



1



2



Karen Greenhalgh
karen@cybertygr.com

- Certified in Healthcare Privacy Compliance (CHPC)
- Certified in Healthcare Compliance (CHC)
- Healthcare Information Systems & Privacy Practitioner (HCISPP) ISC²
- Founder Cyber Tygr
- HHS led CISA 405(d) task group member
- Healthcare and Public Health Sector Coordinating Counsel Joint Cybersecurity
- NCHICA Privacy and Security Taskforce



**PROUD
MEMBER**



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

3

3



Erik Decker

- Chief Information Security and Privacy Officer
- Association for Executives in Healthcare Information Security (AEHIS)
- Co-Chair HHS 405(d) group
- HHS Joint Cyber Workgroup
- 2017 Chicago CISO of the Year



AT THE FOREFRONT
**UChicago
Medicine**

Information
Technology



**PROUD
MEMBER**



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

4

4

Agenda

- ▶ Why consider HICP?
- ▶ Challenges
- ▶ Dangers
- ▶ Solutions
- ▶ Introduce HICP
 - Top 5 Current Threats
 - 10 Mitigation Practices
- ▶ Resources and Templates
- ▶ Why adopt HICP?
- ▶ Questions



5

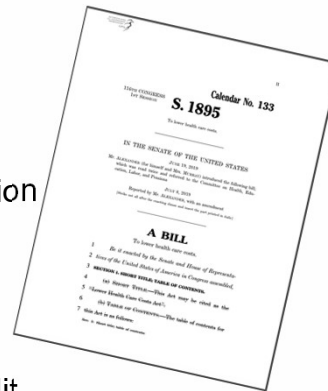


Why consider HICP?
cute name for a serious tool

6

Lower Health Care Costs Act – Section 502

- ▶ Senate Bill 1895
- ▶ 88% probability of passing
- ▶ Recognition of Security Practices
 - Approaches promulgated under section 405(d) of the Cybersecurity Act 2015
- ▶ Smoother Sailing
 - Mitigate fines
 - Early favorable termination of an audit
 - Limit remedies from HHS
- ▶ Documentation for 12 months



Enforcement Discretion Regarding HIPAA CMP

TABLE 1—PENALTY TIERS UNDER THE ENFORCEMENT RULE

Culpability	Minimum penalty/ violation	Maximum penalty/ violation	Annual limit
No Knowledge	\$100	\$50,000	\$1,500,000
Reasonable Cause	1,000	50,000	1,500,000
Willful Neglect—Corrected	10,000	50,000	1,500,000
Willful Neglect—Not Corrected	50,000	50,000	1,500,000

TABLE 2—PENALTY TIERS UNDER NOTIFICATION OF ENFORCEMENT DISCRETION

Culpability	Minimum penalty/ violation	Maximum penalty/ violation	Annual limit
No Knowledge	\$100	\$50,000	\$25,000
Reasonable Cause	1,000	50,000	100,000
Willful Neglect—Corrected	10,000	50,000	250,000
Willful Neglect—Not Corrected	50,000	50,000	1,500,000



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

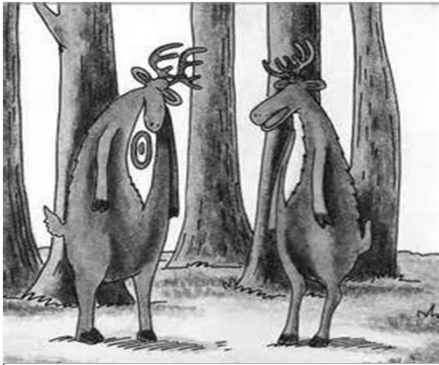
HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Healthcare Industry we have serious challenges

9


HEALTHCARE – HACKERS #1 TARGET



“FULLZ”
A compilation or package of information on a prospective fraud or identity theft victim.

- Most valuable record - \$500/record
- Least investment in cybersecurity
- Lack of qualified personnel
- Patient Safety Issues
- Medical Devices & IoT (Internet of Things)

“Bummer of a birthmark, Hal.”



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

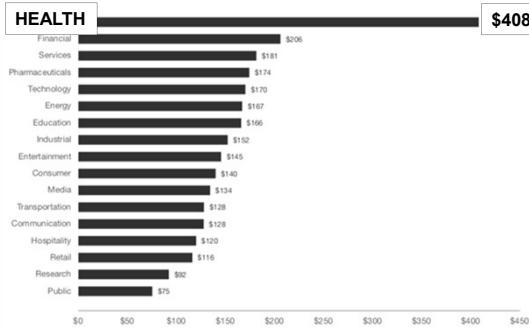
HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

10

Cost of a Data Breach – per record

Figure 7: Per capita cost by industry sector
Measured in US\$



- Civil Money Penalties
- Interrupt critical business operations
- Reduction in credit worthiness
- Reputation
- Loss of future business
- Patient Safety

