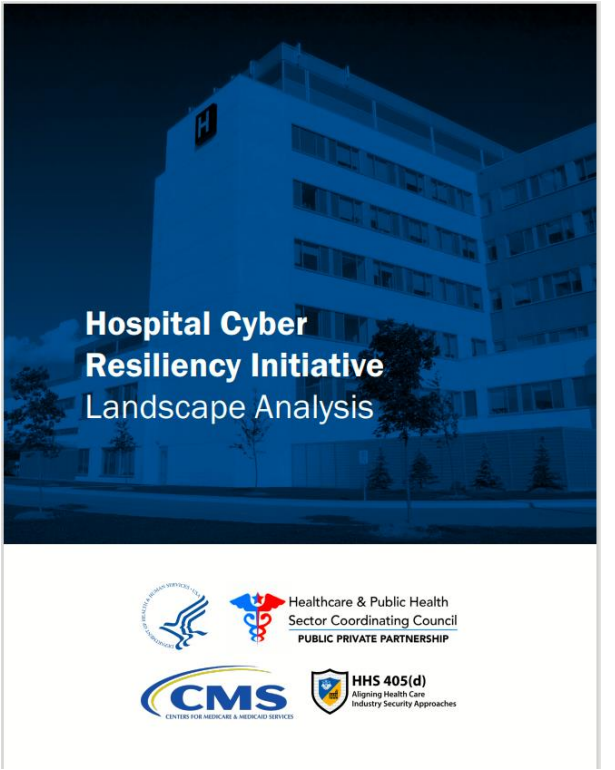
The task group members help drive all aspects of the 405(d) program, to include official program products, awareness campaigns, engagements, and outreach channels.

The task group is actively collaborating and working on a host of new resources for the sector including a new ERM Cybersecurity publication, and Operational Continuity Cyber Incident Checklist which both are planned to be released in 2023.

Hospital Resiliency Landscape Analysis

- **Erik Decker- Intermountain, 405(d) Industry Co-Lead, Chair, Cybersecurity Working Group of HSCC**

- **Douglas Nock, Rob Wood Centers for Medicare & Medicaid Services**

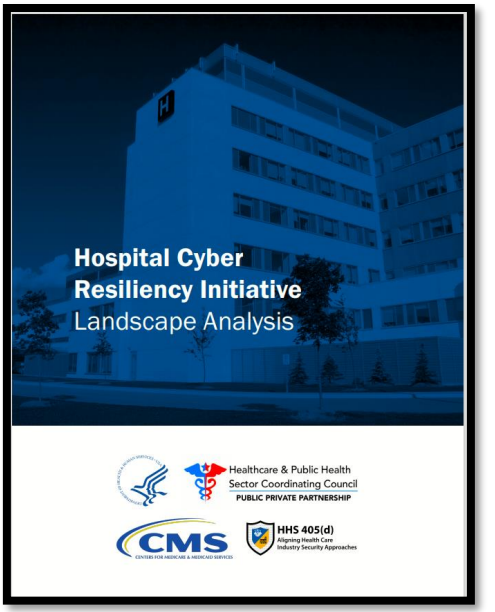


Hospital Cyber Resiliency Initiative Landscape Analysis

The HPH Sector has faced dramatic increases in cyber-attacks intended to cause disruption to the care continuum. In response to this growing threat, the HHS 405(d) Program conducted Landscape Analysis, which reviewed active threats attacking hospitals and the cybersecurity capabilities of hospitals operating in the United States.

Document Overview:

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



*Data Sources: The quantitative data was gathered by utilizing CHIME's Most Wired Surveys, a separate survey in partnership with Censinet and the American Hospital Association of 59 hospitals, and 20 conversations with geographically and demographically diverse hospitals

Key Observations

Our analysis from the two (2) quantitative studies combined with participating hospital conversations resulted in a series of key observations- See below for a few

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

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

    1. Adoption of MFA is taking place in over 90% of surveyed hospitals- why not 100%?
    2. 89% of the hospitals surveyed indicated that they were conducting regular vulnerability scanning at least on a quarterly basis
    3. 86% of the hospitals surveyed responded that their users are informed and trained on performing their cybersecurity related duties and responsibilities
    4. The delivery of in-home care, accelerated by COVID-19, is growing and expanding the cyber threat landscape

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

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

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

Key Observations Continued…

6. **There is significant variation in cybersecurity resiliency among hospitals**

7. **The use of antiquated hardware, systems, and software by hospitals is concerning**
    6. 96% of small, medium, and large sized hospitals claim they were operating with end-of-life operating systems or software with known vulnerabilities, which is inclusive of medical devices.

