HHS 405(d)
Aligning Health Care Industry Security Approaches

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

405(d) Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Christopher Gibson, OSCP, GXPN
Information Security Manager, IU Health

Indiana University Health

1

The Current State of Healthcare Cybersecurity

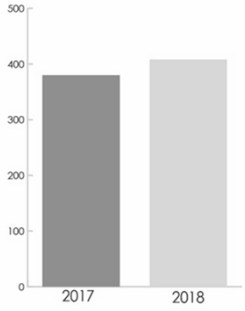
Indiana University Health

2

2

Cybersecurity Impacts to the Healthcare Sector

According to a study from IBM Security and the Ponemon Institute, the cost of a data breach for health care organizations rose from



$380 per breached record in 2017 to **$408** per record in 2018

4 in 5

U.S. physicians have experienced some form of a cybersecurity attack

$6.2 billion

lost by U.S. Health Care System in 2016 due to data breaches

3

3

405(d)- Aligning Healthcare Industry Security Approaches

Task Group Summary

Indiana University Health

4

4

Overview

- What is the 405(d) initiative?
  - An industry-led process to develop consensus-based guidelines, practices, and methodologies to strengthen the HPH-sector's cybersecurity posture against cyber threats.
- Who is participating
  - The 405(d) Task Group is convened by HHS and comprised of over 150 information security officers, medical professionals, privacy experts, and industry leaders.
- Our Mandate
  - To strengthen the cybersecurity posture of the HPH Sector, Congress mandated the effort in the Cybersecurity Act of 2015 (CSA), Section 405(d).

5

5

Origins of the 405(d) Task Group

- 2017 HHS convened the 405(d) Task Group leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership.
- Qualitative research to establish the level of the health sector's awareness and prioritization of cybersecurity
- Series of one-on-one interviews with practitioners and practice administrators from the Northwest, Northeast, and Southeast
- 7 Focus Groups— 4 in-person, 3 virtual
- Qualitative Research with medical professionals, HPH, CIOs/CISOs, etc

6

6

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

Publication Development Process

Indiana University Health

Stages of Publication

- Pretest
  - National pretesting sessions were both in-person and virtual, and feedback was gathered with focus groups of 9-15 participants via roundtable discussion. A total of 123 took part in the pretesting efforts
  - Feedback was used to make final modifications to the publication

Stages of Publication

- Release
  - The four-volume publication includes a main document, two technical volumes, and a resources and templates volume.
  - It seeks to aid Healthcare and Public Health organizations to develop meaningful cybersecurity objectives and outcomes.
  - It does this by raising awareness, providing vetted cybersecurity practices, and helping to move towards consistency in mitigating the current, most pertinent cybersecurity threats to the sector.

Going Forward

- Become the leading collaboration center for developing healthcare cybersecurity focused resources
- Continue to build upon the HICP publication
- Develop new cybersecurity resources
- Sec. 502 of the Senate Lower Health Care Costs Act of 2019 specifically calls out this work as an example of “recognized security practices” that may help to mitigate fines and/or cause a favorable early end to an audit if a covered entity or business associate has a data breach.

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

Document Organization and Content

5 Threats and 10 Practices

Indiana University Health

11

11

Document Construction (1/2)

- 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.

12

12

Document Construction (2/2)

- *Technical Volume 2* discusses these ten cybersecurity practices for medium and large healthcare organizations.
- *Resources and Templates* provides mappings to the NIST Cybersecurity Framework, a HICP assessment process, templates and acknowledgements for its development.

13

13

5 Current Threats

- Email Phishing Attacks
- Ransomware Attacks
- Loss or Theft of Equipment or Data
- Internal, Accidental, or Intentional Data Loss
- Attacks Against Connected Medical Devices that May Affect Patient Safety

14

14

10 Practices (1/2)

- Email Protection Systems
- Endpoint Protection Systems
- Access Management
- Data Protection and Loss Prevention
- Asset Management

15

10 Practices (2/2)

- Network Management
- Vulnerability Management
- Incident Response
- Medical Device Security
- Cybersecurity Policies

16

What HICP Is…

- A call to action to manage real cyber threats
- Written for multiple audiences (clinicians, executives, and technical)
- Designed to account for organizational size and complexity (small, medium and large)
- A reference to "get you started" while linking to other existing knowledge
- Aligned to the NIST Cybersecurity Framework
- Voluntary

17

17

What HICP Is <u>Not</u>…

- A new regulation
- An expectation of minimum baseline practices to be implemented in all organizations
- The definition of "reasonable security measures" in the legal system
- An exhaustive evaluation of all methods and manners to manage the threats identified
- Your guide to HIPAA, GDPR, State Law, PCI, or any other compliance framework

