LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

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

Five Threats Series:
Threat 1 - E-mail Phishing Attack

March 2019

In Partnership With

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

Agenda

Time	Topic	Speaker
5 Minutes	Opening Remarks & Introductions	405(d) Team
5 Minutes	CSA Section 405(d)'s Mandate, Purpose, and Desired Goals	Toney Rogers
5 Minutes	HICP Overview	Tony Rogers
10 Minutes	Using HICP and Supporting Resources	Tony Rogers
40 Minutes	Threat 1 – Email Phishing Attack and Mitigating Practices	Stephen Dunkle/Tony Rogers
5 Minutes	Looking Forward	Tony Rogers
5 Minutes	Upcoming Five Threats	405(d) Team
15 Minutes	Questions	

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

CSA Section 405(d)'s Mandate, Purpose, and Desired Goals

Cybersecurity Act of 2015 (CSA): Legislative Basis

CSA Section 405

Improving Cybersecurity in the Health Care Industry

- Section 405(b): Health care industry preparedness report
- Section 405(c): Health Care Industry Cybersecurity Task Force
- **Section 405(d): Aligning Health Care Industry Security Approaches**

Industry-Led Activity to Improve Cybersecurity in the Healthcare and Public Health (HPH) Sector

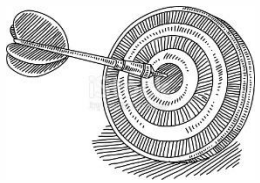
WHAT IS THE 405(d) EFFORT?

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.

HOW WILL 405(d) ADDRESS HPH CYBERSECURITY NEEDS?



With a targeted set of applicable & voluntary practices that seeks to cost-effectively reduce the cybersecurity risks of healthcare organizations.

WHY IS HHS CONVENING THIS EFFORT?

To strengthen the cybersecurity posture of the HPH Sector, Congress mandated the effort in the Cybersecurity Act of 2015 (CSA), Section 405(d).

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

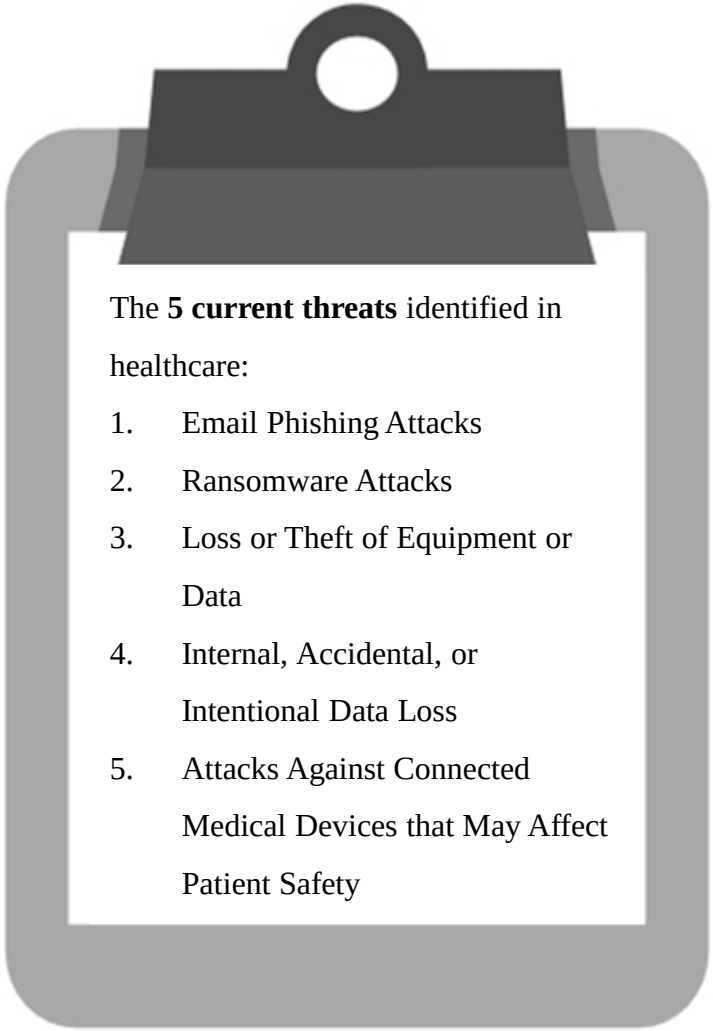
OFFICE OF THE CHIEF INFORMATION OFFICER

HICP Publication Overview

Document - Content Overview (1/2)