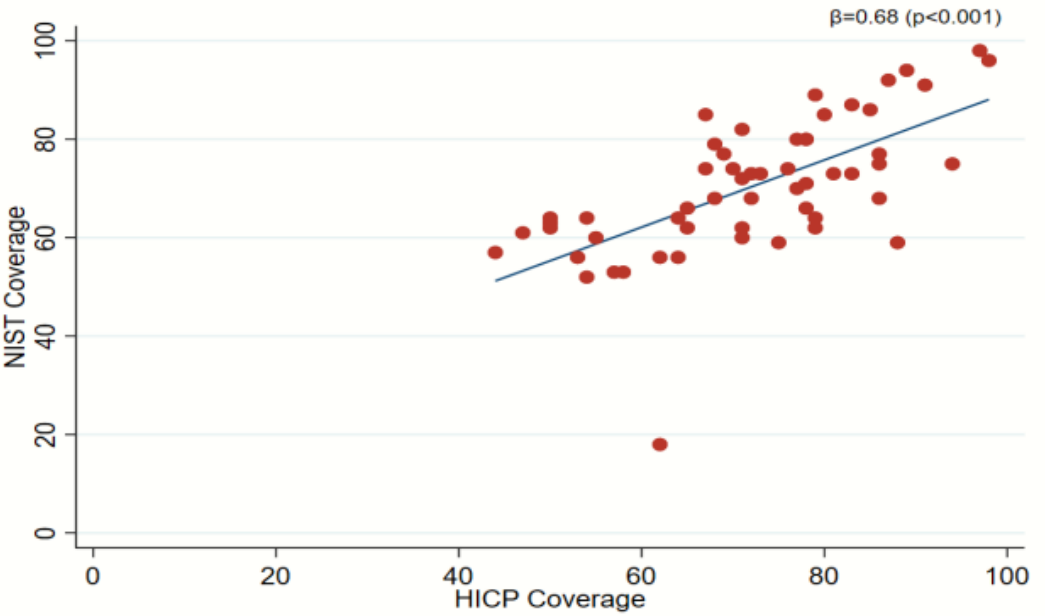
8. **Cybersecurity insurance premiums continue to rise**
    6. On average, cybersecurity premiums increased by 46% in 2021. Five of fifty-six hospitals surveyed in 2022 experienced increases more than 100%, whereas 32 experienced increases just below 35%.

9. **Securing cyber talent with requisite skills and experience is challenging**

10. **Adopting HICP improves cyber resiliency**
    - An interesting correlation that was uncovered during analysis was a strong connection between those who have adopted HICP and robust NIST CSF coverage. This indicates that organizations that focus on HICP Practices will gain value and benefit towards managing implementation of the NIST CSF cybersecurity framework.

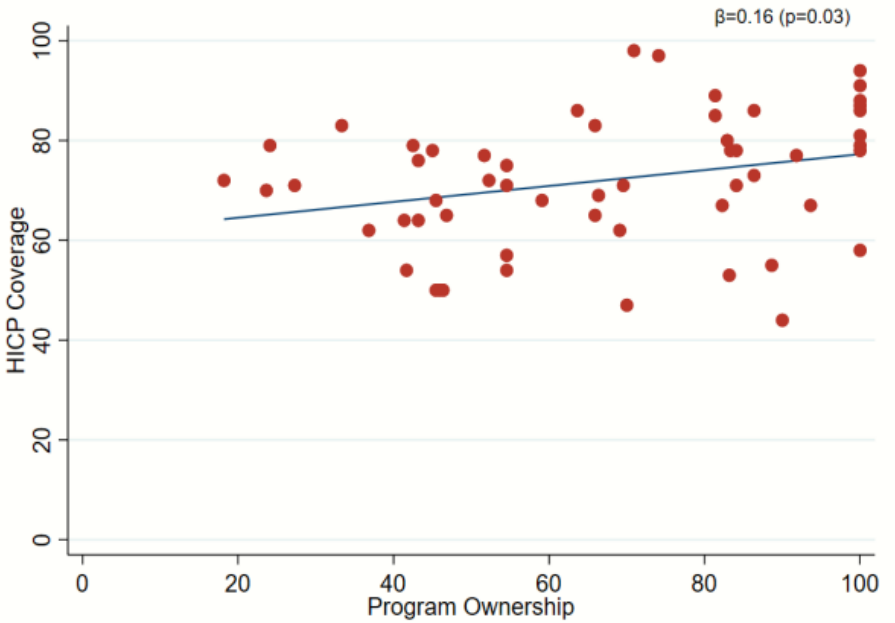
Correlation of HICP and NIST Coverage

Figure 1 Correlation of HICP and NIST coverage



Quantified Association of HICP Coverage

Figure 2 Quantified association of HICP coverage



Threat Analysis

Our assessment, based on the data sources used, identified numerous cybersecurity threats to U.S. hospitals, such as:

1. Ransomware and Ransomware-as-a-Service (RaaS) attacks
2. Cloud exploitations by threat actors; with data suggesting a 95% increase from 2021 in cloud exploitation cases
3. Phishing/Spear-Phishing Attacks; specifically those attacks that overcome MFA through social engineering
4. Software and zero-day vulnerabilities
5. Distributed Denial of Service attacks (DDoS)

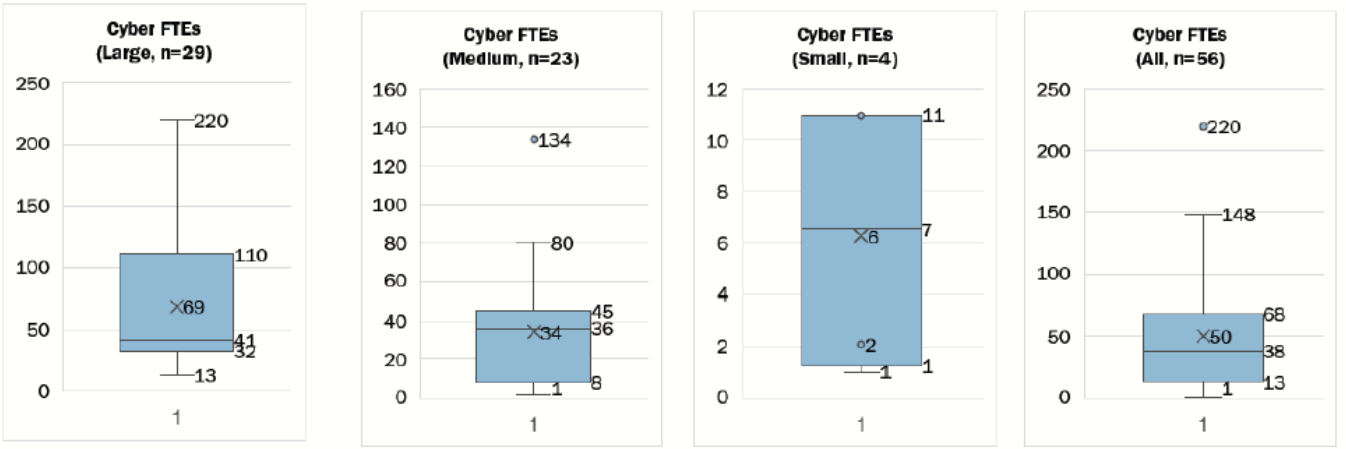
Threat Analysis- Key Take Aways

- Human Directed Attacks make up 71% of attacks
- Access Broker theft up 112%, used by the human directed attacks
- Time to move off initial intrusion point is 1 hour 28 minutes (this is the lateral movement off the originally compromised host to another stage to obfuscate)

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.

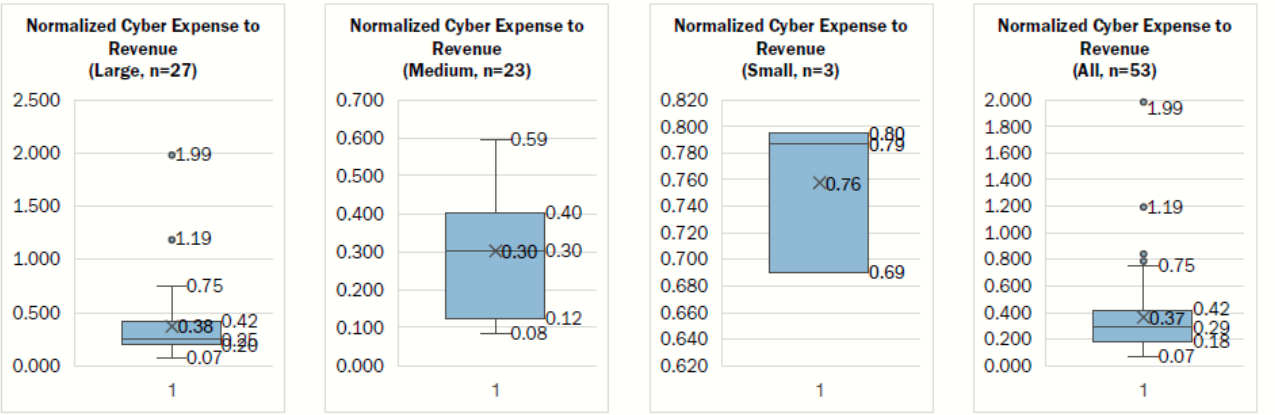
Figure 7 Staffing Analysis of organizations by size



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.