2018 Cost of a Data Breach: Ponemon Institute



11

Churn Rates – loss of business

Figure 16: Abnormal churn rates by industry

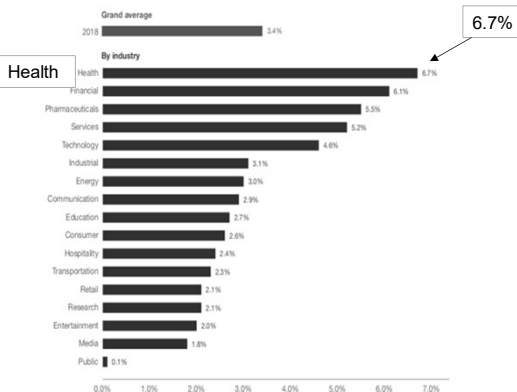
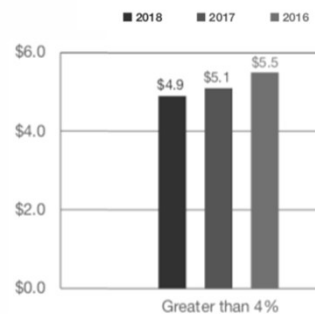


Figure 14: Average total cost by abnormal churn rate
Measured in US\$ millions



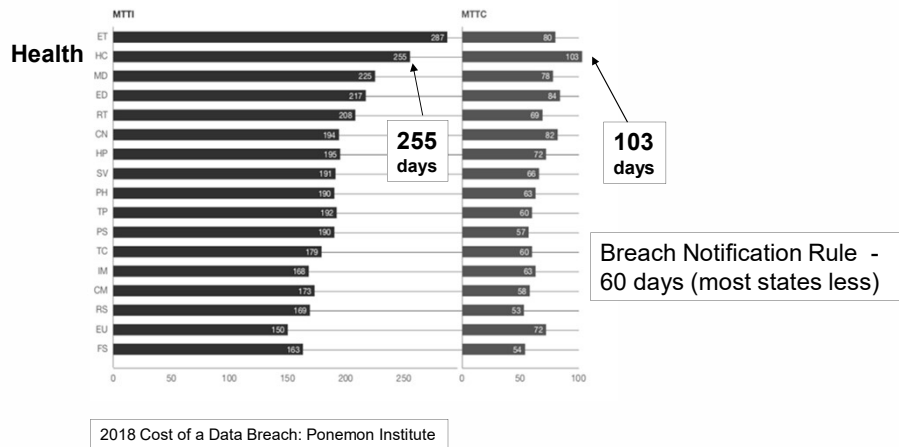
2018 Cost of a Data Breach: Ponemon Institute



