NAVIGATING CYBERSECURITY IN PHARMACY

NELLY CONTE SCHMIDT EDD, MMS, BSPH

COLEGIO DE FARMACEUTICOS DE PUERTO RICO

COLEGIADOS...UNIDOS
SOMOS MÁS FUERTES

CONVENCIÓN ANUAL
CFPR 2024

COLEGIO DE FARMACEUTICOS DE PUERTO RICO

COLEGIADOS...UNIDOS
SOMOS MÁS FUERTES

CONVENCIÓN ANUAL

CFPR 2024 • 22 AL 25 DE AGOSTO
Sheraton Puerto Rico
Hotel & Casino, San Juan

Divulgación de Conflicto de Interés

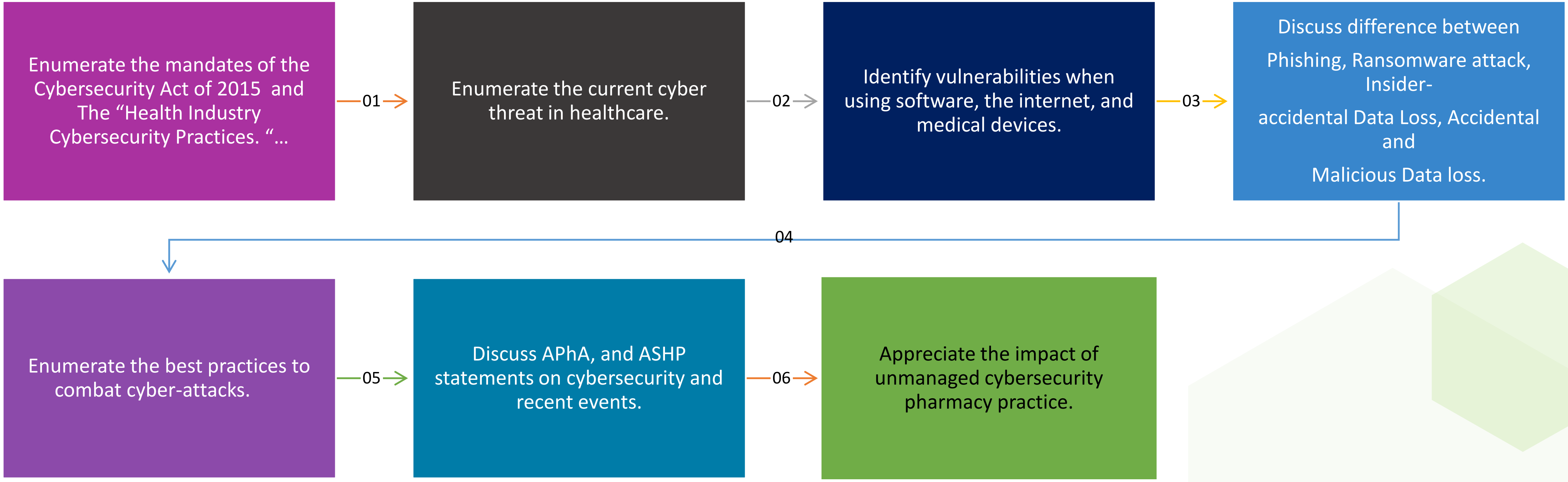
Nelly Conte EdD, MMS, BSPh, facultad para esta actividad de
Educación Continua desea divulgar que no tienen conflicto de interés financiero
ni otras relaciones con los fabricantes de productos comerciales, proveedores de servicios
comerciales o patrocinadores comerciales.

Nelly Conte EdD, MMS, BSPh, faculty for this
Continuing Education activity, has no relevant financial relationship(s)
with ineligible companies to disclose.

“The Colegio de Farmacéuticos de Puerto Rico is accredited by the
Accreditation Council for Pharmacy Education as a provider of continuing pharmacy education.”

Provider Number: 0151

Objectives



Enumerate the mandates of the Cybersecurity Act of 2015 and The “Health Industry Cybersecurity Practices. “…

01

Enumerate the current cyber threat in healthcare.

02

Identify vulnerabilities when using software, the internet, and medical devices.

03

Discuss difference between

Phishing, Ransomware attack, Insider-

accidental Data Loss, Accidental and

Malicious Data loss.

04

Enumerate the best practices to combat cyber-attacks.

05

Discuss APhA, and ASHP statements on cybersecurity and recent events.

06

Appreciate the impact of unmanaged cybersecurity pharmacy practice.

Impact of Cyberattacks (IBM)

- Healthcare data breach costs

$10.93 million

- Hospitals have an average loss of $8M per ransomware incident (CISA, 2023).

- Pharmaceutical industry ranked third

$4.8 million

What is the impact of a Cyber Attack?

- Lost of access to data such as medical history, treatment regimens, or prescriptions
- Loss of data or files, and shutdown
- Loss of ability to maintain operations, critical infrastructure, and critical systems impacting the organization’s revenue
- Unavailability of medical devices and equipment

What is the impact of a Cyber Attack?

- Identity theft
- Intellectual property theft
- Civil Money Penalties
- Loss of reputation
- Loss of future business

Recent Breach Change Healthcare

- Change Healthcare- one of the largest healthcare processors (subsidiary of UnitedHealthcare)
- Cyber attack occurred on February 2024
- The attack was contained, and a recovery plan put in place.
- Many industries gave Change Healthcare technical support.
- Support system was put in place for customers and providers.
- Change Healthcare paid $22 million in Bitcoin in ransom. ($**1,526,932,556,996).**

Testimony hearing: https://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf

Testimony Hearing: Change Healthcare

- The server had no multifactor authentication (MFA).
- A third of the American population was affected.
- Government agencies that were involved: Energy and Commerce, CMS, Administration of Strategic Preparedness and Response.
- The Oversight and Investigation Subcommittee convened a hearing with UnitedHealthcare.
- OCR's investigation of Change Healthcare and UHG will focus on whether a breach occurred and compliance with the HIPAA Rules.

Testimony hearing: mhttps://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf

The 405(d) Program Mandate

The 405(d) Program Mandate

- The 405(d) Program started as a congressional mandate under the Cybersecurity Act of 2015 (CSA), Section 405(d) to strengthen the cybersecurity posture of the healthcare and public health sector.

One goal:

“to **develop a document** that brought forth cybersecurity awareness and provided best practices for mitigating the most pertinent cyber issues within **the healthcare sector.”**

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Healthcare &
Sector Coor
PUBLIC PRIV

Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

The 405(d) Task Group

- **Developed a General Guidance and two Technical Volumes. (2022)**
- Goals:
  1. Cost-effectively reduce cybersecurity risks for a range of health care organizations;
  2. Support **voluntary** adoption and implementation; and
  3. Actionable, practical, and relevant to healthcare stakeholders of every size and resource level.
- Based upon (National Institute of Standards and Technology) NITS Cybersecurity Framework

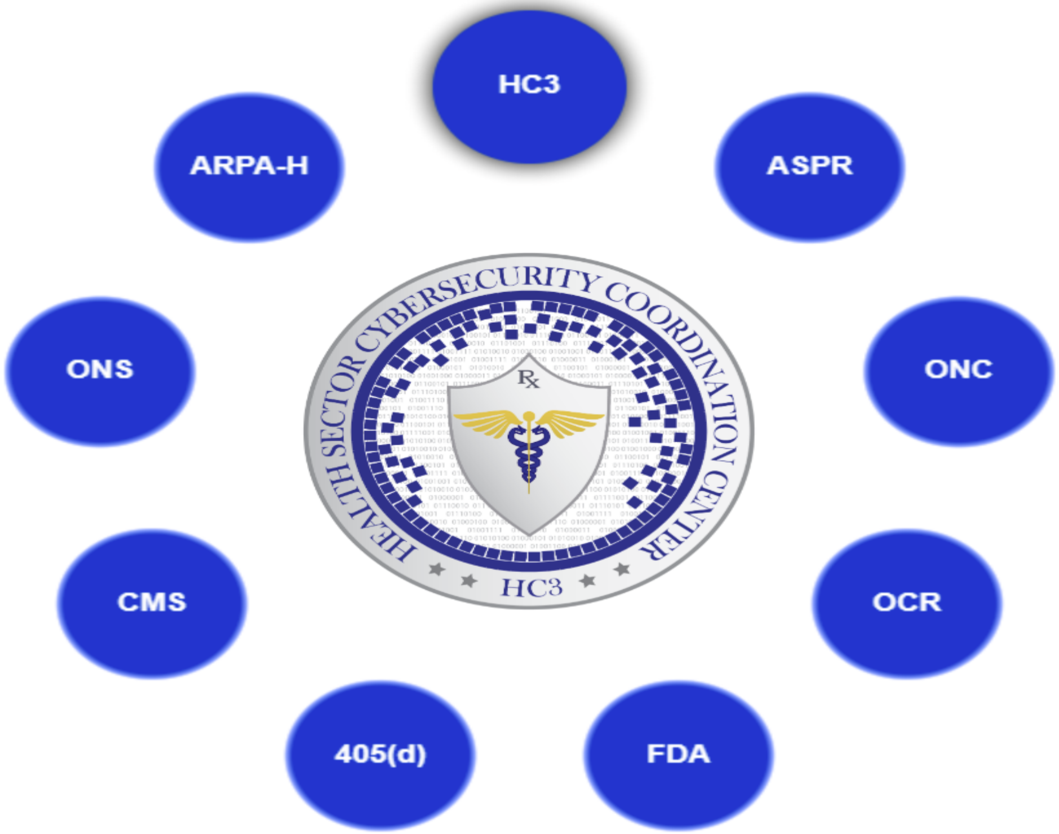
Graphic Source: https://405d.hhs.gov/Documents/HICP-Main-508.pdf

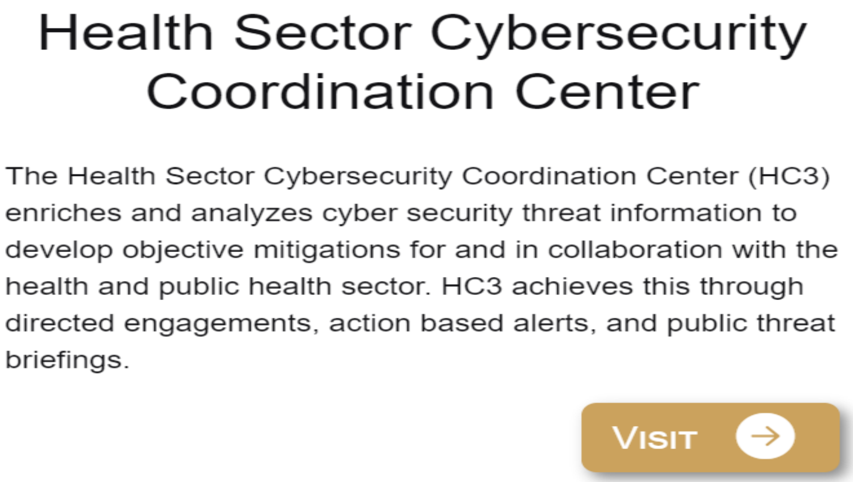
Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

- Is a Call to Action: Healthcare Delivery Organizations (HDOs)

1. Cybersecurity, is a priority for Patient Safety
2. HDO's need to make bold changes and investments
3. Effective cybersecurity is a shared responsibility

Cyber Security is a Shared Responsibility





Health Sector Cybersecurity Coordination Center

The Health Sector Cybersecurity Coordination Center (HC3) enriches and analyzes cyber security threat information to develop objective mitigations for and in collaboration with the health and public health sector. HC3 achieves this through directed engagements, action based alerts, and public threat briefings.

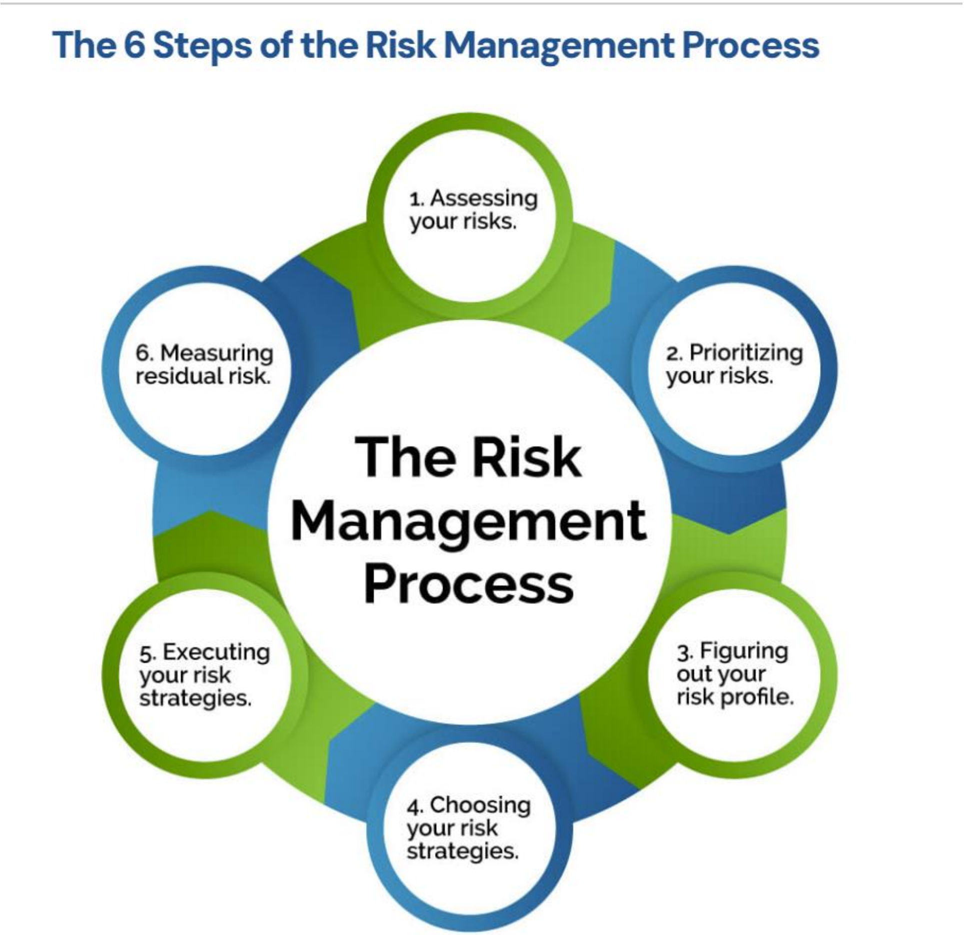
https://hhscyber.hhs.gov/

Cyber Threats

Vulnerabilities versus Threats

- A vulnerability is a weakness or flaw in an operating system, network, or application.
- Easy to guess passwords, unpatched systems, lack of encryption, insecure network configurations, human error or outdated software are all vulnerabilities.
- Lack of risk assessment and mitigation causes vulnerability.
- A threat is an actor (outsider or insider) who tries to exploit vulnerabilities to gain unauthorized access to data or systems.