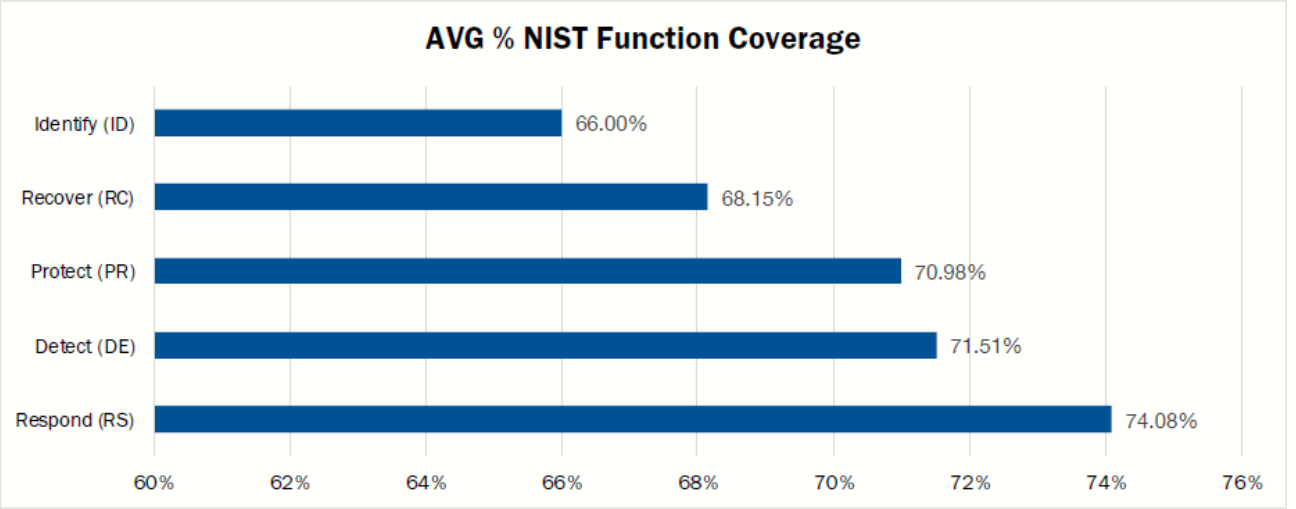
Figure 8 Normalized Cyber expense to revenue



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%)

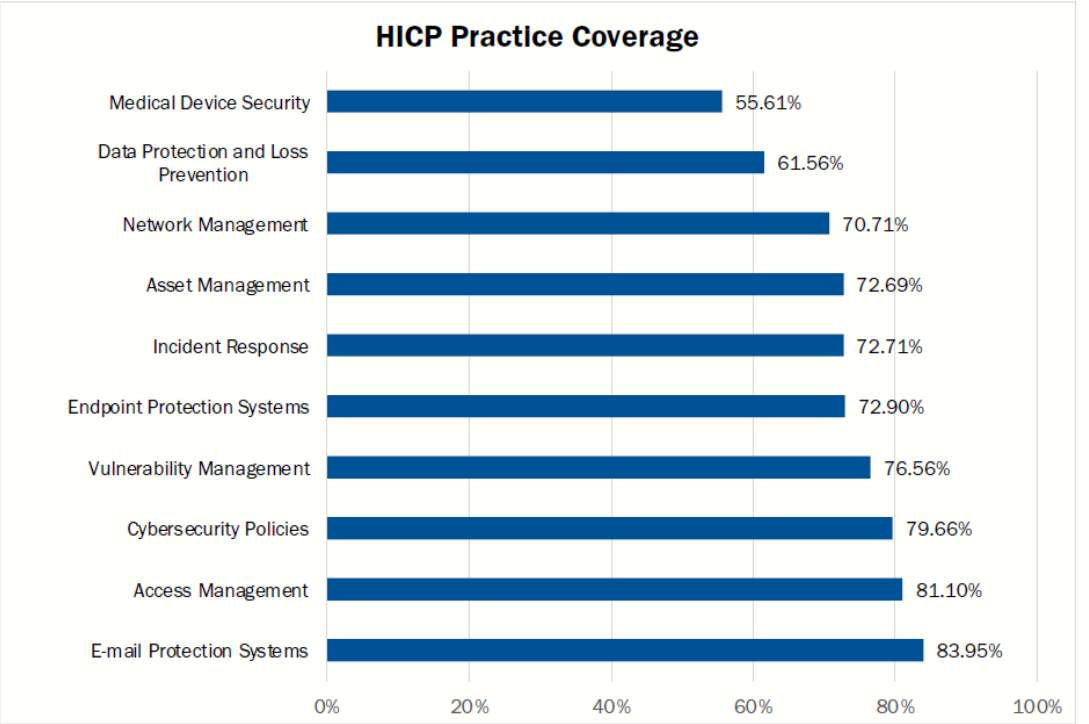
Figure 9 NIST Category level percent of coverage



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

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

HICP 2023 Overview

Cindi Bassford – Partner at Guidehouse and 405(d) Wave Lead

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

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.