12

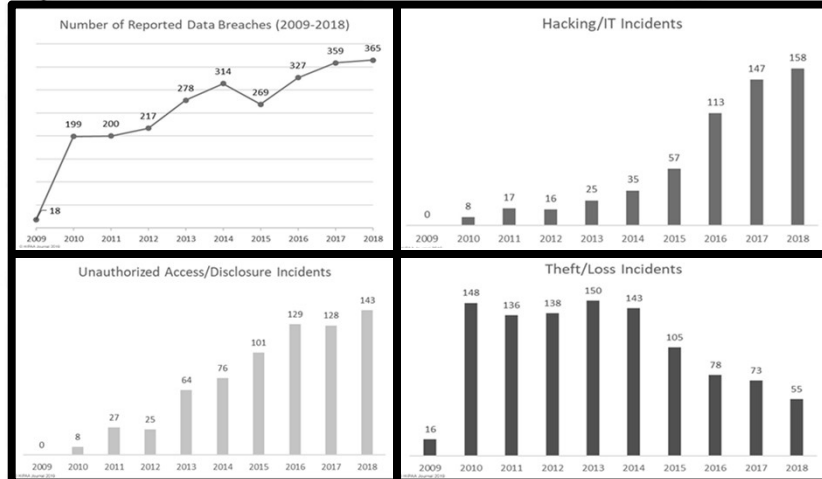
Identify & Contain – 358 days

Figure 26. Days to identify and contain the data breach by industry sector



Healthcare Breach and Incident Volumes

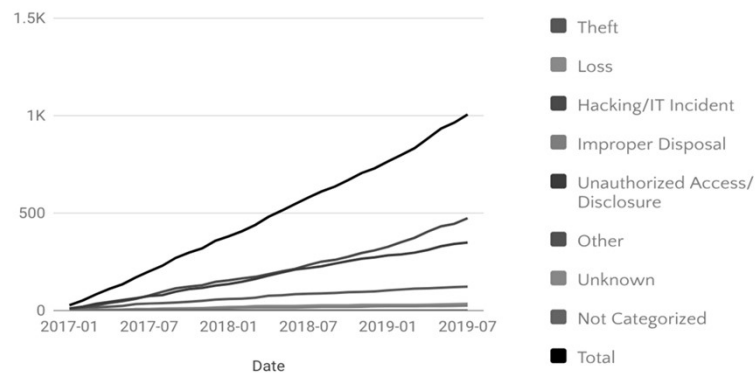
General Statistics



Healthcare Breaches

01/2017 – 07/2019

Cumulative Sum of Breaches By Month

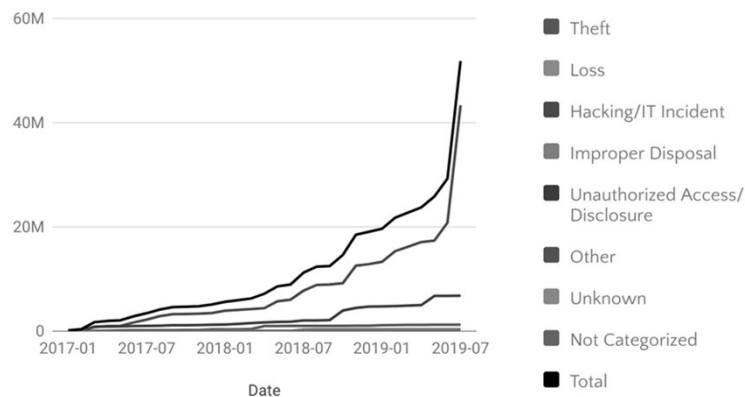


15

Healthcare Records Lost

2019 already double 2018 total – 32 Million Records

Cumulative Sum of Records Lost by Month 01/2017 – 07/2019



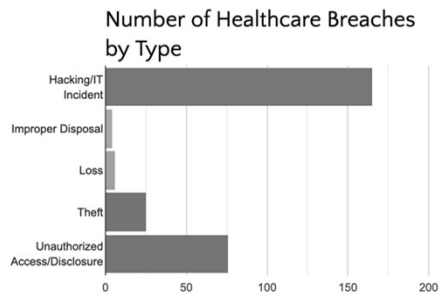
16

Healthcare Breach and Incident Volumes

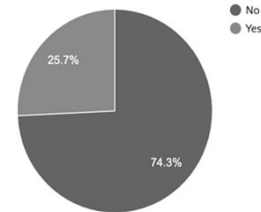
Jan – July 2019

NUMBER OF BREACHES
276

RECORDS LOST BY BUSINESS ASSOCIATES
23,269,686



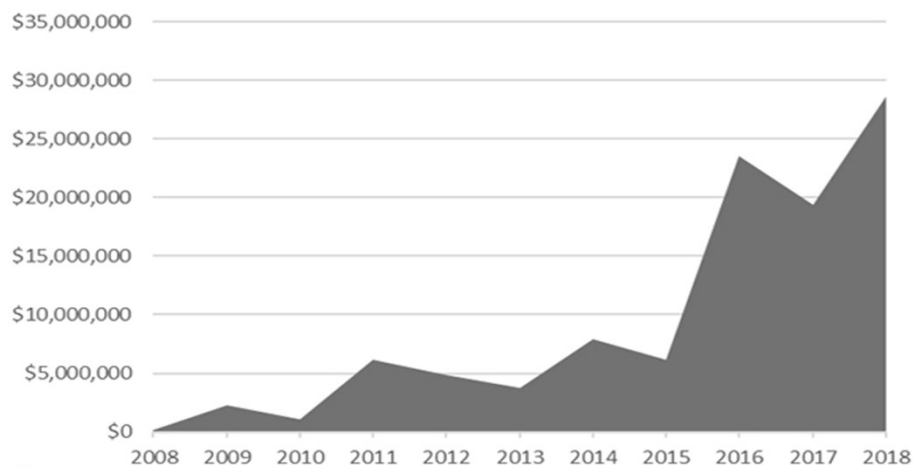
Was the Breach Caused by a Business Associate?



17

Healthcare Breach and Incident Volumes

Total HIPAA Penalty Amounts by Year



© HIPAA Journal 2019

18

Typical HIPAA Violations

1. Risk Analysis was not thorough
2. Lack of safeguards
3. Improper disposal
4. Business Associate Agreements
5. Missing or deficient policies and procedures
6. Failure to manage identified risk, e.g. encryption
7. No patching of software
8. 3rd party disclosure
9. Insider threat
10. Insufficient backup or contingency plan



It's NOT a suggestion...it's the law!

10/2/2019

19

19

Medical Device Vulnerabilities



SIEMENS Search for ...