Risk Mitigation Process and Strategies



The 6 Steps of the Risk Management Process

The Risk Management Process

1. Assessing your risks.

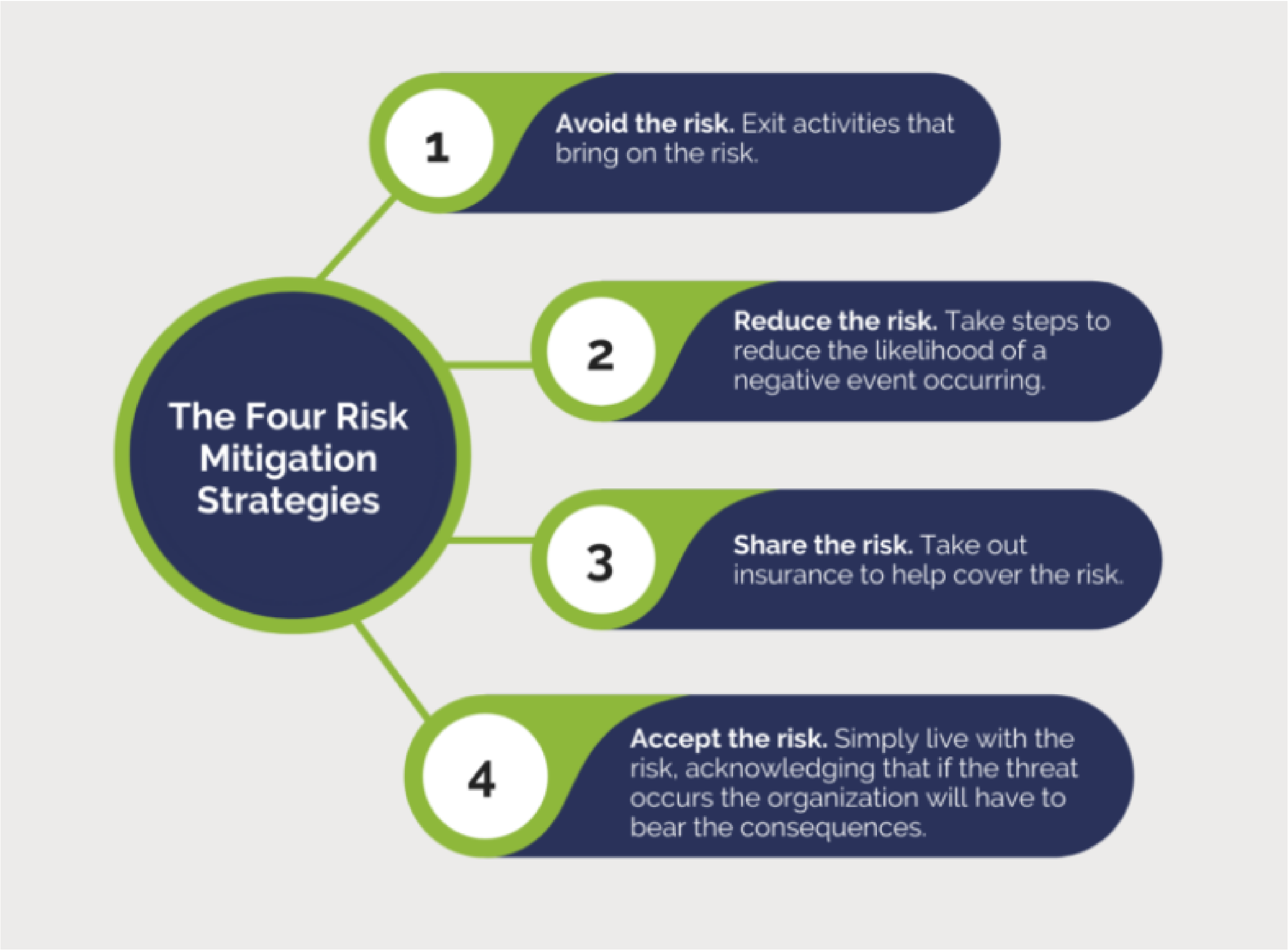
2. Prioritizing your risks.

3. Figuring out your risk profile.

4. Choosing your risk strategies.

5. Executing your risk strategies.

6. Measuring residual risk.



The Four Risk Mitigation Strategies

1 **Avoid the risk.** Exit activities that bring on the risk.

2 **Reduce the risk.** Take steps to reduce the likelihood of a negative event occurring.

3 **Share the risk.** Take out insurance to help cover the risk.

4 **Accept the risk.** Simply live with the risk, acknowledging that if the threat occurs the organization will have to bear the consequences.

https://www.mha-it.com/2020/01/29/risk-management/

Five Current Threats

1. Social Engineering Attacks

2. Ransomware Attacks

3. Loss or Theft of Equipment or Data

4. Internal, Accidental, or Intentional Data Loss

5. Attacks Against Connected Medical Devices that may Affect Patient Safety

Created by Iconfield
from Noun Project

Created by Margarita Rudenko
from Noun Project

Social Engineering Cyber Attacks (Phishing)

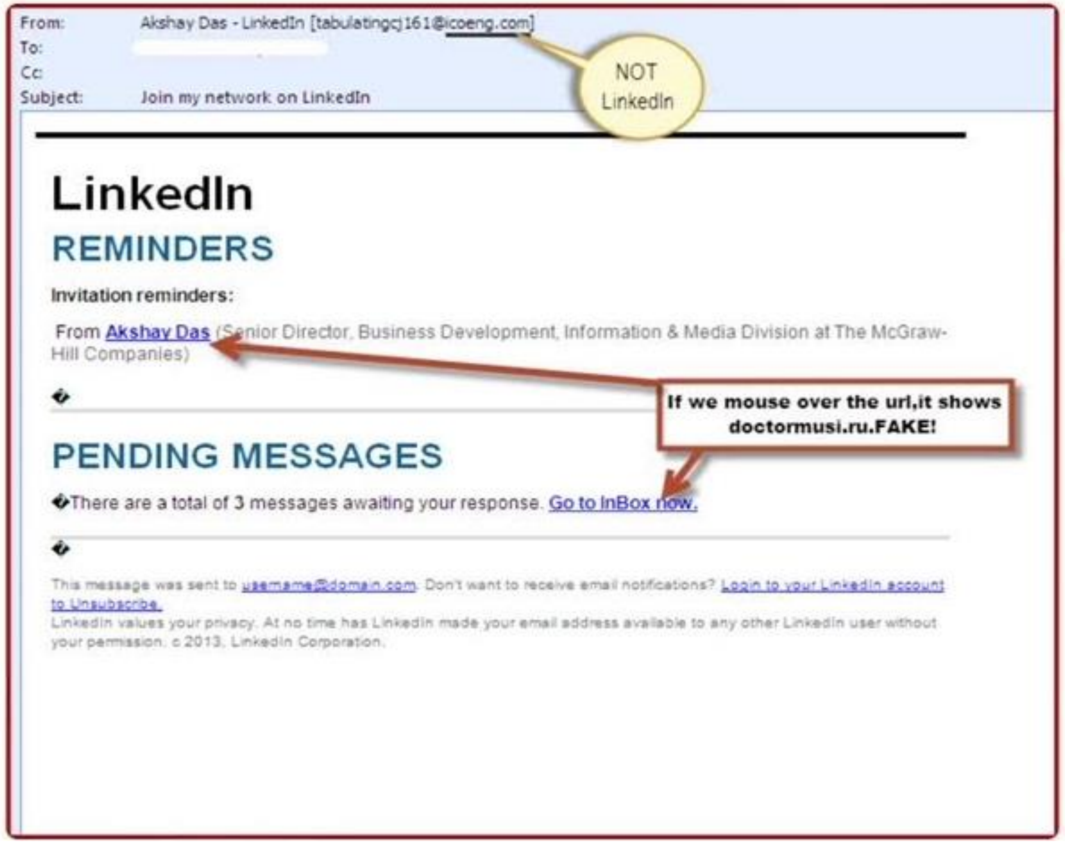
Social engineering- use of fraudulent emails, text messages, phone calls or websites to trick people into sharing sensitive data, downloading malware.

Whaling- a type of phishing attack where a particularly important person in the organization is targeted.

Smishing- the fraudulent practice of sending text messages alleging to be from reputable companies to induce individuals to reveal personal information.

Middle-of-a-Man (MITM)- a threat actor puts themselves in the middle of two parties, typically a user and an application, to intercept their communications and data exchanges

Do you see what I see?



From: Akshay Das - LinkedIn [tabulatingcj161@icoeng.com]
To:
Cc:
Subject: Join my network on LinkedIn

LinkedIn

REMINDERS

Invitation reminders:

From Akshay Das (Senior Director, Business Development, Information & Media Division at The McGraw-Hill Companies)

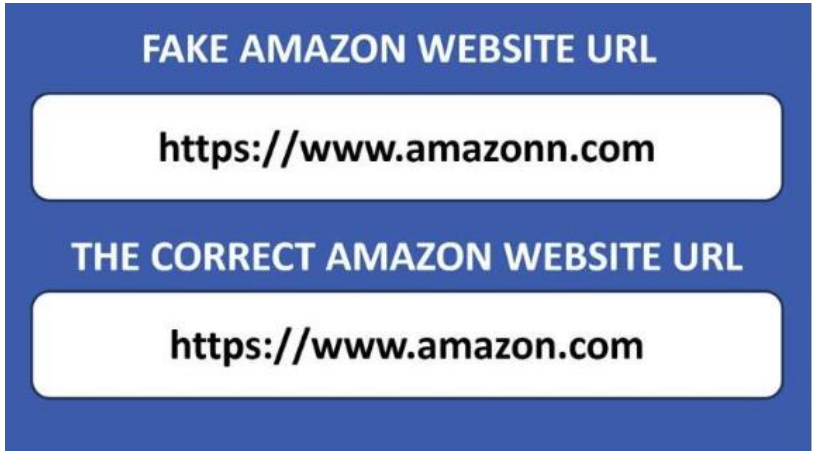
�

PENDING MESSAGES

�There are a total of 3 messages awaiting your response. Go to InBox now.

�

This message was sent to username@domain.com. Don't want to receive email notifications? Login to your LinkedIn account to Unsubscribe.
LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. c 2013, LinkedIn Corporation.

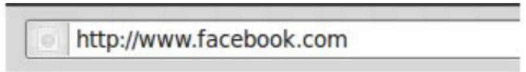


FAKE AMAZON WEBSITE URL

https://www.amazonn.com

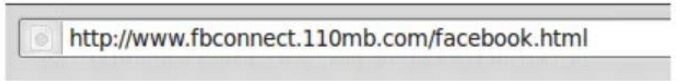
THE CORRECT AMAZON WEBSITE URL

https://www.amazon.com



http://www.facebook.com

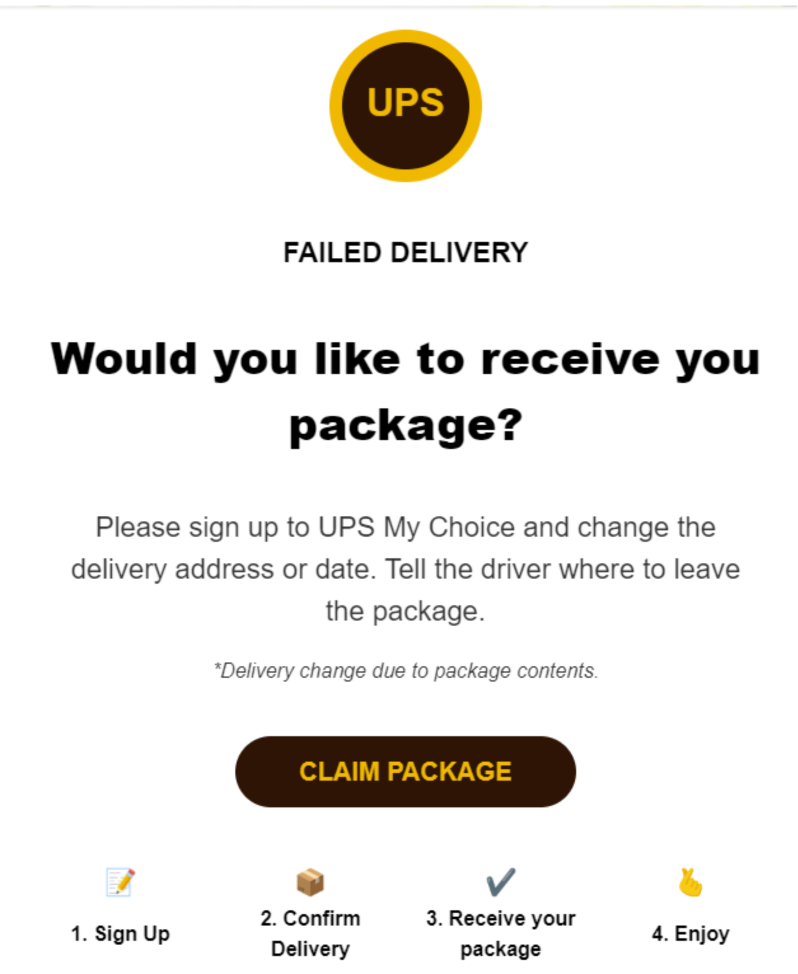
Real URL



http://www.fbconnect.110mb.com/facebook.html

Fake URL

Social Engineering Examples



UPS

FAILED DELIVERY

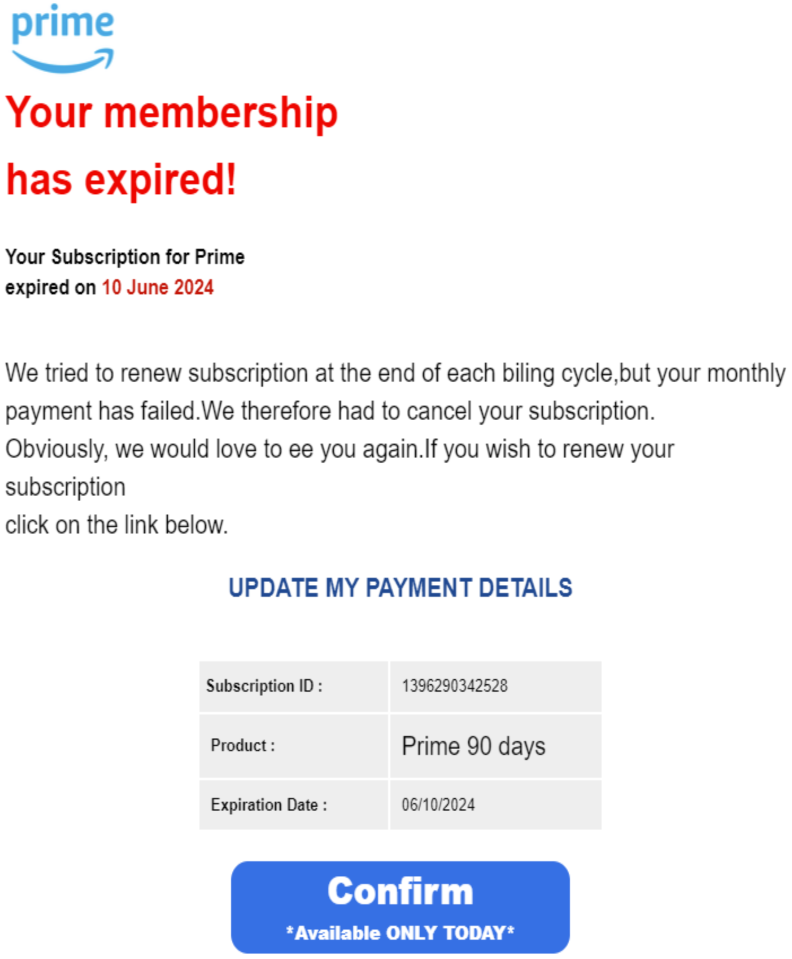
Would you like to receive you package?