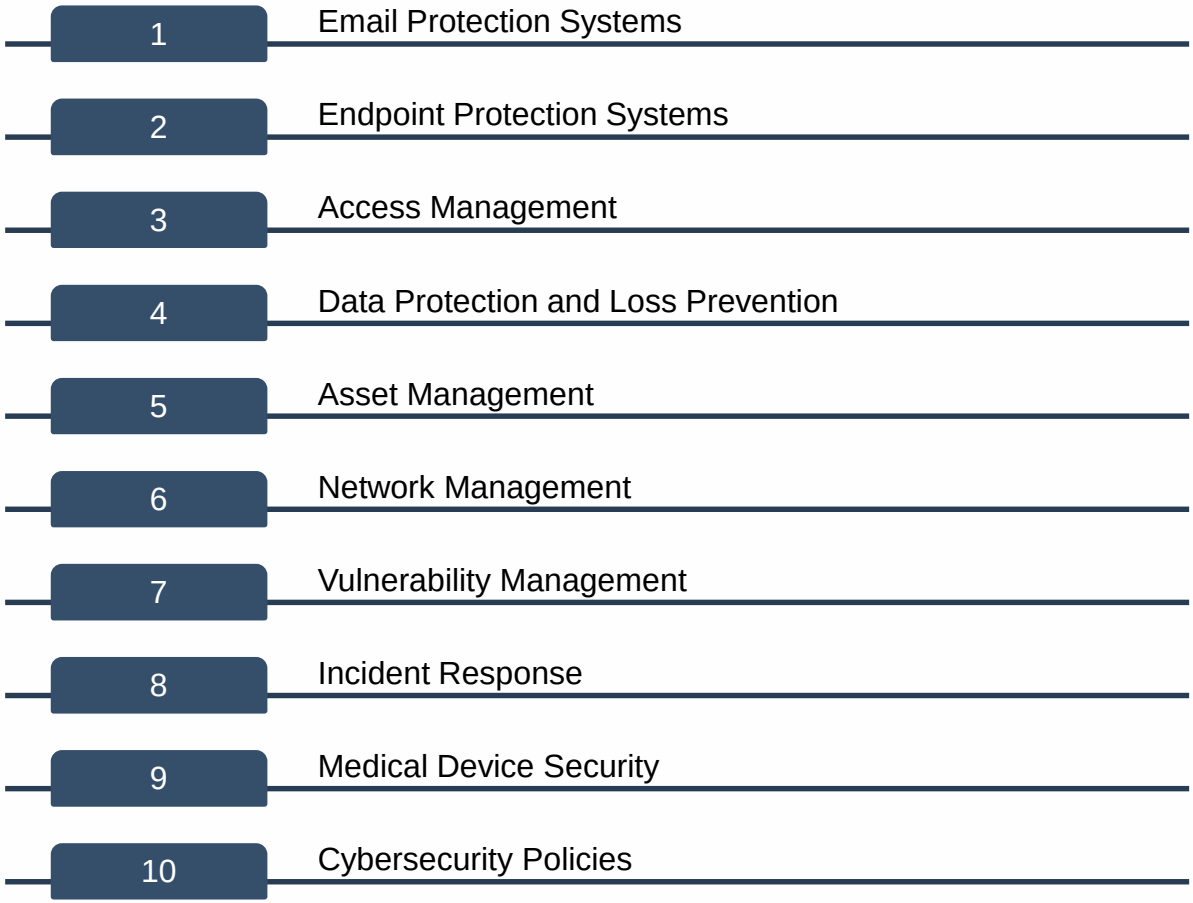
After significant analysis of the current cybersecurity issues facing the HPH Sector, the Task Group agreed on the development of three documents—a main document and two technical volumes, and a robust appendix of resources and templates:

- 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.
- *Resources and Templates* provides mappings to the NIST Cybersecurity Framework, a HICP assessment process, templates and acknowledgements for its development.



Document - Content Overview (2/2)

The document identifies **ten (10) practices**, which are tailored to small, medium, and large organizations and discussed in further detail in the technical volumes:



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Using HICP and Supporting Resources