HICP 2023 Edition

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.

Updates were made across the Main Document and each of the ten practices in the technical volumes. Below is a list of the MAJOR updates.

Main Document updates Overview:

- 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**.
- Email Phishing is now Social Engineering

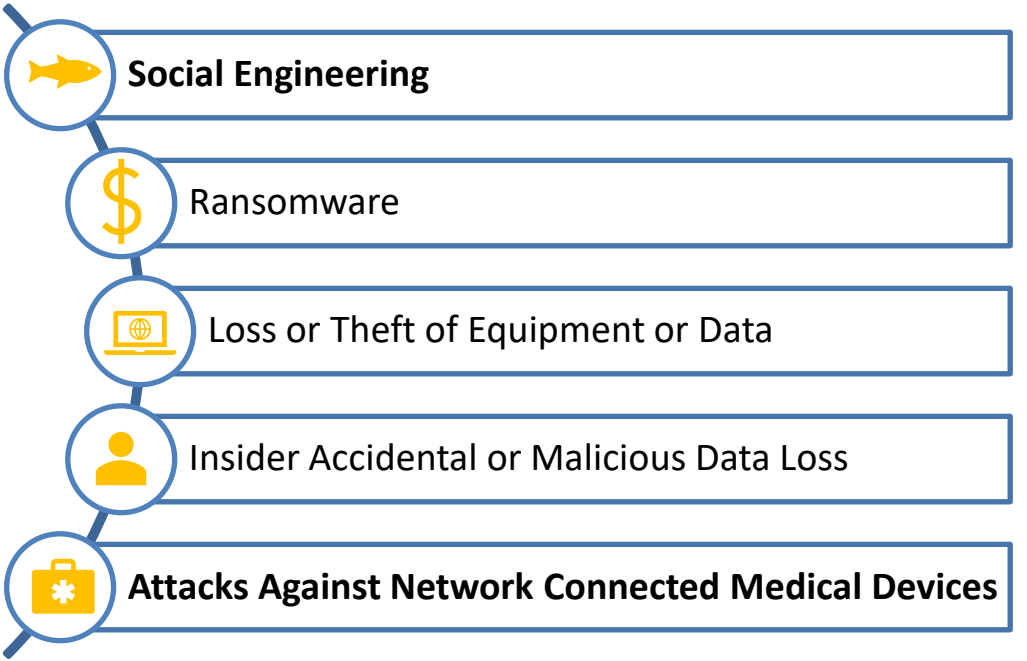
Top Ten Practices Updates:

- Cybersecurity Practice #9 on Network Connected Medical Devices has been fully updated
- Cyber Practice #10 is now Cybersecurity Oversight and Governances

Additional NEW sub-practices have been included:

- Cyber insurance
- Cybersecurity Risk Assessment and Management
- Attack Simulations
- Medical Devices (Major Updates)

Top 5 Threats



Top 10 Practices

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset management
6. Network Management
7. **Vulnerability Management**
8. **Incident Response**
9. **Medical Device Security**
10. **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

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

Cybersecurity Practice #9 Network Connected Medical Devices

- 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.

Cybersecurity Practice #10 Cybersecurity Oversight and Governance

A new executive summary was added to this practice in **Technical Volume 1 AND 2** and the section scope and introduction completely revised to focus on alignment with the resources, capability and needs of the small (tech volume 1) and medium/large (Tech Volume 2) healthcare organizations.

Tech Volume 1
Sub-Practices
10.S.A Policies
10.S.B. Cybersecurity Risk Assessment and Management
10.S.C. Security Awareness and Training
10.S.D. Cyber Insurance

405(d) Resources
Prescription Poster: Cybersecurity Policies

Tech Volume 2
Medium Sub-Practices
10.M.A Policies
10.M.B Cybersecurity Risk Assessment and Management
10.M.C Security Awareness and Training

Large Sub-Practices
10.L.A Cyber Insurance
405(d) Resources
Prescription Poster: Cybersecurity Policies

Cybersecurity Practice #10 Cybersecurity Oversight and Governance

Sub-practice A: Policies

- Revised to align taxonomy and scope for applicability to a small/medium-large healthcare organizations.