Please sign up to UPS My Choice and change the delivery address or date. Tell the driver where to leave the package.

**Delivery change due to package contents.*

CLAIM PACKAGE

📝 1. Sign Up	📦 2. Confirm Delivery	✔️ 3. Receive your package	🫰 4. Enjoy



prime

Your membership has expired!

Your Subscription for Prime expired on 10 June 2024

We tried to renew subscription at the end of each biling cycle,but your monthly payment has failed.We therefore had to cancel your subscription. Obviously, we would love to ee you again.If you wish to renew your subscription
click on the link below.

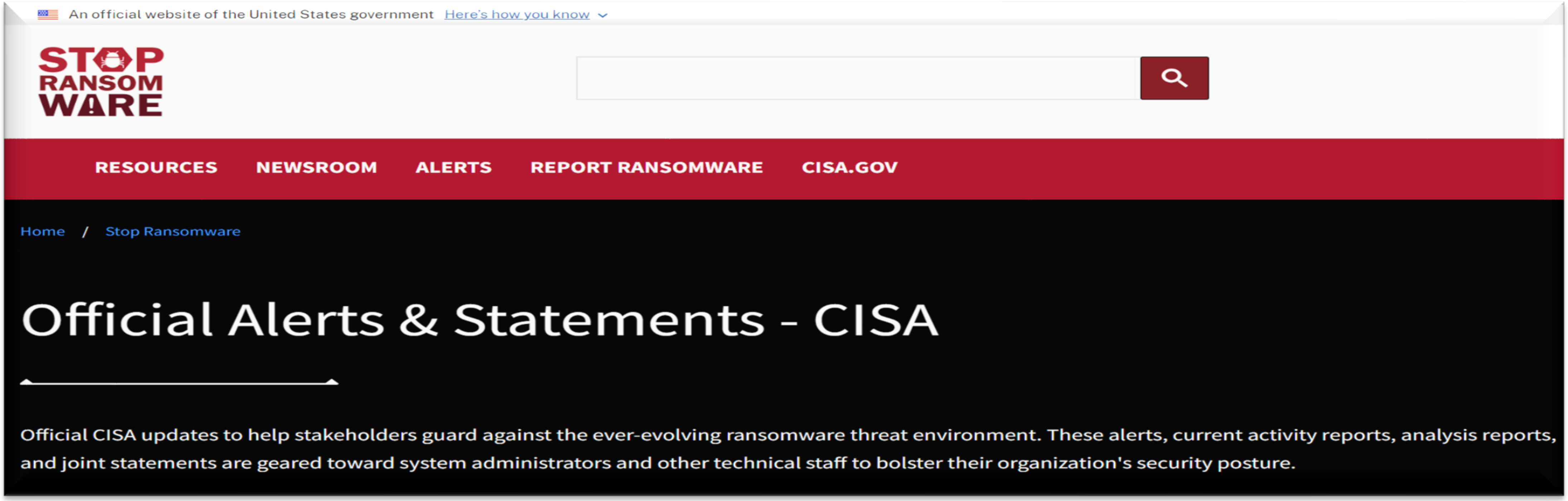
UPDATE MY PAYMENT DETAILS

Subscription ID :	1396290342528
Product :	Prime 90 days
Expiration Date :	06/10/2024

Confirm
Available ONLY TODAY

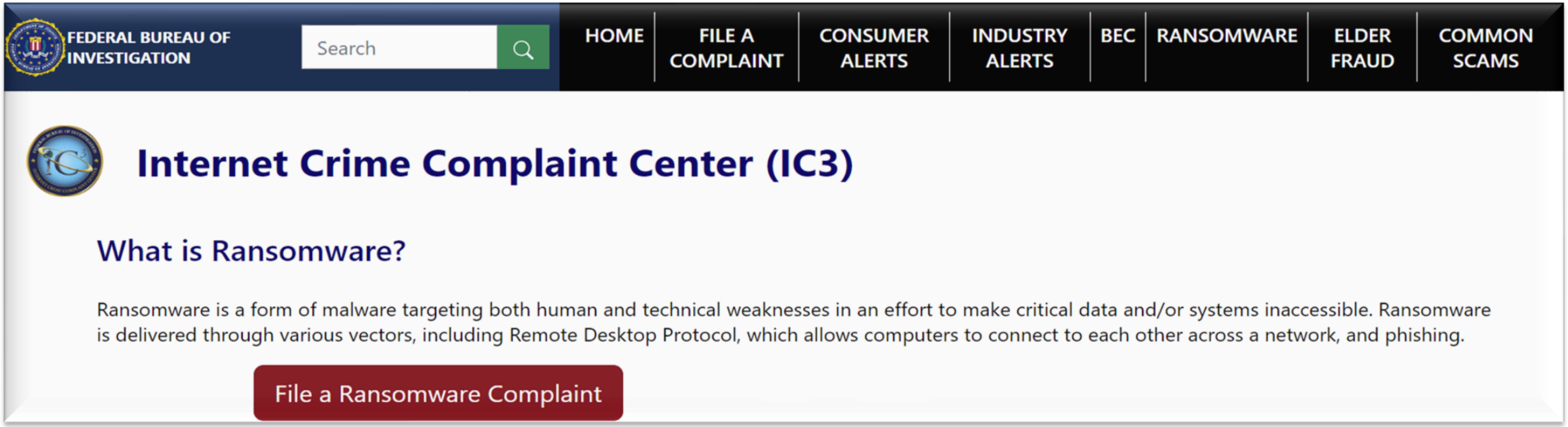
Ransomware Attack

- Extorsion software (malware) that gets access to device(s) locks up computers, operating systems or individual files.
- Prevents from accessing your device and the data stored on it, usually by encrypting the victims' files.
- It demands a ransom from the institution or person attacked.



Official Alerts & Statements - CISA

Official CISA updates to help stakeholders guard against the ever-evolving ransomware threat environment. These alerts, current activity reports, analysis reports, and joint statements are geared toward system administrators and other technical staff to bolster their organization's security posture.



Internet Crime Complaint Center (IC3)

What is Ransomware?

Ransomware is a form of malware targeting both human and technical weaknesses in an effort to make critical data and/or systems inaccessible. Ransomware is delivered through various vectors, including Remote Desktop Protocol, which allows computers to connect to each other across a network, and phishing.

Loss o Theft of Equipment and Data

- One laptop is stolen every 53 seconds.
- 74% occurred in public places or traveling.
- 70 millions smartphones are lost, 7% recovered.

YOUR COMPUTER IS YOUR LIFE

Crime Statistics: https://gitnux.org/laptop-theft-statistics/

Data Loss

- Usually happens from not using proper **passwords,**
- Not abiding to password policies,
- Sharing passwords,
- Using unsecured internet sites,
- Unplugging unknown UBS.

5-characers- instantly
8 –character U&L-2 minutes
8-character U&L, symbol-35 minutes
10-characters U&L, symbols -5 months

Source: Komando Security.com

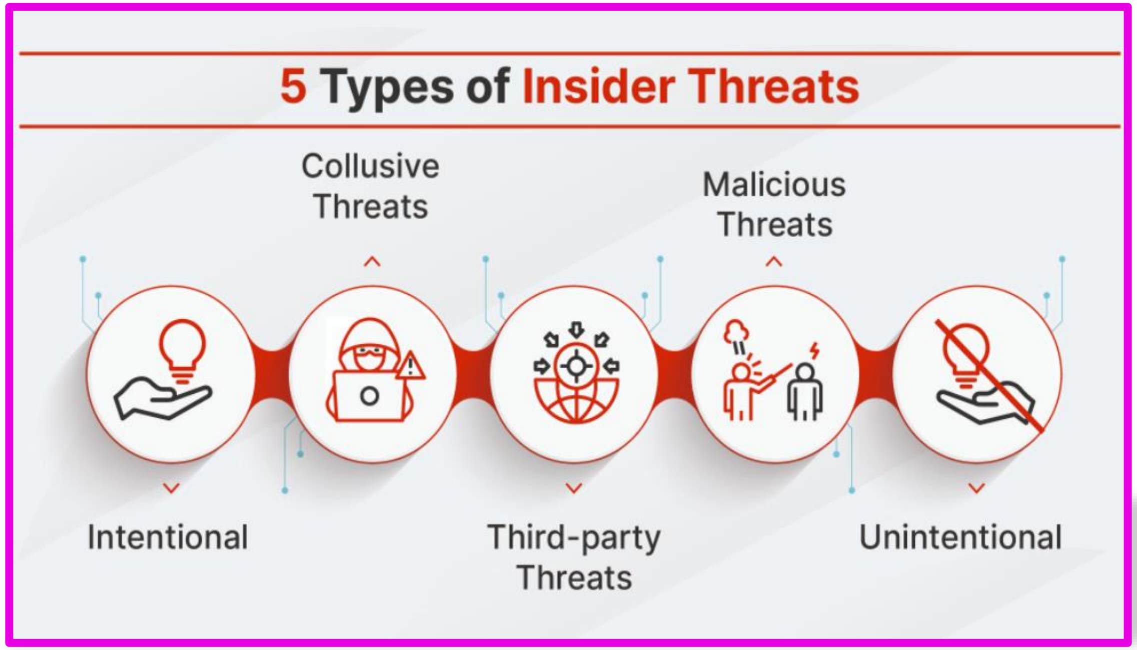
Internal Accidental or Intentional Data Loss

Accidental Insider Threat

- Mistake, error or negligence
- Accidental data leaks/loss

Intentional Insider Threat

- Malicious loss or theft to the organization network, infrastructure or database.



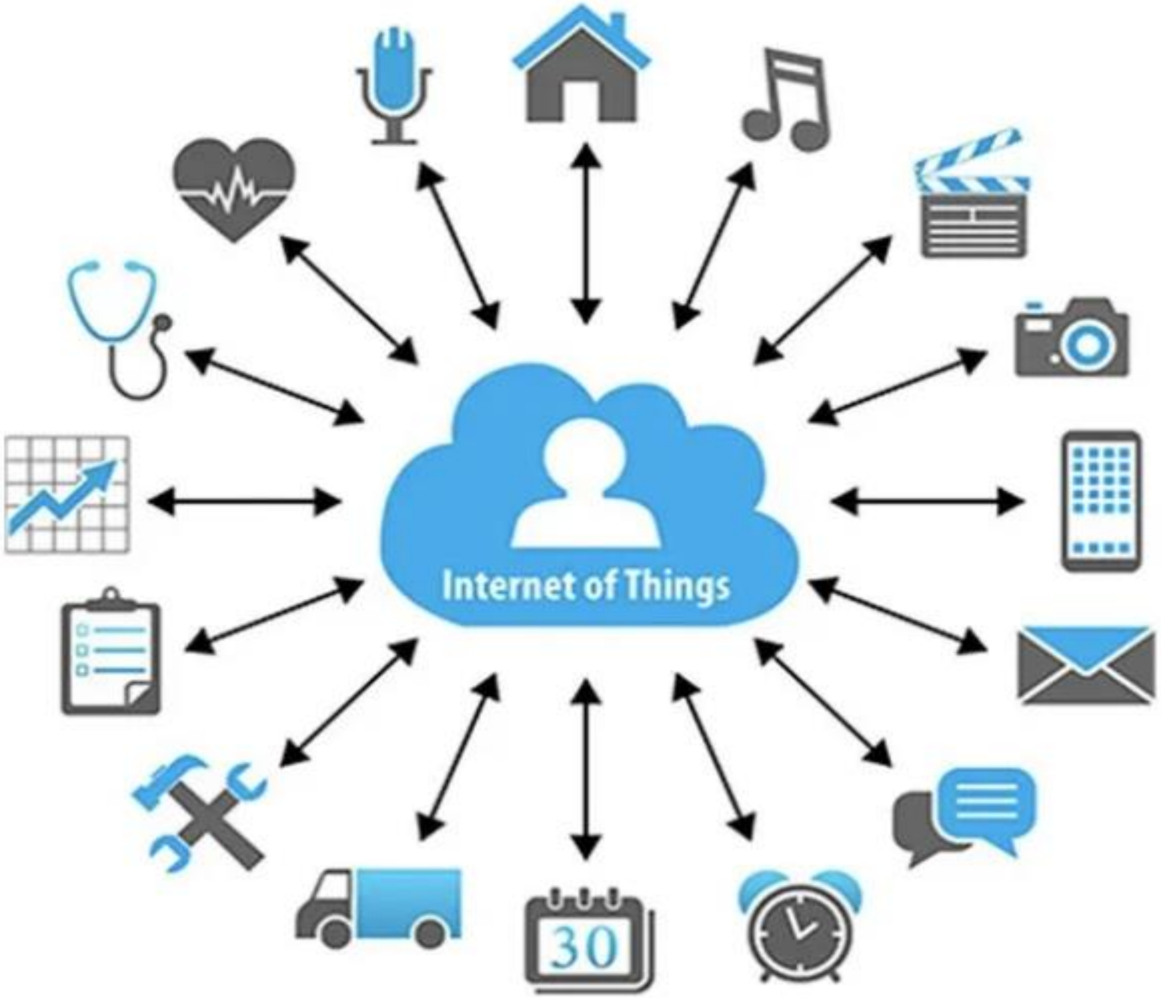
Source: Komando Security.com

Source: https://www.fortinet.com/

According to CISA (Cybersecurity & Infrastructure Security Agency) an Insider is Known and Trusted

- Employees, interns, organization members, and those to whom the organization has given sensitive information and access.
- A person given a badge or access device identifying them as someone with regular or continuous access
- A person to whom the organization has supplied a computer and/or network access.
- A person who develops the organization’s products and services.
- A person who is knowledgeable about the organization’s trade secrets.