Introduction and Executive Summary

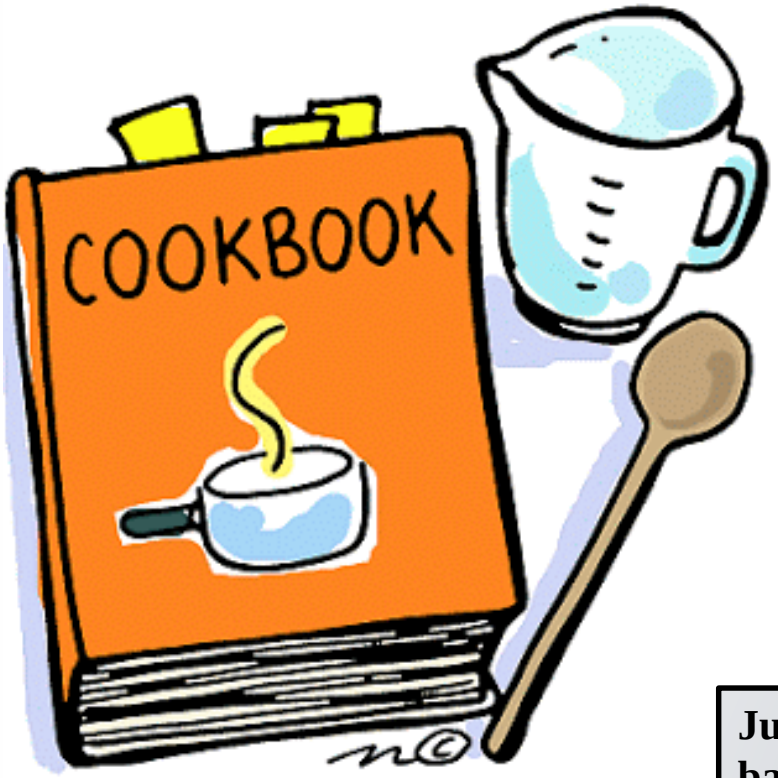
HICP is…

- 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

HICP is **not**…

- 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
  - You might have other practices in place that are more effective than what was outlined!
- Your guide to HIPAA, GDPR, State Law, PCI, or any other compliance framework

HICP is a Cookbook!



So you want a recipe for managing phishing?

1. 5 oz of Basic E-Mail Protection Controls (1.M.A)
2. A dash of Multi-Factor Authentication (1.M.B)
3. 2 cups of Workforce Education (1.M.D)
4. 1 cup of Incident Response plays (8.M.B)
5. 1 tsp of Digital Signatures for authenticity (1.L.B)
6. Advanced and Next General Tooling to taste (1.L.A)

Preheat your email system with some basic email protection controls necessary to build the foundation of your dish. Mix in MFA for remote access, in order to protect against potential credential theft.

Let sit for several hours, while providing education to your workforce on the new system, and how to report phishing attacks. While doing so, ensure to provide education on how digital signatures demonstrating authenticity of the sender. When finished baking, sprinkle with additional tooling to provide next level protection.

Just like with any cookbook the recipes provide the basic ingredients to making a meal. It does not:

- **Instruct you how to cook**
- **Instruct you on what recipes to use**
- **Limit your ability for substitutions**

The skill of the cook is what makes the dish!

How to Evaluate Your Organization's Size

HICP is designed to assist organizations of various sizes implement resources and practices that are tailored and cost effective to their needs.

- How "large and complex an organization you might be relates to several factors:
  - Health Information Exchanges
  - IT Capability
  - Cybersecurity Investment
  - Size (provider)
  - Size (acute/post-acute)
  - Size (hospital)
  - Complexity
- Determining where you fit is your decision

[Main Document](), p. 11

Medium

Best Fit		Small	Medium	Large
Common Attributes	Health information exchange partners	One or two partners	Several exchange partners	Significant number of partners or partners with less rigorous standards or requirements Global data exchange
	IT capability	No dedicated IT professionals on staff, IT may be outsourced on a break/fix or project-by project-basis	Dedicated IT resources on staff No or limited dedicated security resources on staff	Dedicated IT resources with dedicated budget CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Nonexistent or limited funding	Funding allocated for specific initiatives Potentially limited future funding allocations Cybersecurity and IT budgets are blended	Dedicated budget with strategic roadmap specific to cybersecurity
Provider Attributes	Size (provider)	1–10 physicians	11–50 physicians	Over 50 physicians
	Size (acute / post-acute)	1–25 providers	26–500 providers	Over 500 providers
	Size (hospital)[15]	1–50 beds	51–299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated delivery networks Participate in accountable care organization or clinically integrated network
Other Org Types			Practice Management Organization Managed Service Organization Smaller device manufacturers Smaller pharmaceutical companies Smaller payor organizations	Health Plan Large Device Manufacturer Large pharmaceutical organization