18

18

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

How to Use the Practices

Indiana University Health

19

19

Practices and Sub-Practices

Cybersecurity Practice 2: Endpoint Protection Systems		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	2.M.A	Basic Endpoint Protection Controls
Large Sub-Practices	2.L.A	Automate the Provisioning of Endpoints
	2.L.B	Mobile Device Management
	2.L.C	Host Based Intrusion Detection/Prevention Systems
	2.L.D	Endpoint Detection Response
	2.L.E	Application Whitelisting
	2.L.F	Micro-segmentation/virtualization strategies
Key Mitigated Risks	• Ransomware Attacks • Theft or Loss of Equipment or Data	

- 10 practices, 89 sub-practices
- Each practice has a corresponding set of sub-practices broken out by organization size
- Includes suggested metrics for measuring effectiveness
- Some practices will mitigate more that one threat

20

20

Example Metrics

- Percentage of endpoints encrypted based on a full fleet of known assets, measured weekly.
- Percentage of endpoints that meet all patch requirements each month.
- Percentage of endpoints with active threats each week.
- Percentage of endpoints that run non hardened images each month.
- Percentage of local user accounts with administrative access each week.

21

21

Prioritize Your Threats

- Implementing all the practices and sub-practices could be daunting, even for a large sized organization
- Recommendation—Review the threats and implement the most impactful practices first
  - A toolkit is being developed to help with this process

22

22

Prioritize Your Threats (Example)

Factor		
Select your organizations size		Medium
Prioritize the threats (5 being highest priority, 1 being lowest priority)		
A	Email Phishing Attack	1
B	Ransomware Attack	4
C	Loss or Theft of Equipment or Data	5
D	Insider, Accidental or Intentional Data Loss	3
E	Attacks Against Connected Medical Devices that may affect Patient Safety	2

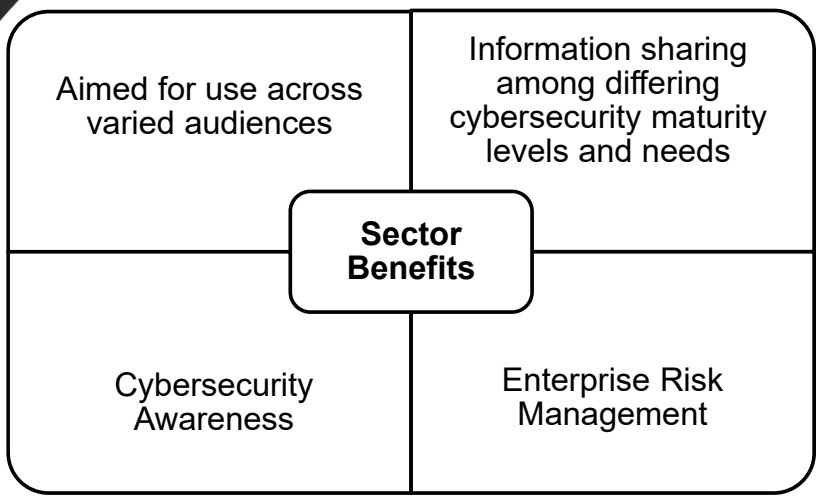
CP #	Cybersecurity Practices	Priority Rank Based on Threat Model Inputs
8	Incident Response	28
3	Access Management	23
2	Endpoint Protection Systems	23
5	Asset Management	20
6	Network Management	16
7	Vulnerability Management	16
10	Cybersecurity Policies	15
1	Email Protection Systems	13
9	Medical Device Security	11
4	Data Protection and Loss Prevention	11

23

23

Healthcare and Public Health (HPH) Sector Coordinating Council Benefits

https://healthsectorcouncil.org/



This joint HHS and industry-led initiative aims to increase awareness and foster consistency with cybersecurity practices for a wide range of stakeholders

24

24

What's Next for 405(d)?

- Over the course of the next year the 405(d) Team plans to continue to develop awareness of the HICP publication and engage with stakeholders by:
  - Building additional supporting materials/resources to spotlight the HICP publication and related content
  - Develop means to collect feedback and implementation of HICP practices and methods
  - Hosting additional outreach engagements

25

Questions?

26

Thank You!

- 405(d) contact info:
  - Visit us at: www.phe.gov/405d
  - Email us at: CISA405d@hhs.gov
- My contact info:
  - Christopher.Gibson@IUHealth.org
  - https://www.linkedin.com/in/christopher-gibson-oscp/