Internet of Things



Source: https://medium.com/@bmuha1/what-is-the-iot-introduction-to-the-internet-of-things-57335391cd5f

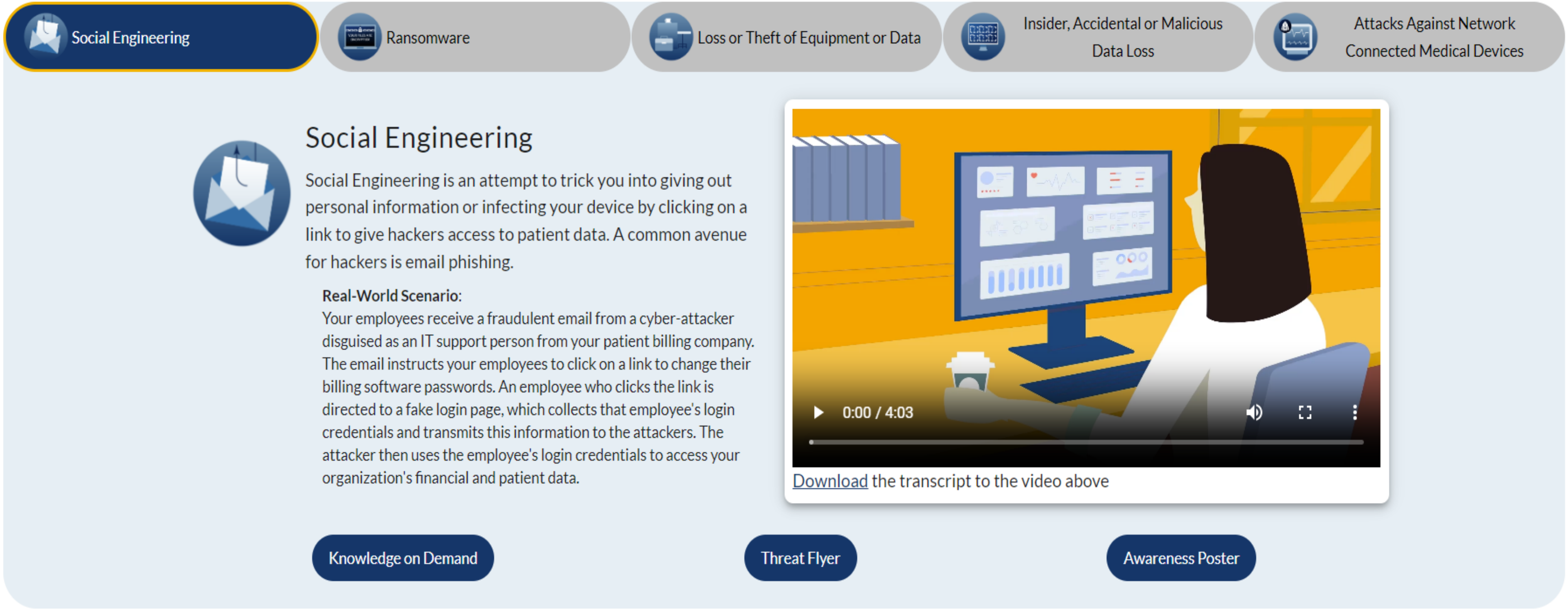
Attacks to Connected Medical Devices

“The Internet of Things”

- Oracle defines IoT as “physical objects embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet”.

What devices you have at home that qualify as IoT?

Have you heard about the top 5 threats facing the HPH sector?


Social Engineering
Ransomware
Loss or Theft of Equipment or Data
Insider, Accidental or Malicious Data Loss
Attacks Against Network Connected Medical Devices
0:00 / 4:03
Knowledge on Demand
Threat Flyer
Awareness Poster

Social Engineering

Social Engineering is an attempt to trick you into giving out personal information or infecting your device by clicking on a link to give hackers access to patient data. A common avenue for hackers is email phishing.

Real-World Scenario:
Your employees receive a fraudulent email from a cyber-attacker disguised as an IT support person from your patient billing company. The email 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.

Download the transcript to the video above

https://405d.hhs.gov/cornerstone/hicp

Knowledge Check #1

Ransomware’s *defining characteristic*(s) include:

a) It immediately shuts down your computer system
b) It will deny access to user’s data
c) Is a type of malicious software
d) Causes your font type to appear blurry

From: CISA’s training; Ransomware-Not if, but when

Knowledge Check #2

Which of the following activities can cause data to be damaged or lost?

a) Staying online too long
b) Never fully shutting your computer down
c) Unauthorized access to a system
d) Always keeping your computer charging

From: CISA's training; Loss or Theft of Equipment and Data

Knowledge Check #3

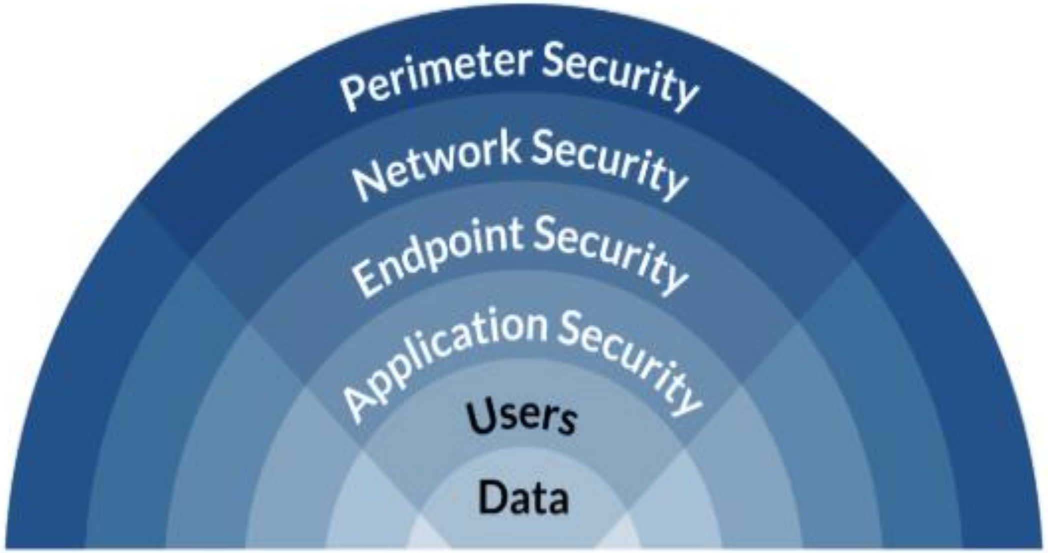
- This is the password you selected: Dove67@

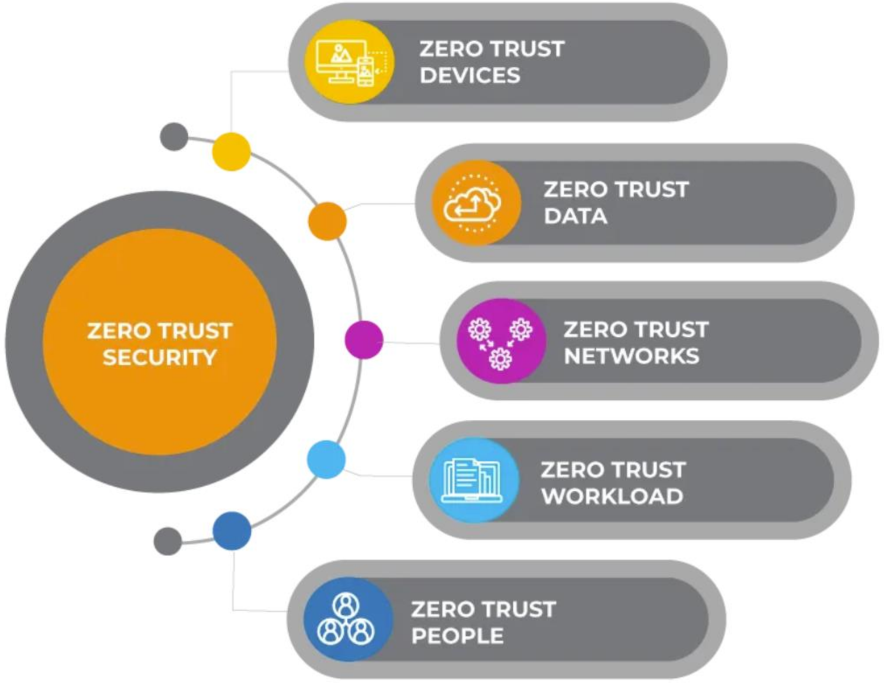
- Do you think Dove67@ is a good password?

Combat with Best Practices

Approaches Promulgated Under Section 405(d)

Figure 5. Defense-in-depth model





Pillars — Zero Trust Security Model

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, 2023 Edition. P.15.

https://medium.com/google-cloud/zero-trust-security-model-a-new-approach-to-network-security-9dee89564b3e

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Healthcare & Sector Coor PUBLIC PRIV

Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations

Healthcare & Public Health Sector Coordinating Council PUBLIC PRIVATE PARTNERSHIP

Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations

Healthcare & Public Health Sector Coordinating Council PUBLIC PRIVATE PARTNERSHIP

Technical Volumes: Mitigation Practices

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

405(d) Recommended Practices (Vol. 1)

Email Protection Systems	Endpoint Protection Systems	Access Management	Data Protection and Loss Prevention
Configure Basic security Controls Training workforce on cyberattacks	Install and update approved endpoint security software, firewalls Update passwords	Account configuration Provision of policies	Data classification policy Procedure on handling sensitive data

Endpoint: https://www.gartner.com/reviews/market/endpoint-protection-platforms

405(d) Recommended Practices (Vol. 1)

Assets Management

Inventory of all IT Assets

Training procurement of new devices

Secure removal of or decommission of devices

Network Management

Segment devices into Various networks

Manage physical security and visitors access

Employ and intrusion prevention system (IPS) for continuous monitoring

Vulnerability Management

Procedure to assess/discover vulnerabilities and remediate

405(d) Recommended Practices (Vol. 1)

Incident Response

Establish procedures
To manage a cyberattack

Keep abreast by joining
Sharing Analysis Center

Network Connected Devices

Secure medical devices
That are connected

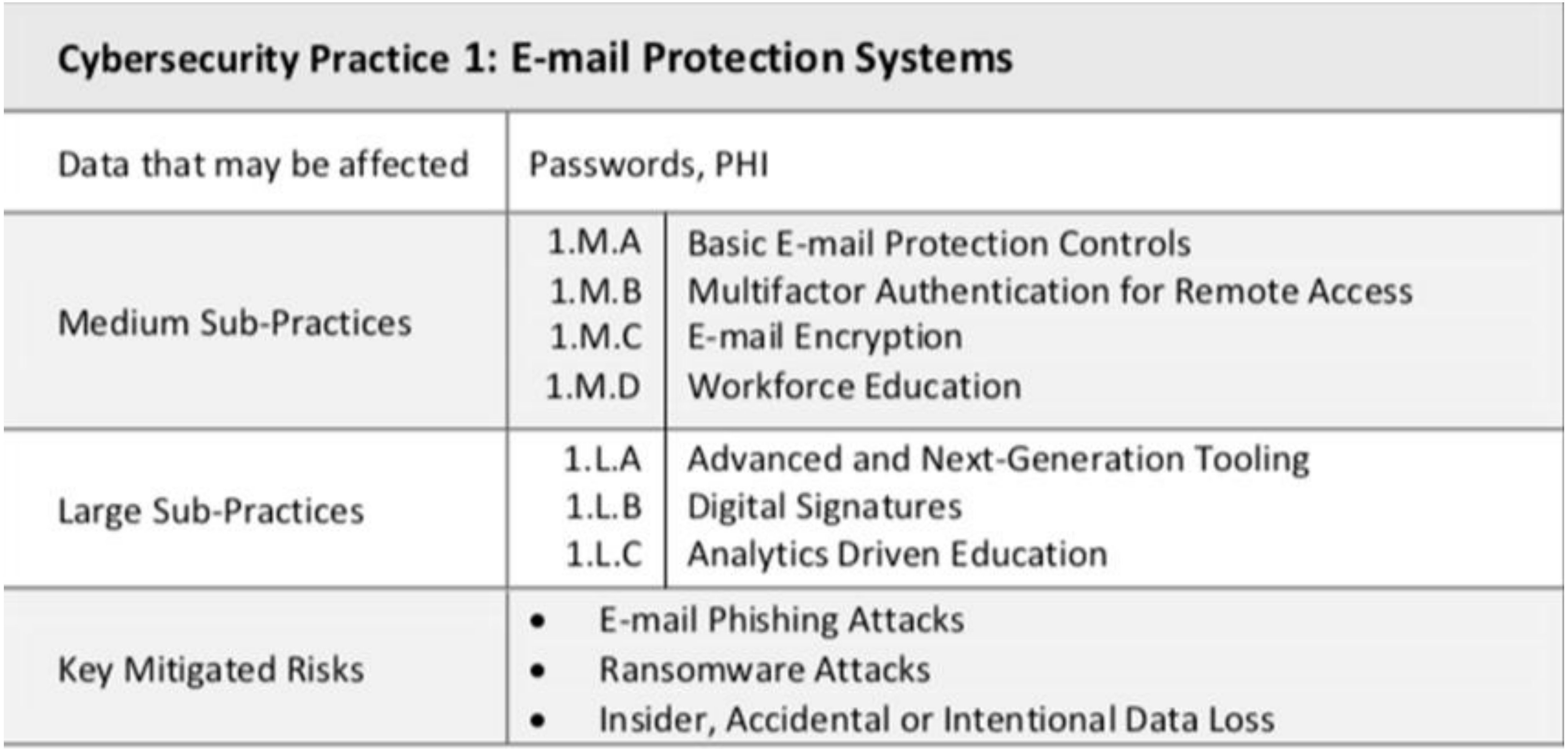
Manage physical security
and visitors access