Table 1. Selecting the "Best Fit" For Your Organization

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

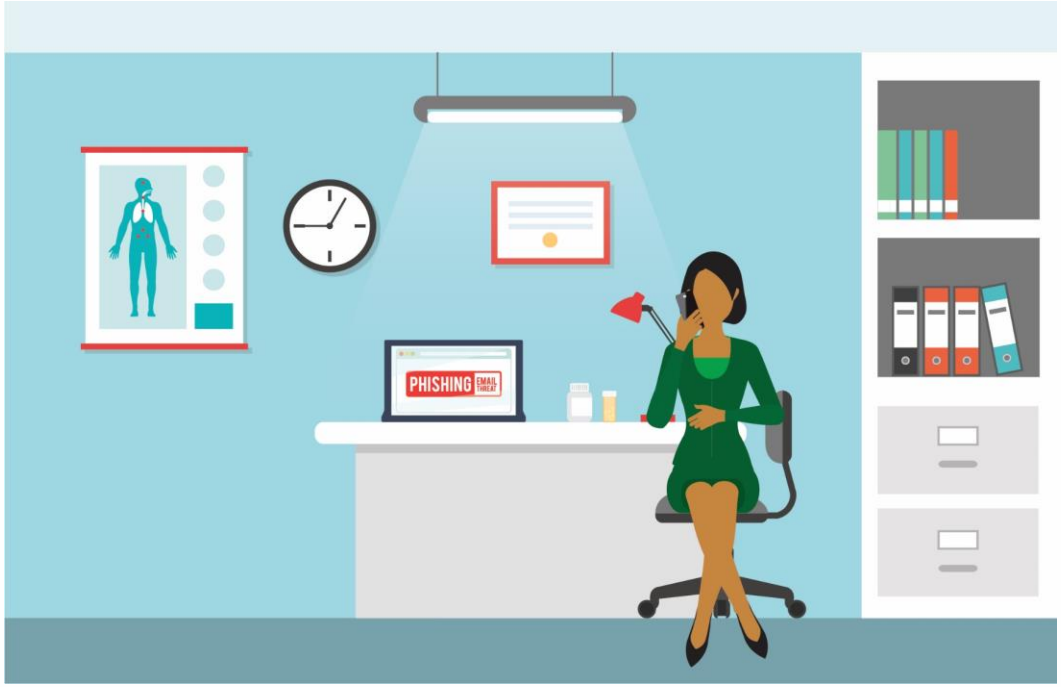
OFFICE OF THE CHIEF INFORMATION OFFICER

Threat 1 – E-Mail Phishing Attack & Mitigating Practices

What is E-Mail Phishing?

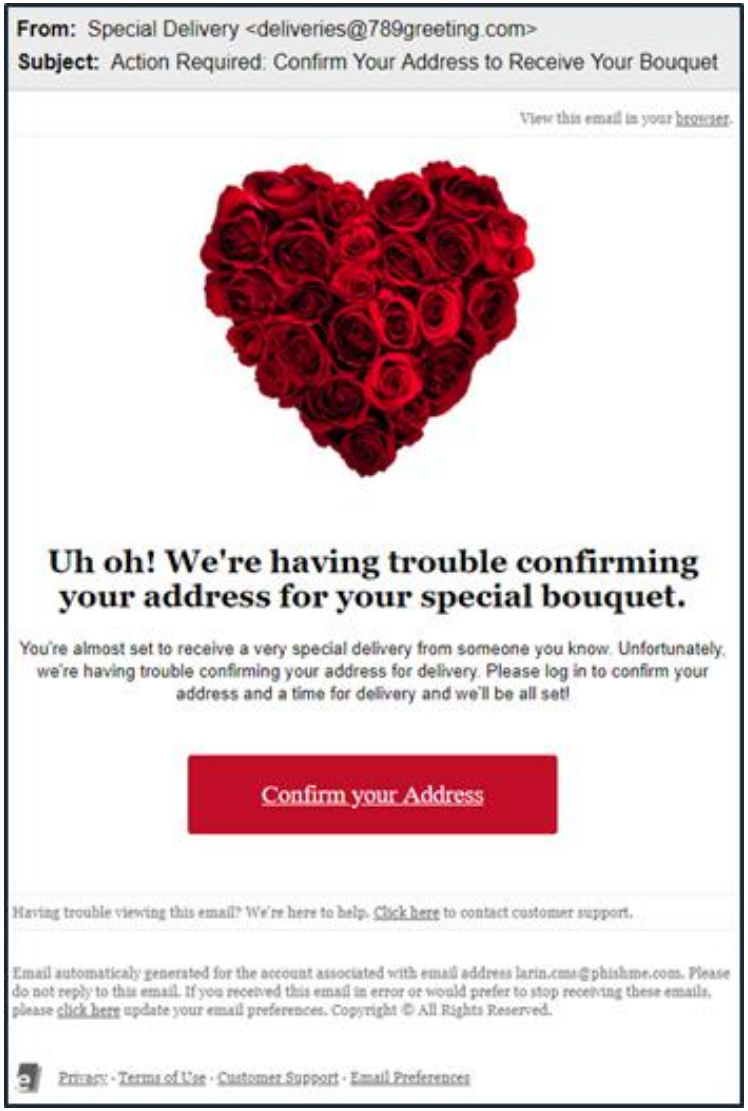
E-mail phishing is an attempt to trick you, a colleague, or someone else in the workplace into giving out information using e-mail. An inbound phishing e-mail includes an active link or file (often a picture or graphic). The e-mail appears to come from a legitimate source, such as a friend, coworker, manager, company, or even the user's own e-mail address.

Clicking to open the link or file takes the user to a website that may solicit sensitive information or proactively infect the computer. Accessing the link or file may result in malicious software being downloaded or access being provided to information stored on your computer or other computers within your network.