Sub-practice B: Cybersecurity Risk Assessment and Management

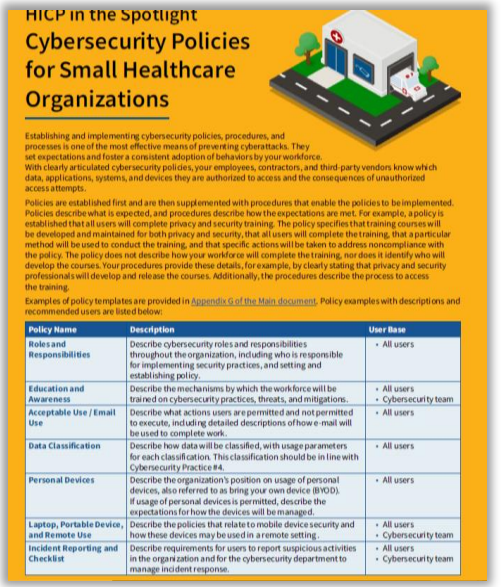
- Significant revision to scope and discussion to encompass thorough exploration of the role of the risk assessment in managing the security of information technology.

Sub-practice C: Security Awareness and Training

- Complete revision with newly added content which includes security policy training.

Sub-practice D: Cyber Insurance

- Added section to discuss the importance of cyber insurance and guidance for procuring insurance



HICP in the Spotlight

Cybersecurity Policies for Small Healthcare Organizations

Establishing and implementing cybersecurity policies, procedures, and processes is one of the most effective means of preventing cyberattacks. They set expectations and foster a consistent adoption of behaviors by your workforce. With clearly articulated cybersecurity policies, your employees, contractors, and third-party vendors know which data, applications, systems, and devices they are authorized to access and the consequences of unauthorized access attempts.

Policies are established first and are then supplemented with procedures that enable the policies to be implemented. Policies describe what is expected, and procedures describe how the expectations are met. For example, a policy is established that all users will complete privacy and security training. The policy specifies that training courses will be developed and maintained for both privacy and security, that all users will complete the training, that a particular method will be used to conduct the training, and that specific actions will be taken to address noncompliance with the policy. The policy does not describe how your workforce will complete the training, nor does it identify who will develop the courses. Your procedures provide these details, for example, by clearly stating that privacy and security professionals will develop and release the courses. Additionally, the procedures describe the process to access the training.

Examples of policy templates are provided in Appendix G of the Main document. Policy examples with descriptions and recommended users are listed below:

Policy Name	Description	User Base
Roles and Responsibilities	Describe cybersecurity roles and responsibilities throughout the organization, including who is responsible for implementing security practices, and setting and establishing policy.	• All users
Education and Awareness	Describe the mechanisms by which the workforce will be trained on cybersecurity practices, threats, and mitigations.	• All users • Cybersecurity team
Acceptable Use / Email Use	Describe what actions users are permitted and not permitted to execute, including detailed descriptions of how e-mail will be used to complete work.	• All users
Data Classification	Describe how data will be classified, with usage parameters for each classification. This classification should be in line with Cybersecurity Practice #4.	• All users
Personal Devices	Describe the organization's position on usage of personal devices, also referred to as bring your own device (BYOD). If usage of personal devices is permitted, describe the expectations for how the devices will be managed.	• All users
Laptop, Portable Device, and Remote Use	Describe the policies that relate to mobile device security and how these devices may be used in a remote setting.	• All users • Cybersecurity team
Incident Reporting and Checklist	Describe requirements for users to report suspicious activities in the organization and for the cybersecurity department to manage incident response.	• All users • Cybersecurity team

Sub Practice: Attack Simulations (7.L.C)

The last time you want to find out about a vulnerability is during a cyber-attack. Attack simulations, also known as threat emulation exercises, can help you expose your known and unknown vulnerabilities and stress-tests your organization's cybersecurity. The purpose of a threat emulation exercise is to closely mimic the tactics, techniques, and procedures (TTPs) of real-world adversaries and determine how they might be leveraged against your organization.

Key Information in New Sub-Practice:

When it comes to building a threat emulation exercise there are three phases that all the activities fall under: **Get in, Stay in** and **Act.** The goals of these phases include activities such as:

- Acquiring elevated access to a domain controller or other critical servers.
- Accessing a client data repository, intellectual property, and/or application data.
- Creating a new cloud instance in the client's on-premises or cloud infrastructure.
- Gaining access to and leaving a physical note in a datacenter or other restricted area.
- Posting a comment into production source code.
- Obtaining physical access to data or devices and accessing the ability to remove the data/device.
- Keeping a low profile (i.e., not generating alerts that will raise suspicions or having the attack infrastructure get burned).