Oversight and Governance

Establish cybersecurity
Governance, procedure,
expected practices and
oversight

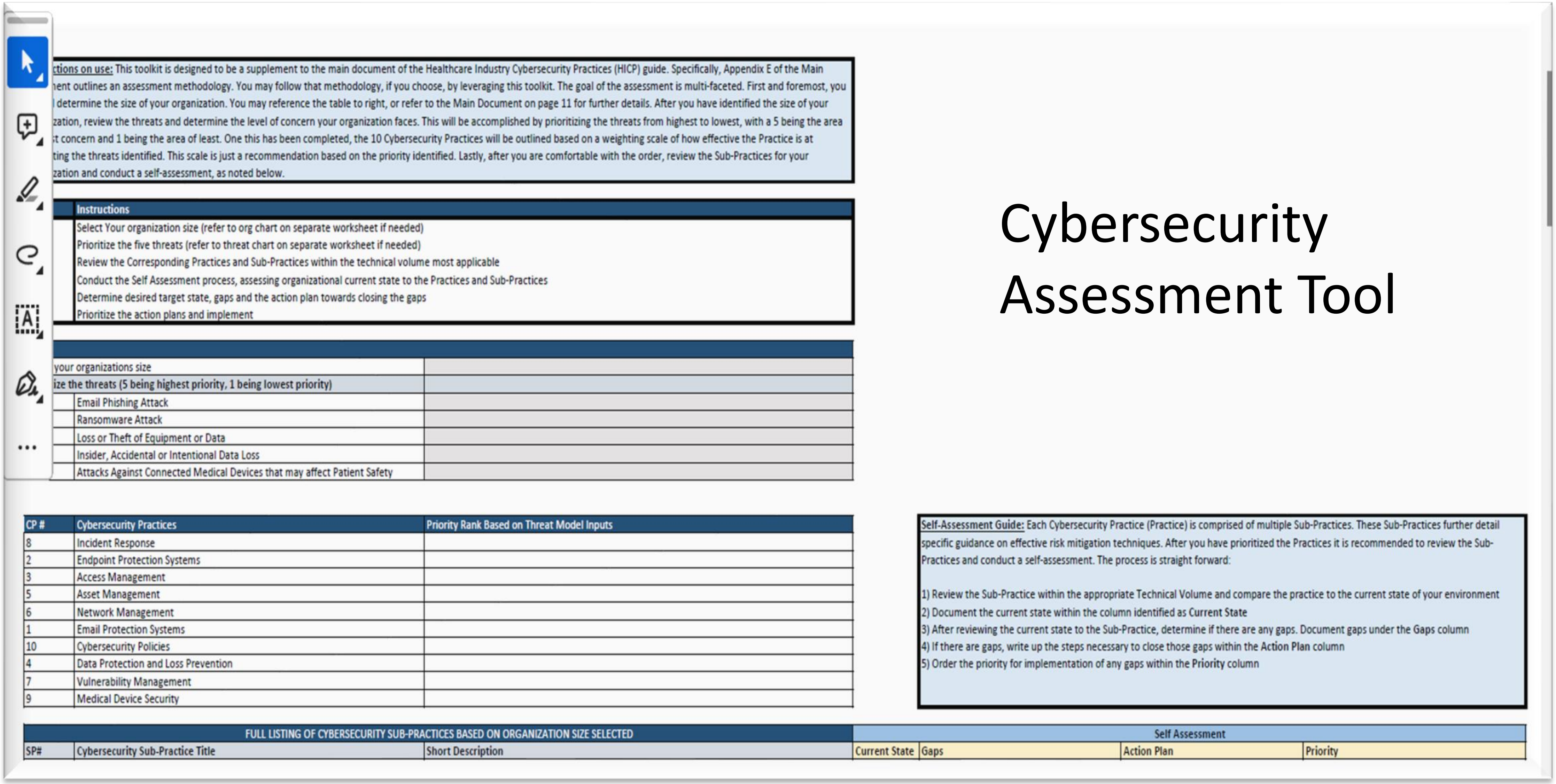
Sharing Analysis Center: https://www.fsisac.com/
FBI/IC3: https://www.ic3.gov/Home/IndustryAlerts
CISA: https://www.cisa.gov/

Vulnerability Management Example



Cybersecurity Practice 1: E-mail Protection Systems		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	1.M.A	Basic E-mail Protection Controls
	1.M.B	Multifactor Authentication for Remote Access
	1.M.C	E-mail Encryption
	1.M.D	Workforce Education
Large Sub-Practices	1.L.A	Advanced and Next-Generation Tooling
	1.L.B	Digital Signatures
	1.L.C	Analytics Driven Education
Key Mitigated Risks	• E-mail Phishing Attacks • Ransomware Attacks • Insider, Accidental or Intentional Data Loss	

Cybersecurity Assessment Tool



ctions on use: This toolkit is designed to be a supplement to the main document of the Healthcare Industry Cybersecurity Practices (HICP) guide. Specifically, Appendix E of the Main
nent outlines an assessment methodology. You may follow that methodology, if you choose, by leveraging this toolkit. The goal of the assessment is multi-faceted. First and foremost, you
l determine the size of your organization. You may reference the table to right, or refer to the Main Document on page 11 for further details. After you have identified the size of your
zation, review the threats and determine the level of concern your organization faces. This will be accomplished by prioritizing the threats from highest to lowest, with a 5 being the area
t concern and 1 being the area of least. One this has been completed, the 10 Cybersecurity Practices will be outlined based on a weighting scale of how effective the Practice is at
ting the threats identified. This scale is just a recommendation based on the priority identified. Lastly, after you are comfortable with the order, review the Sub-Practices for your
zation and conduct a self-assessment, as noted below.

	Instructions
	Select Your organization size (refer to org chart on separate worksheet if needed)
	Prioritize the five threats (refer to threat chart on separate worksheet if needed)
	Review the Corresponding Practices and Sub-Practices within the technical volume most applicable
	Conduct the Self Assessment process, assessing organizational current state to the Practices and Sub-Practices
	Determine desired target state, gaps and the action plan towards closing the gaps
	Prioritize the action plans and implement

your organizations size		
ize the threats (5 being highest priority, 1 being lowest priority)		
	Email Phishing Attack	
	Ransomware Attack	
	Loss or Theft of Equipment or Data	
	Insider, Accidental or Intentional Data Loss	
	Attacks Against Connected Medical Devices that may affect Patient Safety	

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

Self-Assessment Guide: Each Cybersecurity Practice (Practice) is comprised of multiple Sub-Practices. These Sub-Practices further detail specific guidance on effective risk mitigation techniques. After you have prioritized the Practices it is recommended to review the Sub-Practices and conduct a self-assessment. The process is straight forward:

1) Review the Sub-Practice within the appropriate Technical Volume and compare the practice to the current state of your environment
2) Document the current state within the column identified as Current State
3) After reviewing the current state to the Sub-Practice, determine if there are any gaps. Document gaps under the Gaps column
4) If there are gaps, write up the steps necessary to close those gaps within the **Action Plan** column
5) Order the priority for implementation of any gaps within the **Priority** column

FULL LISTING OF CYBERSECURITY SUB-PRACTICES BASED ON ORGANIZATION SIZE SELECTED			Self Assessment			
SP#	Cybersecurity Sub-Practice Title	Short Description	Current State	Gaps	Action Plan	Priority

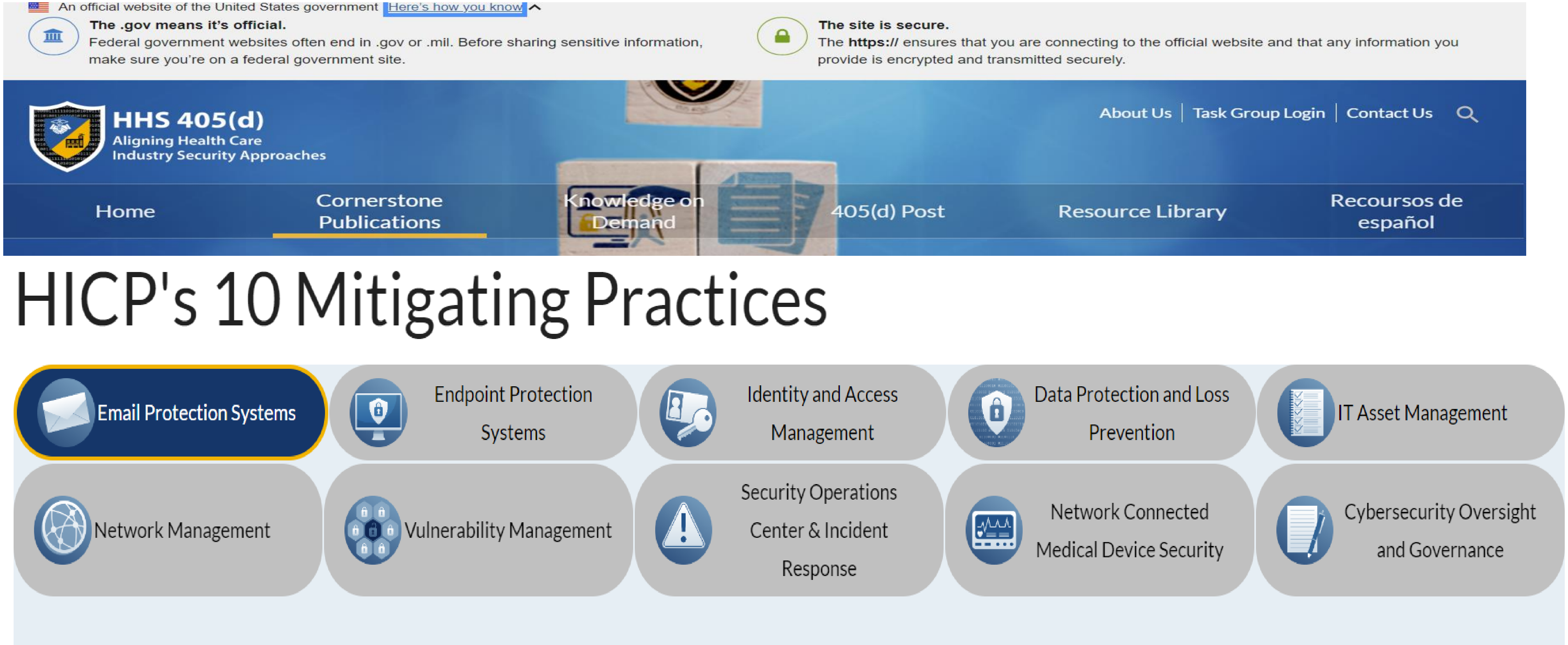
Example

You are a Supervisor at a hospital pharmacy. You delegated the first day of training of a new employee to one of your staff pharmacists. The staff pharmacist shared her password to provide the opportunity for the new employee to practice reviewing electronic orders.

Process	Threat	Potential Effect	S	O	Causes	Controls	D
STEP 2 (check emails)	In what ways it can go wrong?	What are the impacts?	1	1	What causes to go wrong?	What are the existing controls?	Y,N

S= severity 1-low, 2-moderate, 3- high
O= occurrence 1-rarely, 2- often 3- many
D= detectability 1- Yes, 2- No

Where to Find The Mitigating Practices



An official website of the United States government Here's how you know

The .gov means it's official.
Federal government websites often end in .gov or .mil. Before sharing sensitive information, make sure you're on a federal government site.

The site is secure.
The **https://** ensures that you are connecting to the official website and that any information you provide is encrypted and transmitted securely.

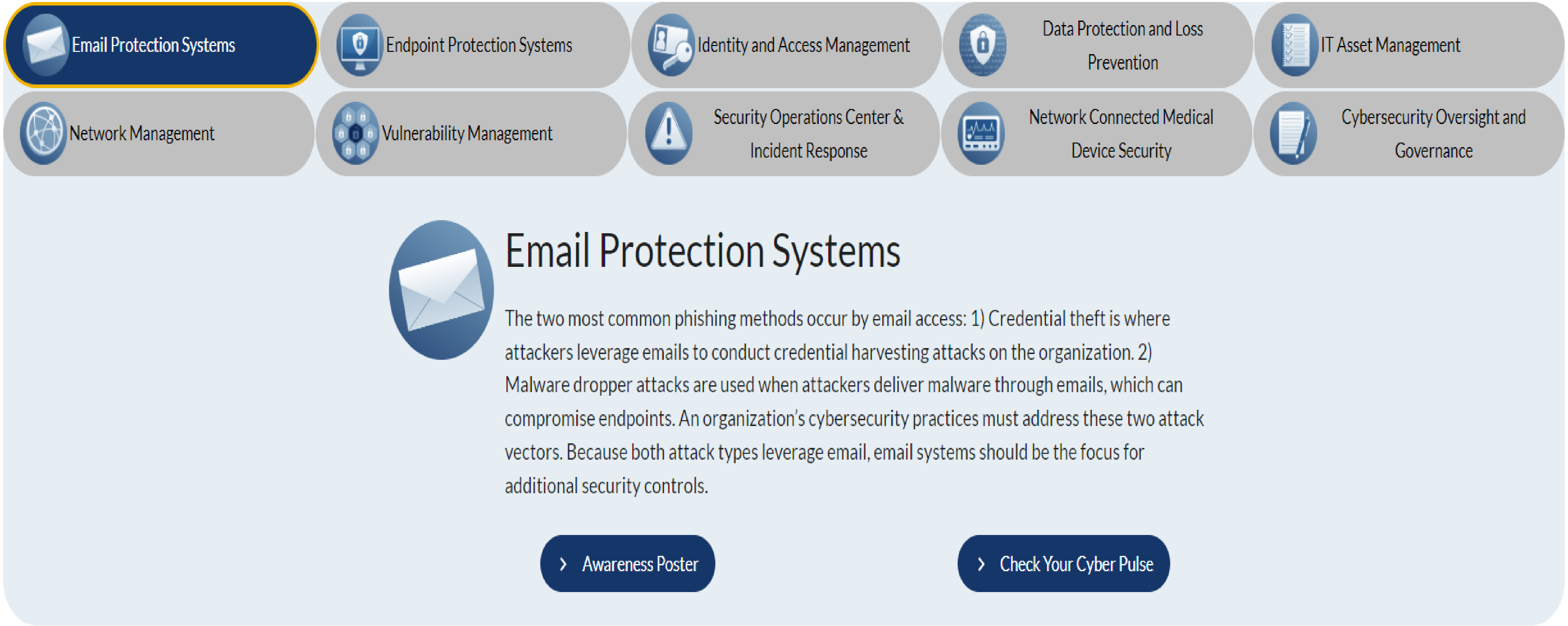
HHS 405(d)
Aligning Health Care Industry Security Approaches