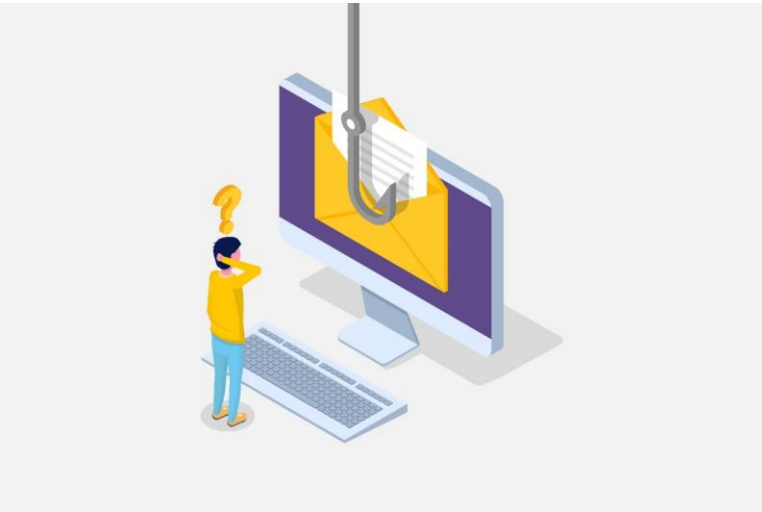
E-Mail Phishing Scenario

- **Real-World Scenario:** Your employees receive a fraudulent e-mail from a cyber-attacker disguised as an IT support person from your patient billing company. The e-mail instructs your employees to click on a link to change their billing software passwords. An employee who clicks the link is directed to a fake login page, which collects that employee's login credentials and transmits this information to the attackers. The attacker then uses the employee's login credentials to access your organization's financial and patient data.
- **Impact**: A pediatrician learns that an attacker stole patient data using a phishing attack and used it in an identity theft crime.



E-Mail Phishing Remains a Challenge

According to the 2017 Verizon Data Breach Report, "Weak or stolen passwords were responsible for 80% of the hacking related breaches". The report further identifies phishing attacks (a type of hacking attack) as the most common first point of unauthorized entry into an organization. After monitoring 1,400 customers and 40 million simulated phishing campaigns, the *PhishMe 2017 Enterprise Resiliency and Defense Report* concluded that the average susceptibility of users within an organization falling prey to a phishing attack is 10.8 percent.



Tin Zaw, "2017 Verizon Data Breach Investigations Report (DBIR) from the Perspective of Exterior Security Perimeter," Verizon Digital Media Service, last modified July 26, 2017, https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/.
Ian Murphy, "How Susceptible Are You to Enterprise Phishing?" Enterprise Times, last modified December 1, 2017, https://www.enterprisetimes.co.uk/2017/12/01/susceptible-enterprise-phishing/.

Common E-Mail Phishing Methods

The two most common phishing methods are **credential theft** (leveraging e-mail to conduct a credential harvesting attack on the organization) and **malware dropper attacks** (e-mail delivery of malware that can compromise endpoints).

An organization's cybersecurity practices must address these two attack vectors. Because both attack types leverage e-mail, e-mail systems should be the focus for additional security controls.

E-Mail Phishing Mitigating Practices - Small Organizations

Technical Volume 1 provides health care cybersecurity practices for small health care organizations. For the purpose of this volume, *small organizations* generally do not have dedicated information technology (IT) and security staff dedicated to implementing cybersecurity practices due to limited resources.

E-Mail Phishing Mitigating Practices in *Technical Volume 1* can be found in **Cybersecurity Practice #1** and **Cybersecurity Practice #8** along with their corresponding sub practices.

Cybersecurity Practice #1: E-mail Protection Systems

- E-mail system configuration
- Education
- Phishing simulations

Cybersecurity Practice #8 Incident Response

- ISAC/ISAO Participation

E-Mail Phishing Mitigating Practices - Small Organizations

For each Sub-Practice, *Technical Volume 1* provides:

- Considerations your organization can take to enhance the security posture
- Implementing education and awareness activities that can assist your employees and partners in protecting your organization against phishing attacks

Here are just a few examples of what can be found within the sub-practices of **Cybersecurity Practice #1.**

E-mail system configuration

Avoid "free" or "consumer" e-mail systems for your business; such systems are not approved to store, process, or transmit PHI. We recommend contracting with a service provider that caters to the health care or public health sector.

Education

- Establish and maintain a training program for your workforce that includes a section on phishing attacks.

Phishing simulations

- Implement regular (e.g., monthly or quarterly) anti-phishing campaigns with real-time training for your staff. Many third parties provide low-cost, cloud-based phishing simulation tools to train and test your workforce. Such tools often include pre-configured training that is easy to distribute and that your workforce can complete independently.

E-Mail Phishing Mitigating Practices - Small Organizations

Practice	Sub-Practice	To Consider	NIST Reference
E-mail Protection Systems	(1.S.A): E-mail System Configuration	• Tag external e-mails to make them recognizable to staff • Implement multifactor authentication (MFA)	NIST FRAMEWORK REF: PR.DS-2, PR.IP-1, PR.AC-7
Email Protection Systems	(1.S.B): Education	• Be suspicious of e-mails from unknown senders, e-mails that request sensitive information such as PHI or personal information, or e-mails that include a call to action that stresses urgency or Importance • Train staff to recognize suspicious e-mails and to know where to forward them • Never open e-mail attachments from unknown enders	NIST FRAMEWORK REF: PR.AT-1
Email Protection Systems	(1.S.C): Phishing Simulations	• Implement proven and tested response procedures when employees click on phishing e-mails	NIST FRAMEWKORK REF: PR.AT
Incident Response	(8.S.B): ISAC/ISAO Participation	• Establish cyber threat information sharing with other health care organizations	NIST: DETECT - ID.RA-2