Information on: Cyber Range Training Courses, Cyber Range Challenges, and the Observe the Attack Series

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

Sub Practice: Cybersecurity Risk Assessment and Management (10.S.B and 10.M.B)

A cybersecurity risk assessment (RA) helps your organization measure the likelihood of known threats and vulnerabilities compromising data and information assets. This allows for identifying any gaps in cybersecurity safeguards and controls that are in place and determines if it reduces the risk to an acceptable level. An RA is an important step in both protecting your workers and your organization and complying with the HIPAA Security Rule. It helps you focus on the risks that really matter and prepare for what could go wrong. An RA can help your organization understand potential risks and prioritize the risks that need to be fully addressed. This should not be done in a silo but should be an organizational collaborative effort.

Key Information in New Sub-Practice:

An effective RA should:

- Document the threats and vulnerabilities to the information system.
- Evaluate the potential impact and the effectiveness of existing safeguards and controls.
- Determine the likelihood of occurrence that the threat or vulnerability could compromise data or information system assets.

It is important to remember that performing an RA is an ongoing process, in which an organization:

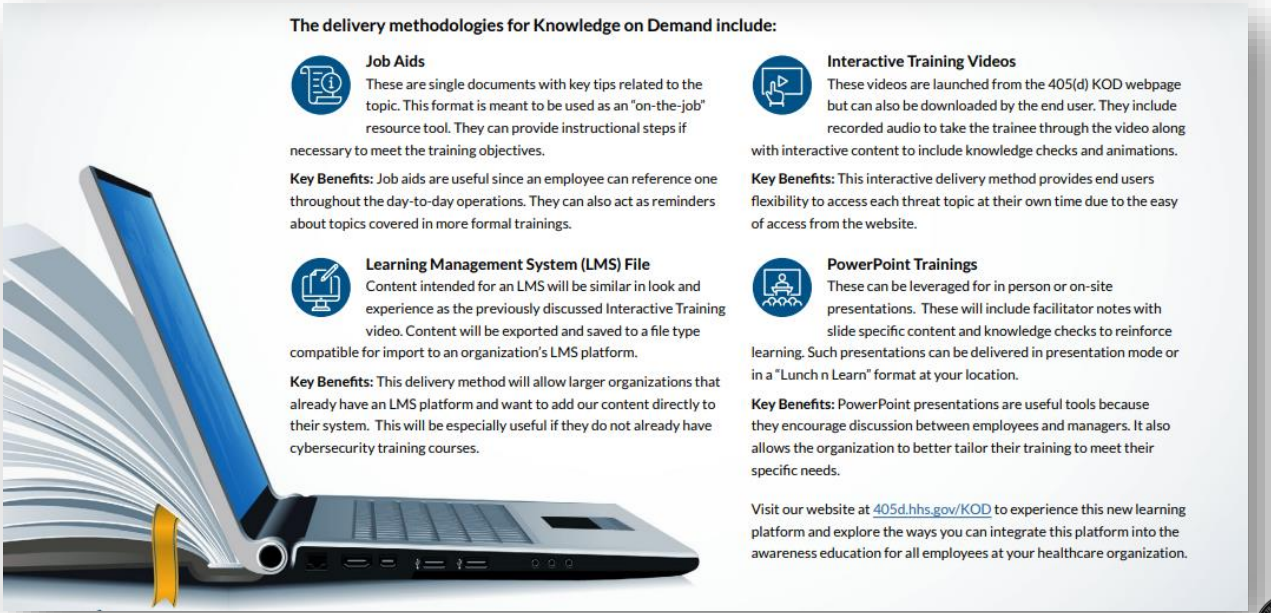
- Regularly reviews its records to track access to PHI and detect security incidents.
- Periodically evaluates the effectiveness of current security measures.
- Regularly evaluates potential threats and vulnerabilities to PHI.