HICP's 10 Mitigating Practices

- Email Protection Systems
- Endpoint Protection Systems
- Identity and Access Management
- Data Protection and Loss Prevention
- IT Asset Management
- Network Management
- Vulnerability Management
- Security Operations Center & Incident Response
- Network Connected Medical Device Security
- Cybersecurity Oversight and Governance

https://405d.hhs.gov/cornerstone/hicp

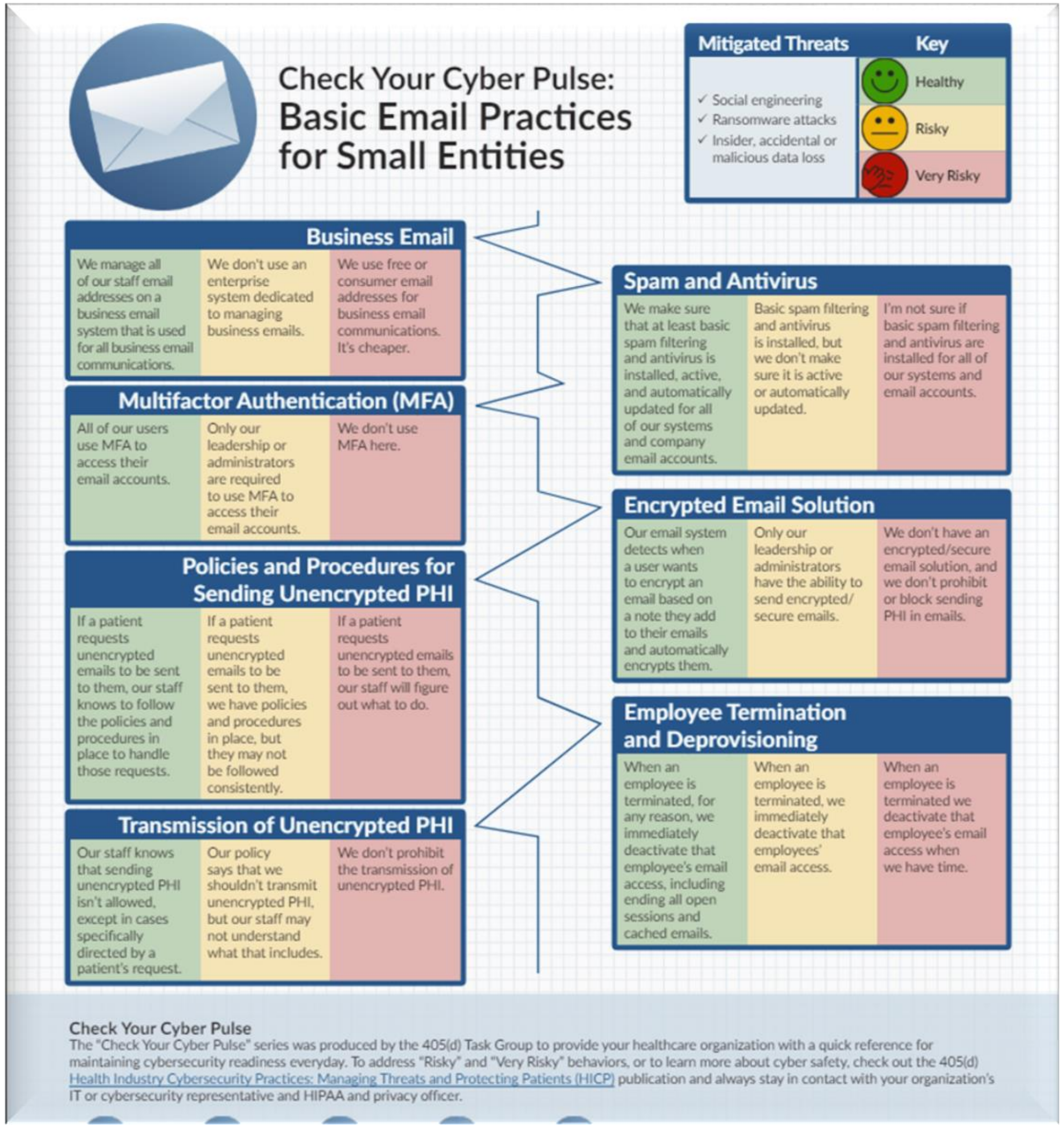
HICP's 10 Mitigating Practices


Email Protection Systems
Endpoint Protection Systems
Identity and Access Management
Data Protection and Loss Prevention
IT Asset Management
Network Management
Vulnerability Management
Security Operations Center & Incident Response
Network Connected Medical Device Security
Cybersecurity Oversight and Governance

Email Protection Systems

The two most common phishing methods occur by email access: 1) Credential theft is where attackers leverage emails to conduct credential harvesting attacks on the organization. 2) Malware dropper attacks are used when attackers deliver malware through emails, which can compromise endpoints. An organization's cybersecurity practices must address these two attack vectors. Because both attack types leverage email, email systems should be the focus for additional security controls.

https://405d.hhs.gov/cornerstone/hicp



Check Your Cyber Pulse: Basic Email Practices for Small Entities

Mitigated Threats	Key
✓ Social engineering ✓ Ransomware attacks ✓ Insider, accidental or malicious data loss	🟩 Healthy 🟨 Risky 🟥 Very Risky

Business Email

We manage all of our staff email addresses on a business email system that is used for all business email communications.	We don't use an enterprise system dedicated to managing business emails.	We use free or consumer email addresses for business email communications. It's cheaper.

Multifactor Authentication (MFA)

All of our users use MFA to access their email accounts.	Only our leadership or administrators are required to use MFA to access their email accounts.	We don't use MFA here.

Policies and Procedures for Sending Unencrypted PHI

If a patient requests unencrypted emails to be sent to them, our staff knows to follow the policies and procedures in place to handle those requests.	If a patient requests unencrypted emails to be sent to them, we have policies and procedures in place, but they may not be followed consistently.	If a patient requests unencrypted emails to be sent to them, our staff will figure out what to do.

Transmission of Unencrypted PHI

Our staff knows that sending unencrypted PHI isn't allowed, except in cases specifically directed by a patient's request.	Our policy says that we shouldn't transmit unencrypted PHI, but our staff may not understand what that includes.	We don't prohibit the transmission of unencrypted PHI.

Spam and Antivirus

We make sure that at least basic spam filtering and antivirus is installed, active, and automatically updated for all of our systems and company email accounts.	Basic spam filtering and antivirus is installed, but we don't make sure it is active or automatically updated.	I'm not sure if basic spam filtering and antivirus are installed for all of our systems and email accounts.

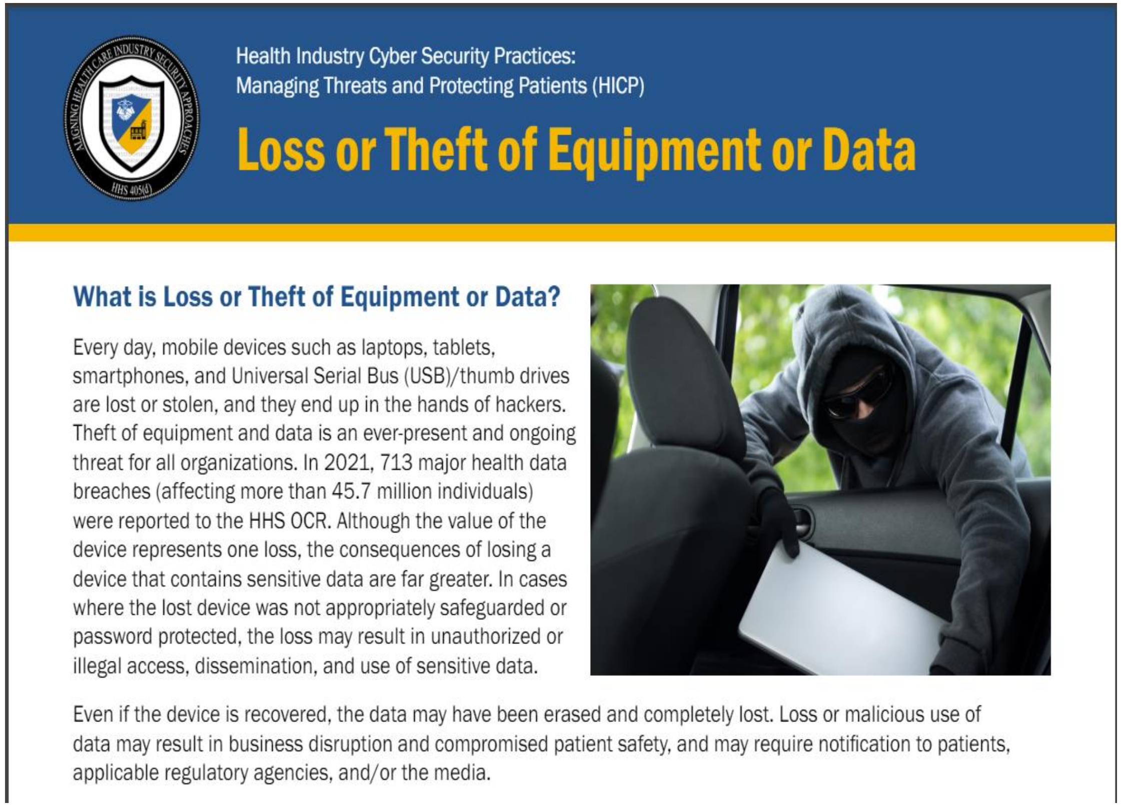
Encrypted Email Solution

Our email system detects when a user wants to encrypt an email based on a note they add to their emails and automatically encrypts them.	Only our leadership or administrators have the ability to send encrypted/secure emails.	We don't have an encrypted/secure email solution, and we don't prohibit or block sending PHI in emails.

Employee Termination and Deprovisioning

When an employee is terminated, for any reason, we immediately deactivate that employee's email access, including ending all open sessions and cached emails.	When an employee is terminated, we immediately deactivate that employees' email access.	When an employee is terminated we deactivate that employee's email access when we have time.

Check Your Cyber Pulse
The "Check Your Cyber Pulse" series was produced by the 405(d) Task Group to provide your healthcare organization with a quick reference for maintaining cybersecurity readiness everyday. To address "Risky" and "Very Risky" behaviors, or to learn more about cyber safety, check out the 405(d) Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication and always stay in contact with your organization's IT or cybersecurity representative and HIPAA and privacy officer.



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

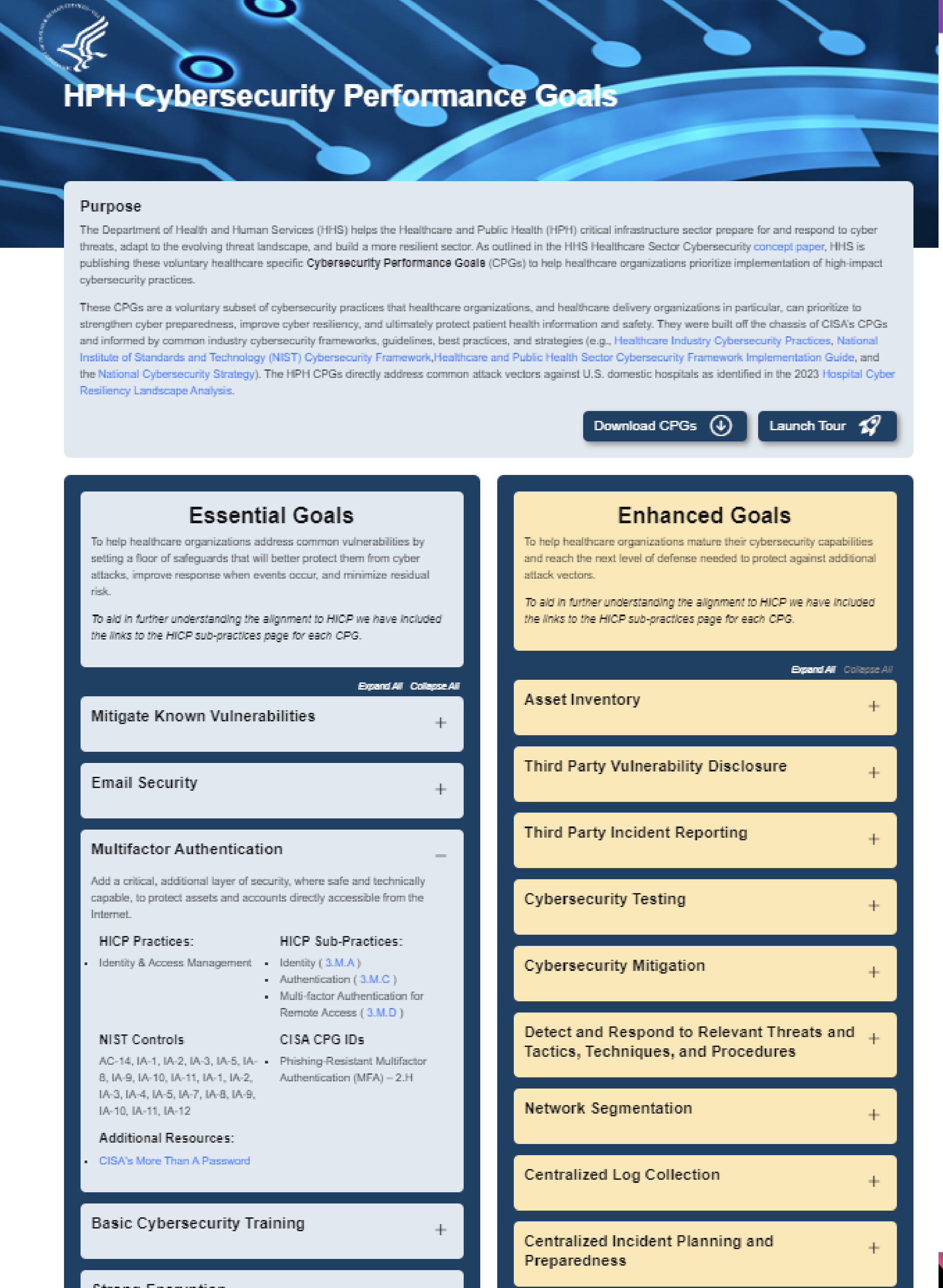
Loss or Theft of Equipment or Data

What is Loss or Theft of Equipment or Data?