E-Mail Phishing Mitigating Practices - Medium & Large Organizations

Technical Volume 2 provides health care cybersecurity practices for Medium/Large health care organizations. For the purpose of this volume,

- Medium-sized health care organizations generally employ hundreds of personnel, maintain between hundreds and a few thousand information technology (IT) assets, and may be primary partners with and liaisons between small and large health care organizations.
- Large health care organizations perform a range of different functions. These organizations may be integrated with other health care delivery organizations, academic medical centers, insurers that provide health care coverage, clearinghouses, pharmaceuticals, or medical device manufacturers. In most cases, large organizations employ thousands of employees, maintain tens of thousands to hundreds of thousands of IT assets, and have intricate and complex digital ecosystems.

E-Mail Phishing Mitigating Practices - Medium & Large Organizations

E-Mail Phishing Mitigating Practices in *Technical Volume 2* can be found in **Cybersecurity Practice #1, Cybersecurity #3, and Cybersecurity Practice #8** along with their corresponding sub practices. Medium sub-practices apply to both medium-sized and large organizations. Large sub-practices apply primarily to large organizations, but could also benefit any other organization that interested in adopting them.

Cybersecurity Practice #1: E-mail Protection Systems

- Basic E-mail Protection Controls
- Multifactor Authentication for Email Remote Access
- E-mail Encryption
- Workforce Education
- Advanced and Next-Generation Tooling (Large)

Cybersecurity Practice #3: Access Management

- Multifactor Authentication for Remote Access

Cybersecurity Practice #8: Incident Response

- Security Operations Center
- Information Sharing and ISACs/ISAOs

E-Mail Phishing Mitigating Practices - Medium/Large Organizations

Here are just a few examples of what can be found within the sub-practices of **Cybersecurity Practice #1 & 8**

Basic E-mail Protection Controls

- E-mail encryption is an important security protection. Multiple encryption techniques exist, though the most common use third-party applications to conduct encryption, invoking them by tagging outbound messages in some form.

Multifactor Authentication for Remote Access

- Two-factor authentication, or multifactor authentication (MFA), is the process of verifying a user's identity using more than one credential. The most common method is to leverage a soft token in addition to a password.

Information Sharing and ISACs/ISAOs

- Sophisticated threat intelligence is realized through involvement with and participation in ISACs and ISAOs. ISACs and ISAOs tend to focus on a specific vertical (such as the Health Information Sharing and Analysis Center within the health care sector) or community (such as the Population Health ISAO).). In all cases, the primary function of these associations is to establish and maintain channels for sharing cyber intelligence. . "Population Health Information Sharing & Analysis Organization, " International ISAO Network, accessed March 10, 2018, http://www.isaonetwork.org/population-health/.

Advanced and Next-Generation Tooling (Large)

- Many sophisticated solutions exist to help combat the phishing and malware problem. These solutions are called *advanced threat protection services*. They use threat analytics and real-time response capabilities to provide protection against phishing attacks and malware.. Examples include URL Click Protection, Attachment Sandboxing, and Automatic Response

E-Mail Phishing Mitigating Practices for Medium/Large Organizations

Practice	Sub-Practice	To Consider	NIST Reference
Email Protection Systems	***(1.L.A): Advanced and Next-Generation Tooling***	• Implement advanced technologies for detecting and testing e-mail for malicious content or links	NIST FRAMEWKORK REF: PR.DS-2, DE.CM-5, DE.CM-7
Access Management	***(3.M.D): Multifactor Authentication for Remote Access***	• Implement multifactor authentication (MFA)	NIST FRAMEWKORK REF: PR.AC-3, PR.AC-7
Incident Response	***(8.M.A): Security Operations Center***	• Implement incident response plays to manage successful phishing attacks	NIST FRAMEWKORK REF: RS.RP
Incident Response	***(8.M.C): Information Sharing and ISACs/ISAOs***	• Establish cyber threat information sharing with other health care organizations	NIST FRAMEWKORK REF: ID.RA-2

E-Mail Phishing Mitigating Practices Metrics for Organizations

Specifically for Medium/Large Organizations **Technical Volume 2** contains a series of suggested metrics to measure the effectiveness of the cybersecurity practice. The metrics for each Cybersecurity Practice can be found directly following the Sub-Practices for Large Organizations. Here are a few examples of the metrics discussed for **Cybersecurity Practice #1:**

Malicious Phishing Attacks	Malicious URLs	Susceptible to Phishing	Malicious Websites
• Number of malicious phishing attacks prevented on a weekly basis. The goal is to ensure that systems are working. A reduction in attacks prevented indicates system misconfiguration. Sudden changes in the rate of phishing attacks should trigger operational checks of to ensure that systems are still operating as intended.	• Number of malicious URLs and e-mail attachments discovered and prevented on a weekly basis. The goal is to measure the effectiveness of advanced tools, like click protection or attachment protection.	• Percentage of users in the organization who are susceptible to phishing attacks based on results of internal phishing campaigns. This provides a benchmark to measure improvements to the workforce's level of awareness. The goal is to reduce the percentage as much as possible, realizing that it is nearly impossible to stop all users from opening phishing e-mails. A secondary goal is to correlate the percentage of susceptible users with the number of malicious websites visited or the number of malicious URLs opened.	Number of malicious websites visited on a weekly basis. The goal is to establish a baseline understanding, then strive for improved awareness through education activities that train employees to avoid malicious websites.