Information on: RA Considerations for cybersecurity and privacy leaders

Knowledge on Demand

405(d) Knowledge on Demand

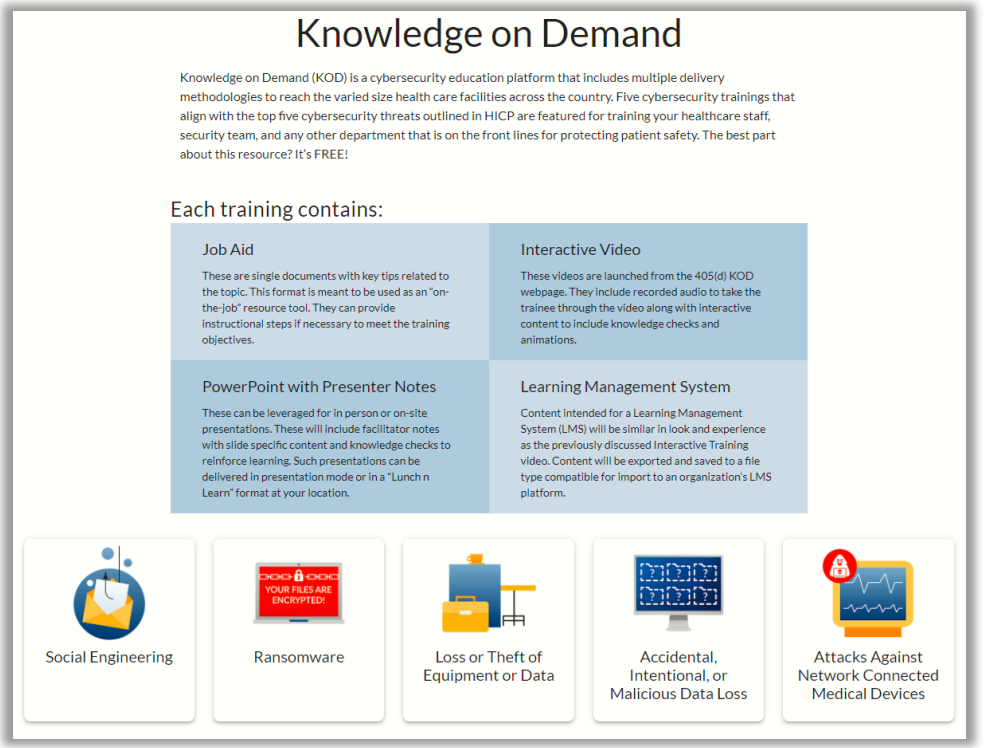
The 405(d) Program, in collaboration with industry, is launching a new cybersecurity training platform on its website—405d.hhs.gov—titled Knowledge on Demand. This new cybersecurity education platform will include multiple delivery methodologies to reach the varied size health care facilities across the country. The platform will include five cybersecurity awareness trainings that align with the top five cybersecurity threats outlined in the landmark 405(d) publication: The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) and its accompanying two volumes.



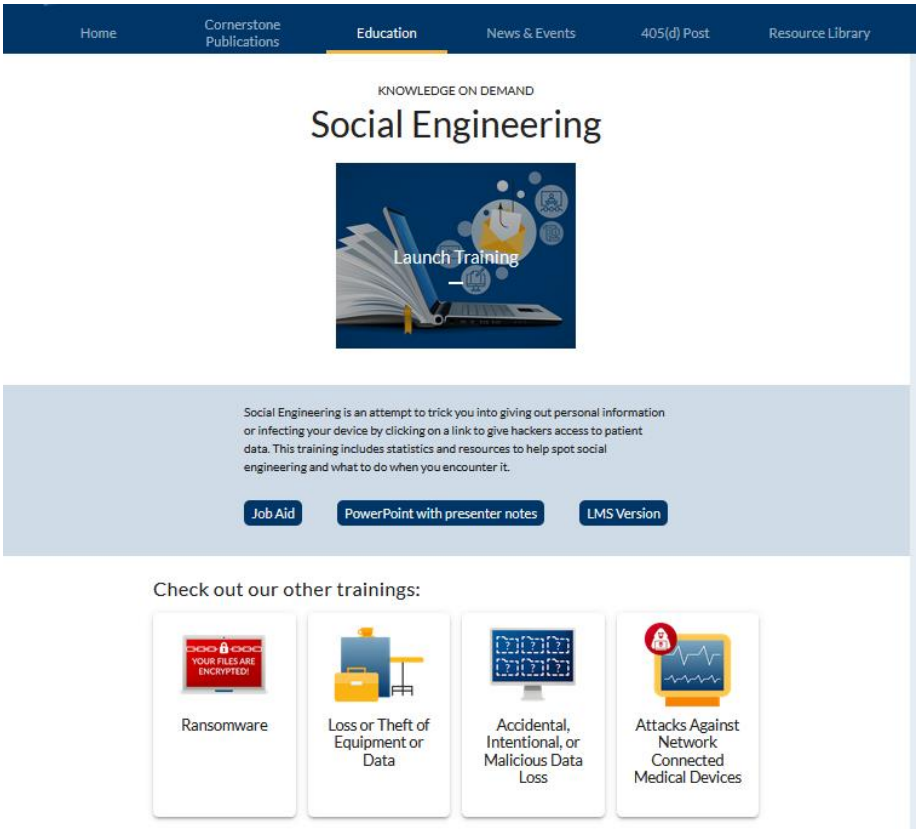
Knowledge on Demand Landing Page

The KOD landing page provides users the ability to navigate each cyber threat training with ease!

- Each Threat Training can be accessed from this page
- Provides an overview of different delivery methods



Training Landing Page



Each threat has a landing page that will look like this. The different delivery methods are explained and listed.

The training video can be launched directly from this page.

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