Every day, mobile devices such as laptops, tablets, smartphones, and Universal Serial Bus (USB)/thumb drives are lost or stolen, and they end up in the hands of hackers. Theft of equipment and data is an ever-present and ongoing threat for all organizations. In 2021, 713 major health data breaches (affecting more than 45.7 million individuals) were reported to the HHS OCR. Although the value of the device represents one loss, the consequences of losing a device that contains sensitive data are far greater. In cases where the lost device was not appropriately safeguarded or password protected, the loss may result in unauthorized or illegal access, dissemination, and use of sensitive data.

Even if the device is recovered, the data may have been erased and completely lost. Loss or malicious use of data may result in business disruption and compromised patient safety, and may require notification to patients, applicable regulatory agencies, and/or the media.

The Department of Health and Human Services (HHS



Purpose

The Department of Health and Human Services (HHS) helps the Healthcare and Public Health (HPH) critical infrastructure sector prepare for and respond to cyber threats, adapt to the evolving threat landscape, and build a more resilient sector. As outlined in the HHS Healthcare Sector Cybersecurity concept paper, HHS is publishing these voluntary healthcare specific **Cybersecurity Performance Goals** (CPGs) to help healthcare organizations prioritize implementation of high-impact cybersecurity practices.

These CPGs are a voluntary subset of cybersecurity practices that healthcare organizations, and healthcare delivery organizations in particular, can prioritize to strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety. They were built off the chassis of CISA's CPGs and informed by common industry cybersecurity frameworks, guidelines, best practices, and strategies (e.g., Healthcare Industry Cybersecurity Practices, National Institute of Standards and Technology (NIST) Cybersecurity Framework,Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide, and the National Cybersecurity Strategy). The HPH CPGs directly address common attack vectors against U.S. domestic hospitals as identified in the 2023 Hospital Cyber Resiliency Landscape Analysis.

Essential Goals

To help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyber attacks, improve response when events occur, and minimize residual risk.

To aid in further understanding the alignment to HICP we have included the links to the HICP sub-practices page for each CPG.

Mitigate Known Vulnerabilities +

Email Security +

Multifactor Authentication –

Add a critical, additional layer of security, where safe and technically capable, to protect assets and accounts directly accessible from the Internet.

HICP Practices:

- Identity & Access Management

HICP Sub-Practices:

- Identity (3.M.A)
- Authentication (3.M.C)
- Multi-factor Authentication for Remote Access (3.M.D)

NIST Controls

AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11, IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12

CISA CPG IDs

- Phishing-Resistant Multifactor Authentication (MFA) – 2.H

Additional Resources:

- CISA's More Than A Password

Basic Cybersecurity Training +

Strong Encryption

Enhanced Goals

To help healthcare organizations mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors.

To aid in further understanding the alignment to HICP we have included the links to the HICP sub-practices page for each CPG.

Asset Inventory +

Third Party Vulnerability Disclosure +

Third Party Incident Reporting +

Cybersecurity Testing +

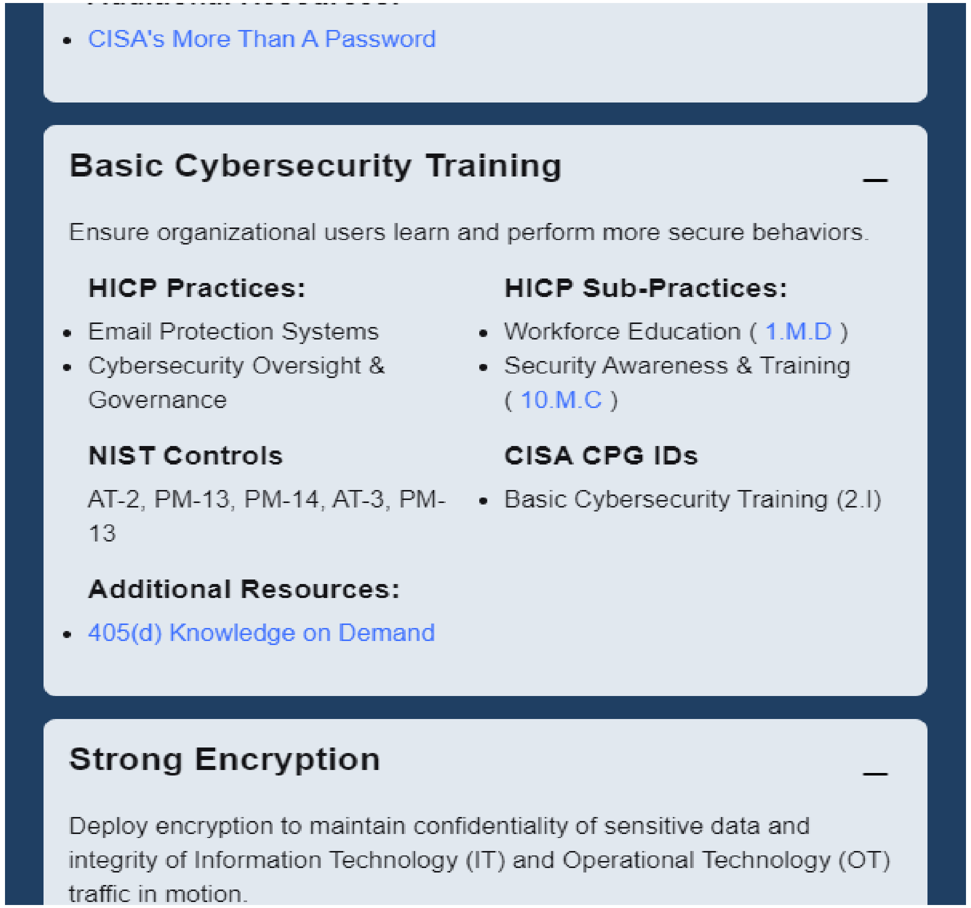
Cybersecurity Mitigation +

Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures +

Network Segmentation +

Centralized Log Collection +

Centralized Incident Planning and Preparedness +



- CISA's More Than A Password

Basic Cybersecurity Training –

Ensure organizational users learn and perform more secure behaviors.

HICP Practices:

- Email Protection Systems
- Cybersecurity Oversight & Governance

HICP Sub-Practices:

- Workforce Education (1.M.D)
- Security Awareness & Training (10.M.C)

NIST Controls

AT-2, PM-13, PM-14, AT-3, PM-13

CISA CPG IDs

- Basic Cybersecurity Training (2.I)

Additional Resources:

- 405(d) Knowledge on Demand

Strong Encryption –

Deploy encryption to maintain confidentiality of sensitive data and integrity of Information Technology (IT) and Operational Technology (OT) traffic in motion.

America’s Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Free Cybersecurity Services and Tools

Knowledge Check #4

Your employee receives a fraudulent email from a cyber-attacker disguised as an IT support person from your patient billing company. The email instructs your employee to click on a link to change their billing software passwords.

- What could happen?= What is the risk?
- Why might it happen?= Vulnerabilities
- What is the impact?= (data breach, ransom of data,,,)
- Is there an existing policy/procedure in place?

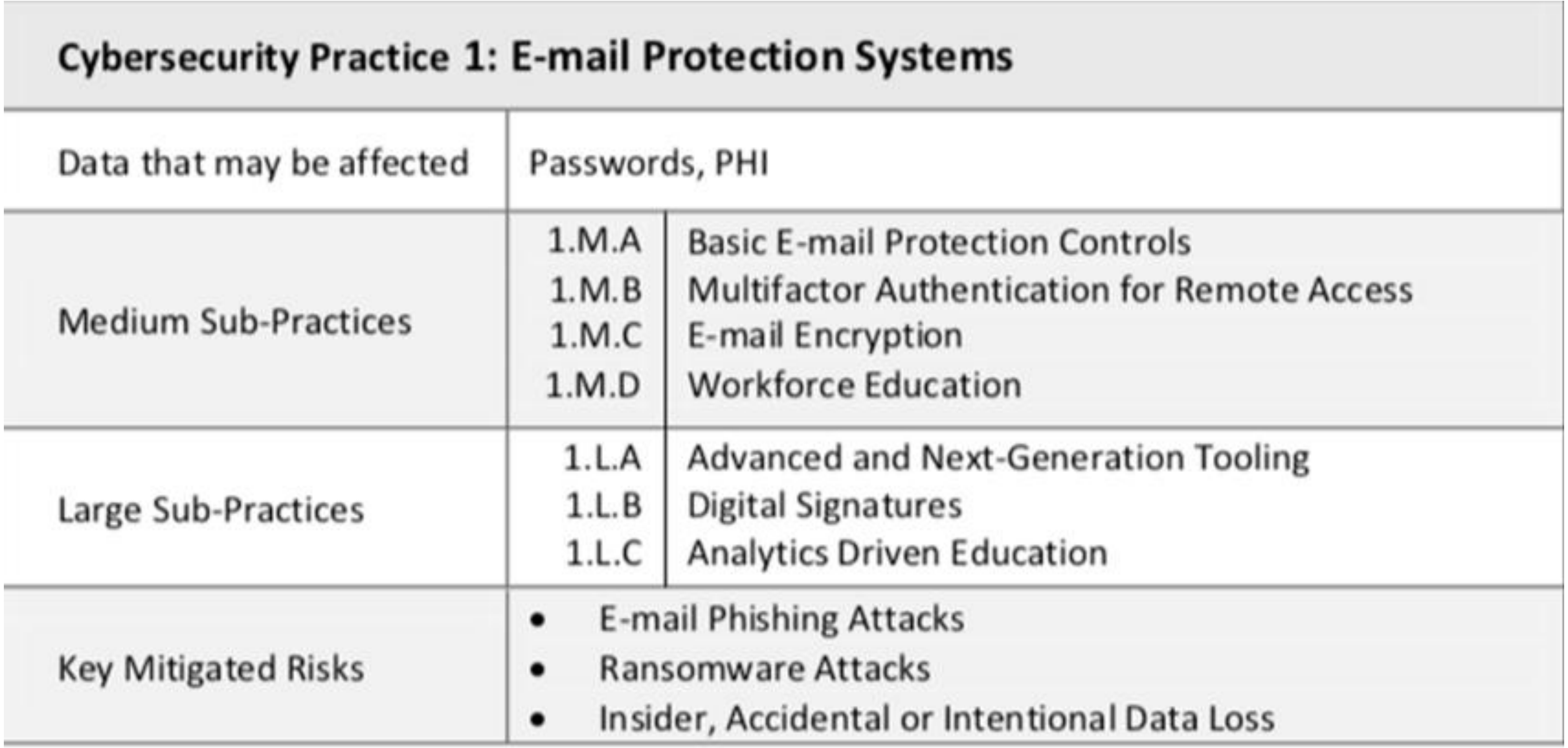
IMGBIN free image

Knowledge Check #5

- JR is a pharmacy technician in charge of preparing the deliveries to the patients' homes. Documentation on deliveries are registered and receipt certification are collected using an iPad®.
- JR car broke and he had to leave his car at the repair shop. By mistake, he left the iPad® in his car. He called the repair shop and secured the iPad® until he returned.

- What could happen?
- Why might it happen?
- What is the impact?

Cyber Security Practice Example-Risk Management-Mitigation



Cybersecurity Practice 1: E-mail Protection Systems		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	1.M.A	Basic E-mail Protection Controls
	1.M.B	Multifactor Authentication for Remote Access
	1.M.C	E-mail Encryption
	1.M.D	Workforce Education
Large Sub-Practices	1.L.A	Advanced and Next-Generation Tooling
	1.L.B	Digital Signatures
	1.L.C	Analytics Driven Education
Key Mitigated Risks	• E-mail Phishing Attacks • Ransomware Attacks • Insider, Accidental or Intentional Data Loss	

Examples of Practices to Combat Cyber Attacks

Cybersecurity Practice Administrative/Governance

- Develop policies and procedures
- Implement yearly, ongoing training
- Perform Risk Assessment
- Communication plan for cyber threat information sharing
- Implement proven and tested response procedures
- Implement incident response to manage successful cyber attacks

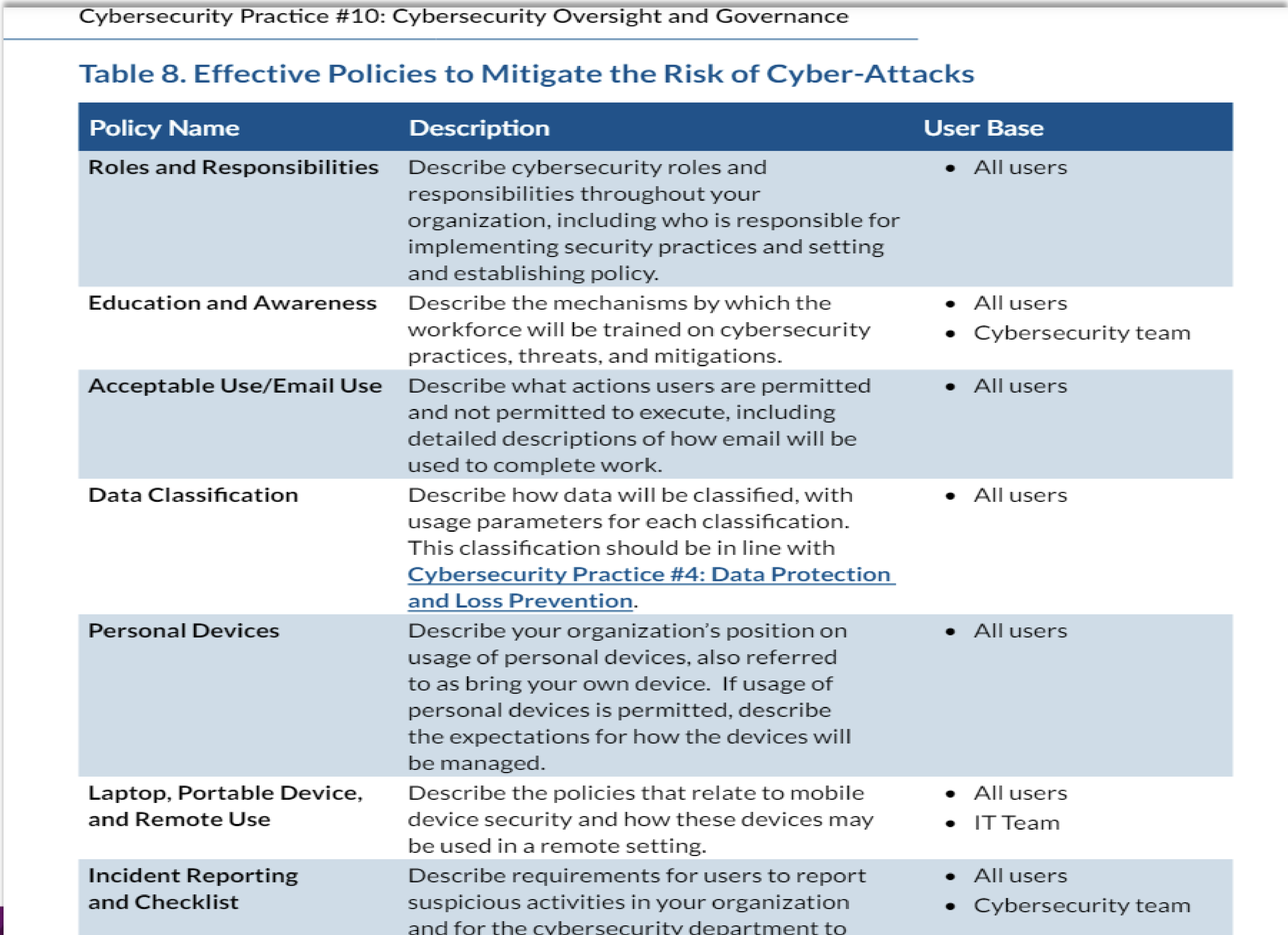
Knowledge Check #6

- You are a Supervisor at a hospital pharmacy. You delegated the first day of training of a new employee to one of your staff pharmacists.
- The staff pharmacist shared her password to provide the opportunity for the new employee to practice reviewing electronic orders.