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Looking Forward

Looking Forward

CSA 405(d) aims to be the leading collaboration center of OCIO/OIS, in partnership with relevant HHS divisions, and the healthcare industry focused on the development of resources that help align health care cybersecurity practices

- **Immediate Next Steps**
  - 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

Questions

Thank you for Joining Us

Visit us at: www.405d.hhs.gov

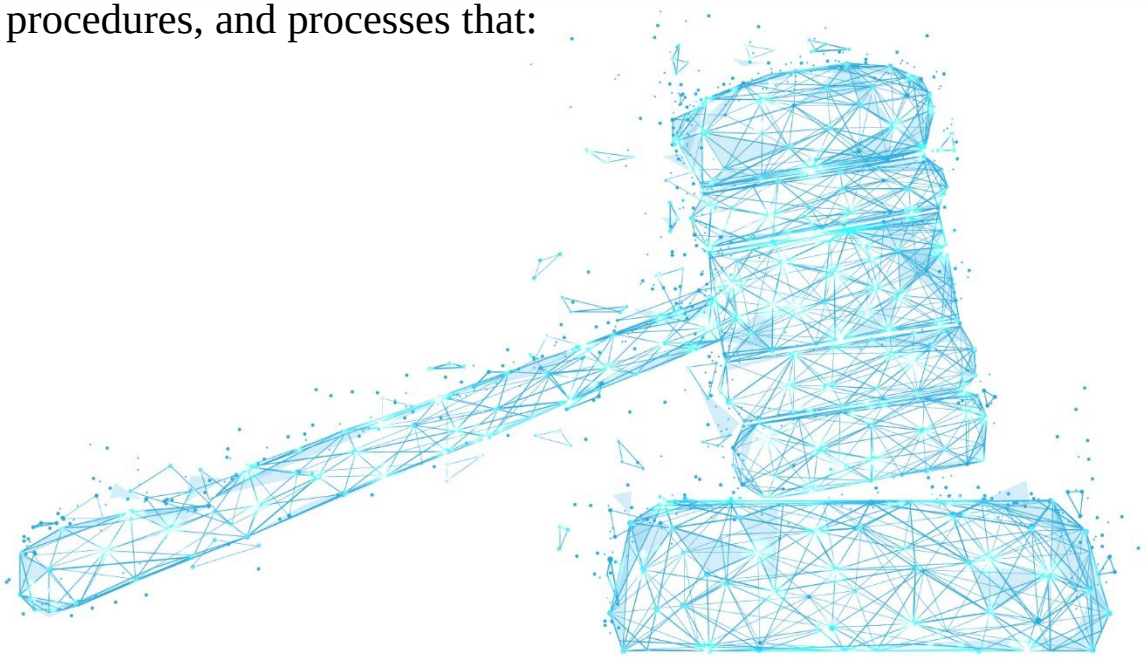
Contact Us at: CISA405d@hhs.gov

APPENDIX

CSA Section 405(d): Legislative Language (1/2)

Authority: Cybersecurity Act of 2015 (CSA), Section 405(d), *Aligning Health Care Industry Security Approaches*

The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that:



CSA Section 405(d): Legislative Language (2/2)

A. Serve as a resource for *cost-effectively reducing cybersecurity risks* for a range of health care organizations;

B. Support *voluntary adoption and implementation* efforts to improve safeguards to address cybersecurity threats;

C. Are consistent with—

   i. The standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)(15));

   ii. The security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note); and

   iii. The provisions of the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111-5), and the amendments made by such Act; and

D. Are updated on a regular basis and applicable to *a range of health care organizations*.

How to Use Practices and Sub-Practices

- There are a total of **10** Cybersecurity Practices, and **89** Sub-Practices.
- Each Cybersecurity Practice has a corresponding set of Sub-Practices, risks that are mitigated by the Practice, and suggested metrics for measuring the effectiveness of the Practice
- Medium Sized orgs can review the Medium Sub-Practices
- Large Sized orgs can review the Medium **and** Large Sub-Practices
- Each Practice is designed to mitigate one or many threats

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	

Sample 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.