- What happened?
- What normally happens?
- Is there room for a new procedure, or policy?

Example of the Use of Cybersecurity Practice-Policy Making

- Divulging your usernames and passwords.
- Downloading and installing software (this is the primary mechanism of installing malware or ransomware)
- Receiving and opening e mails
- Implement proven and tested response procedures when employees click on phishing emails
- Implement incident response plays to manage successful phishing attacks



Cybersecurity Practice #10: Cybersecurity Oversight and Governance

Table 8. Effective Policies to Mitigate the Risk of Cyber-Attacks

Policy Name	Description	User Base
Roles and Responsibilities	Describe cybersecurity roles and responsibilities throughout your 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 email 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: Data Protection and Loss Prevention.	• All users
Personal Devices	Describe your organization's position on usage of personal devices, also referred to as bring your own device. 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 • IT Team
Incident Reporting and Checklist	Describe requirements for users to report suspicious activities in your organization and for the cybersecurity department to	• All users • Cybersecurity team

Example of the Use of Cybersecurity Practice-Technology

Implement Multi-factor authentication (MFA)

- Tag external emails to make them as recognizable to staff.
- Implement advanced technologies for detecting and testing email for malicious content or links.

Knowledge Check #7

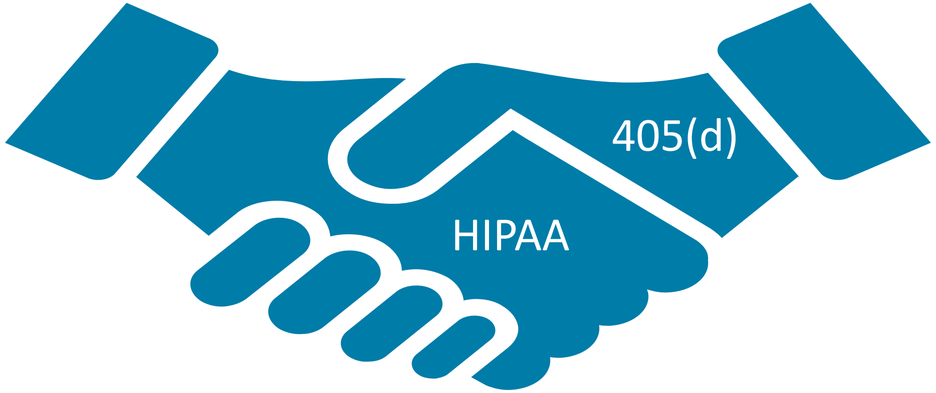
The healthcare provider discovered that a physician had accessed the medical records of celebrities and other patients without authorization. Dr. Zhou accessed the records of patients without authorization 323 times after learning that he would soon be dismissed.

Is this a HIPAA violation? A Cybersecurity violation?

HIPAA Law –Security Rule

405(d) versus HIPAA Security Rules

- Both have practices/standards that are flexible, voluntary.
- HIPAA have a series of “should” standards.
- Both are intended to protect the patients.
- 450(d) has an “enterprise” approach.
- HIPAA has a more “compliance” approach. (penalties and fines
- 405(d) reinforces/supplement HIPAA security rules.



HIPAA ePHI Rules

- General Rules
- Administrative safeguards
- Physical Safeguard
- Technical Safeguards
- Organization Requirements
- Policies and Procedures

Security standards: General rules

- Ensure the **confidentiality, integrity, and availability** of all ePHI that it creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats and hazards to the security or integrity of ePHI;
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

https://csrc.nist.gov/pubs/sp/800/66/r2/final

HIPAA Security Rule

Definitions

- Confidentiality – ePHI is not made available or disclosed to unauthorized persons or processes.
- Integrity- ePHI have not been altered or destroyed in an unauthorized manner.
- Availability- ePHI is accessible and useable upon demand by an authorized person.

General Rules

- Provides addressable implementation specifications.
- Requires the maintenance of security measures to continue reasonable and appropriate protection of ePHI

HIPAA Violations- Office of Civil Rights

Risk Analysis was not thorough

Lack of safeguards

Failure to report breach

Use and disclosure issues

Missing or deficient policies and procedures

Outdated or insufficient training

Inconsistent access monitoring

3rd party disclosure

Lost or stolen device – laptop, USB, smart phone

Lack of encryption

HHS's Office Settles Ransomware Cyber Attack Investigation. https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html

CASE: Doctors’ Management Services

- Best practices implemented to mitigate and prevent cyber-threats:
- Review all vendor and contractor relationships to ensure business associate agreements are in place.
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned.
- Ensure audit controls are in place to record and examine information system activity.
- Implement regular review of information system activity.
- Utilize multi-factor authentication to ensure only authorized users are accessing ePHI.
- Encrypt ePHI to guard against unauthorized access to ePHI.
- Incorporate lessons learned from incidents into the overall security management process.
- Provide training specific to organization and job responsibilities and on regular basis;

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/dms-ra-cap/index.html

Risk Analysis Failures Breach Penalties

- Steven A. Porter, M.D – $100,000 penalty for risk analysis and risk management failures.
- University of Massachusetts Amherst (UMass) – $650,000 penalty for risk management failures.
- Metro Community Provider Network – $400,000 penalty for risk management failures.
- Presence Health – $475,000 settlement for delaying the issuing of breach notifications by a month.

Cybersecurity Practice- Education

- Do you know the sender? If so, were you expecting the email?
- Are there any spelling or grammatical errors, or any other indicators that the tone or style of the email is off?
- Does the email have a sense of urgency or deadline to take an action?
- Before clicking on a link, did you hover over it to see the URL destination?
- If the link is to access the site of an account you have, did you go directly to the site instead of using the link to see if the information can be found directly on their site?
- Do you know the sender, or are you suspicious of the email?
- If in doubt, do NOT open any attachments. Whenever you receive an email that sounds too good to be true or that you were not expecting, verify it before opening it!
- Check with colleagues to find out whether they received the same suspicious email.

Knowledge Check #8

- You are the Pharmacy in Charge at the hospital. The Security officer in cooperation with the Human resource department oversee training new employees.
- Although the institutional training is comprehensive, would you consider offering your in-house training?

ASPH and APhA Statements on Cybersecurity

APhA and ASHP Statements on Cybersecurity

APhA

- Urges policymakers to closely examine the cause, along with patient and business impact, aftermath, responses, penalties, and legal consequences related to the system outages and make the necessary policy changes, including the following:
- Map out the pharmacy ecosystem to identify infrastructure vulnerabilities
- Incentivize minimum standards for cybersecurity
- Establish a federal cyber-insurance program
- Consider and appropriately fund cybersecurity within emergency preparedness and response procedures and practices across the count
- Increase the penalties for breaches and noncompliance.
- End vertical integration practices that result in health care market consolidation

ASHP

- Pause Audits: Health plans and PBM's should be prohibited from conducting audits or compliance reviews until the cyberattack has been resolved.
- Make Pharmacies Whole for Good Faith Dispensing: ASHP is concerned about the uncertainty of receiving reimbursement for a prescription filled in good faith to ensure patient continuity of care and safety.
- Provide Regulatory Flexibility: Exercise flexibility on enforcement until services are restored.
- Strongly advocate key decision-making roles for pharmacists in the planning, selection, design, implementation, and maintenance of medication-use information systems, electronic health records, computerized provider order entry.
- Urge hospitals and HS to involve department of pharmacy in performing appropriate risk assessment.

NCPA Statement of Record

- Include language that PDPs (and their subcontractors, such as PBMs) must communicate with pharmacies and other partners in the provider network within 24 hours of notification of a cyberattack and every 24 hours until essential functions are restored.

- Require PDPs to have their contingency plans posted on their public website, and in the event of a disaster/cyberattack, post the contingency plan and information about restoration of essential functions on their main home page (or linked to on home page)

- HHS should be acting as an immediate conduit for information, particularly for those people who are not included in the vendor-hosted calls or emails.

Policies and Procedures Already in Place?

- Facility security
- Workstation
- Restricting use of external drives
- Keeping passwords secure, do not share password
- Other policies
- Risk Analysis
- Incident response
- HIPAA security trainings.
- Cybersecurity trainings.

Conclusion

- Effective cybersecurity is a shared responsibility involving the people, processes, and technologies that protect digital data and technology investments.
- Cybersecurity requires a top-down approach.
- Cyber attacks are evolving, we need in our pharmacy role to constantly improve the cybersecurity defenses.
- Our priority is patient security.
- Securing our institutions guarantees continuity of health care.

Pre-post

Pre-Post #1

1. **Which of the following activities can cause data to be damaged or lost?**

a) Staying online too long

b) Never fully shutting your computer down

c) Unauthorized access to a system

d) Always keeping your computer charging

Pre-Post #2

2. Insider threats are people who:

a) Have legitimate access to computer systems and networks

b) Have relatives working in the same department.

c) People who are in their probationary period.

d) None of the above

Pre-Post #3

3. Data loss and data security is important but there is little I can do as an individual employee.

a) True

b) False

Pre-Post #4

4. MR is a pharmacist who works for a healthcare organization. Fifty per cent of the time the works remote. Which of the following can help to protect the data at work?

a) Do not plug an unknown USB drive into your computer.
b) Take advantage of security features.
c) Keep personal and business USB drives separate.
d) Disable Autorun.
e) Use and maintain security software and keep all software up to date.
f) All of the above

Pre-Post #5

5. There are increased cybersecurity risks to patient safety with network connected medical devices.

a) True

b) False

Pre-Post #6

6. Hackers like to use Social Engineering Techniques to trick you into making a security mistake. They do this by adding these words or phrases to a message. Select the answer from the list below.

a) Sending a message with a sense of urgency.
b) Including wording that says “quick, time is running out”
c) Mentioning an illness of a family member or friend
d) All of the above

Pre-Post #7

7. There are a few clues to look for if you suspect the e-mail you received is suspicious. Select all that apply.

a) The email contains several grammar and spelling errors.
b) You do not recognize the sender’s name or email.
c) The “from address” does not match the “sender” name.
d) Content with a sense of urgency
e) All of the above

Pre-Post #8

8. Cyber Security is Patient Safety

a) True

b) False

Pre-Post #9

9. Which is not considered a good practice when receiving emails?

a) Asking: Do I know the sender?
b) Asking: Are there any spelling or grammatical errors or any other indicators that the tone or style of the email is off?
c) Hover over it to identify the website address.
d) When in doubt, ask a colleague.

Pre-Post #10

10. The Cybersecurity Act of 2015

a) Promulgates best practices and methodologies to reduce cyber risks.

b) It is a team effort among various federal agencies and the public sector.

c) Applies only to the healthcare industry.

d) It is voluntary.

e) All of the above

References

APhA's cybersecurity recommendations to secure the pharmacy ecosystem and patient safety. Press Release. May 1, 2024. https://www.pharmacist.com/About/Newsroom/aphas-cybersecurity-recommendations-to-secure-the-pharmacy-ecosystem-and-patient-safety

ASPH. From the CEO. Change Healthcare Cyberattack: Preserving Continuity of Care and Preparing for Recovery. Posted March 1, 2024. https://www.ashp.org/about-ashp/ceo-blogs/recent-blogs/change-healthcare-cyberattack-preserving-continuity-of-care-and-preparing-for-recovery?loginreturnUrl=SSOCheckOnly

Examining the Change Healthcare Cyberattack. Testimony of Andrew Witty, Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations. May 1, 2024. https://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf

Guidance on Risk Analysis. HHS Office of Civil Rights (OCR). Last reviewed July 22, 2019. https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

HHS. Health Care and Public Health Sector Cybersecurity Framework Implementation Guide Version 2. March, 2023.

HHS. Health and Public Health Sector Coordinating Council. Public and Private Partnership. Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations. 2023 Edition.

HHS's Office Settles Ransomware Cyber Attack Investigation. https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html

IMB Security. Cost of a Data Breach Report, 2023.

Long, R The Risk Management Process: Manage Uncertainty, Then Repeat. https://www.mha-it.com/2020/01/29/risk-management/

Marron, F. National Institute Standards and Technology. Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. February 2024. Special Publication 800 NIST SP 800-66r2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf

Muha, B. What is the IoT? Introduction to the Internet of Things. Medium. 2019.

NCPA. Statement for the Record: The National Community Pharmacists Association. United States Senate Committee on Finance. May 1, 2024.

NIST SP 800-66r2 Implementing the HIPAA Security Rule February 2024 A Cybersecurity Resource Guide 10. https://csrc.nist.gov/pubs/sp/800/66/r2/final

Para obtener el certificado de Educación Continua

1. Log in en tu cuenta de **CFPR.org**
2. Click en **MI CUENTA**
3. Click en **HISTORIAL DE CURSOS**
4. Seleccionar el curso
5. Completar la evaluación y Prueba
6. Guardar o imprimir el Certificado

ACCESS CODE

CPE MONITOR

CODE

Tiena hasta el 5 de Octubre para
completer la evaluación y prueba
y poder obtener su certificado