Prioritize Your Threats (with Example)

- Implementing all Practices within HICP could be daunting, even for a Large Sized Organization
- Recommendation: Review the threats and implement the most impactful practices first
  - A toolkit will be released shortly to assist with this process

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

E-mail Phishing Attacks: Direct Mitigating Sub-Practices (S)

The below table lists all of the **direct** Sub-Practices for small organizations to mitigate Threat 1: E-mail Phishing Attack, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

Direct || Threat 1: E-Mail Phishing Attacks | Small Organizations		
SP#	**SP Title**	**Short Description**
1.S.A	Email System Configuration	Basic email security controls to enable
1.S.B	Education	Training of workforce on phishing attacks
1.S.C	Phishing Simulations	Conduct phishing campaigns to test and training users
8.S.A	Incident Response	Establish procedures for managing cyber-attacks, especially malware and phishing

E-mail Phishing Attacks: Indirect Mitigating Sub-Practices (S)

The below table lists all of the **indirect** Sub-Practices for small organizations to mitigate Threat 1: E-mail Phishing Attack, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

SP#	SP Title	Short Description
6.S.A	Network Segmentation	Segment devices into various networks, restricting access
6.S.C	Intrusion Prevention	Implement and operate an IPS system to stop well known cyber attacks
8.S.B	ISAC/ISAO Participation	Join an Information Sharing Analysis Center/Organization and receive cyber intel
10.S.A	Policies	Establish cybersecurity policies and a default expectation of practices

E-mail Phishing Attacks: Direct Mitigating Sub-Practices (M)

The below table lists all of the direct and indirect Sub-Practices for medium organizations to mitigate Threat 1: E-mail Phishing Attack, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP#	SP Title	Short Description
1.M.A	Basic Email Protection Controls	Basic email security controls to enable
1.M.B	MFA for Remote Email Access	Enabling multi-factor authentication for remote email access
1.M.D	Workforce Education	Educating workforce on spotting and reporting email based attacks
3.M.D	Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources
6.M.D	Web Proxy Protection	Protect end users browsing the web with outbound proxy technologies
8.M.A	Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks
8.M.B	Incident Response	Establish formal incident response playbooks for responding to cyber attacks

E-mail Phishing Attacks: Indirect Mitigating Sub-Practices (M)

The below table lists all of the indirect Sub-Practices for medium organizations to mitigate Threat 1: E-mail Phishing Attack, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP#	SP Title	Short Description
3.M.A	Identity	Establish a unique identifier for all users, leveraging systems of record
3.M.B	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination
6.M.A	Network Profiles and Firewalls	Deploy firewalls throughout the network
6.M.B	Network Segmentation	Establish a network segmentation strategy with clearly defined zones
6.M.C	Intrusion Prevention Systems	Deploy intrusion prevention systems to protect against known cyber attacks
8.M.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information
10.M.A	Policies	Establish cybersecurity policies and a default expectation of practices

E-mail Phishing Attacks: Direct Mitigating Sub-Practices (L)

The below table lists all of the direct and indirect Sub-Practices for large organizations to mitigate Threat 1: E-mail Phishing Attack, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP#	SP Title	Short Description
1.M.A	Basic Email Protection Controls	Basic email security controls to enable
1.M.B	MFA for Remote Email Access	Enabling multi-factor authentication for remote email access
1.M.D	Workforce Education	Educating workforce on spotting and reporting email based attacks
3.M.D	Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources
6.M.D	Web Proxy Protection	Protect end users browsing the web with outbound proxy technologies
8.M.A	Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks
8.M.B	Incident Response	Establish formal incident response playbooks for responding to cyber attacks
1.L.A	Advanced and Next Generation Tooling	Advanced email security configurations to enable
1.L.B	Digital Signatures	Leverage digital signatures to ensure sender authenticity
1.L.C	Analytics Driven Education	Leverage data and analytics to determine high risk and targeted users, drive education
7.L.A	Penetration Testing	Actively exploit your environment to uncover vulnerabilities and risks
7.L.B	Remediation Planning	Implement formal mechanisms for remediating vulnerabilities and risks
8.L.A	Advanced Security Operations Center	Expand the SOC to a dedicated team that operates 24x7x365
8.L.C	Incident Response Orchestration	Automate the manual response of IR playbooks through advanced tools

E-mail Phishing Attacks: Indirect Mitigating Sub-Practices (L)

The below table lists all of the direct and indirect Sub-Practices for large organizations to mitigate Threat 1: E-mail Phishing Attack, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP#	SP Title	Short Description
3.M.A	Identity	Establish a unique identifier for all users, leveraging systems of record
3.M.B	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination
6.M.A	Network Profiles and Firewalls	Deploy firewalls throughout the network
6.M.B	Network Segmentation	Establish a network segmentation strategy with clearly defined zones
6.M.C	Intrusion Prevention Systems	Deploy intrusion prevention systems to protect against known cyber attacks
8.M.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information
10.M.A	Policies	Establish cybersecurity policies and a default expectation of practices
6.L.A	Additional Network Segmentation	Further implement segmentation strategies for remote VPN access to data center
6.L.D	Network Based Sandboxing/Malware Execution	Monitor common transfer protocols to discover malicious attachments
6.L.E	Network Access Control (NAC)	Ensure endpoints are secure on the network through automated tools
8.L.B	Advanced Information Sharing	Share and receive threat intelligence information from partner organizations