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Security

Vulnerabilities Email Security Virus & Malware IoT Security Endpoint Security

Home > Virus & Threats

SSA-166  **Siemens Medical Products Affected by Wormable Windows Flaw** TXT

SSA-406 TXT

SSA-433 TXT

By Eduard Kovacs on May 28, 2019

SSA-832 [Share](#) [Tweet](#) [Recommend 0](#) [RSS](#) TXT

SSA-932 **Several products made by Siemens Healthineers, a Siemens company that specializes in medical technology, are affected by a recently patched Windows vulnerability tracked as CVE-2019-0708 and BlueKeep.** TXT

SSA-616 TXT

www.siemens.com/global/en/products/services/cert.html# < 1 >

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

20

Wicked Problem

1. Patient safety issue
2. No security agent
3. Unrecognized communication protocols
4. Default passwords & manufacturer remote access
5. Info sharing and vulnerability management
6. Large inventory - 14 medical devices per bed
7. Lack of inventory & configuration control
8. Legacy operating systems are vulnerable
9. Contains ePHI & lacks encryption
10. Network segmentation is intricate and expensive
11. Active scanning of device is danger to patient safety



Written by Bruce Schneier
Info Security Expert



21

Medical Device Security

- ▶ BlueKeep, Deja Blue, EternalBlue
 - Wormable Flaw
 - Similar Wannacry 2017
 - Common Vulnerability Score (CVSS) - Critical
 - Remote Desktop Protocol
 - Unprecedented Microsoft Upgrade – May 2019
 - Almost all versions of Windows
- ▶ Urgent 11
 - VxWorks
 - 2 billion medical and IoT devices
 - No authentication – remote code execution
- ▶ ECRI – scientific analysis
 - **25% of healthcare attacks** from RDP
 - **Connected Medical Device** #1 Hazard 2019
- ▶ Microsoft Ends Support Windows 7 and Mobile – Jan 2020
 - 71% of devices running unsupported Windows version in Jan 2020 (Forescout Healthcare Report)



22



23



24

HACKERS CONVENTIONS



25

 LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

Healthcare Industry
we need serious solutions


26

INSIDE CYBERSECURITY

DAILY NEWS


Senate panel eyes mandating use of NIST cyber framework following Equifax investigation

March 06, 2019 | Rick Weber



NIST CyberSecurity Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes & Procedures		Integration	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

27

27

NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY

NIST CSF

- ▶ Goal
 - Manage risk tolerance
 - Maturity level targeting
 - Implement controls & safeguards
- ▶ HHS supports to increase compliance

NIST Privacy Framework

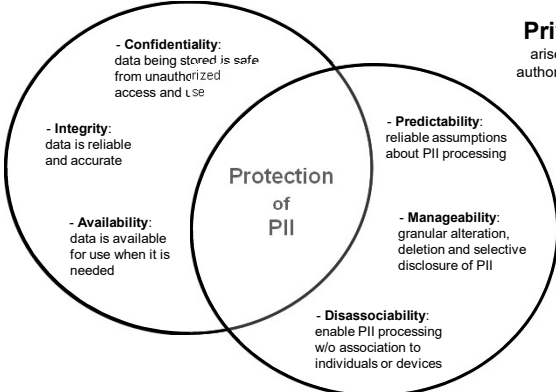
- ▶ Risk-based & Outcomes-based approach
- ▶ Preliminary Draft released September 2019
- ▶ New Functions: Govern, Control, Communicate
- ▶ Likelihood, Problematic Data Action, Impact

Security Risks

arise from unauthorized activity

Privacy Risks

arise as a byproduct of authorized data processing



28

NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY

CYBERSECURITY FRAMEWORK

Office for Civil Rights – Guidance

HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework

In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) as directed in Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The Cybersecurity Framework provides a voluntary, risk-based approach—based on existing standards, guidelines, and practices—to help organizations in any industry to direct their cybersecurity efforts. In the health care space, entities (covered entities and business associates) that create, receive, store, transmit, and manage cybersecurity risks. In the health care space, entities (covered entities and business associates) that create, receive, store, transmit, and manage cybersecurity risks. In the health care space, entities (covered entities and business associates) that create, receive, store, transmit, and manage cybersecurity risks.

Organizations that have already aligned their security programs to either the NIST Cybersecurity Framework or the HIPAA Security Rule may find this crosswalk helpful as a starting place to identify potential gaps in their programs. Addressing these gaps can bolster their **compliance with the Security Rule** and improve their ability to secure ePHI and other critical information and business processes.

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

29

29

DEPARTMENT OF HEALTH & HUMAN SERVICES - USA

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

HICP

Health Industry Cybersecurity Practices

30

15

Cybersecurity Act of 2015 (CSA)

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



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

31

31

405(c) Health Care Industry Cybersecurity Task Force Report

6 IMPERATIVES

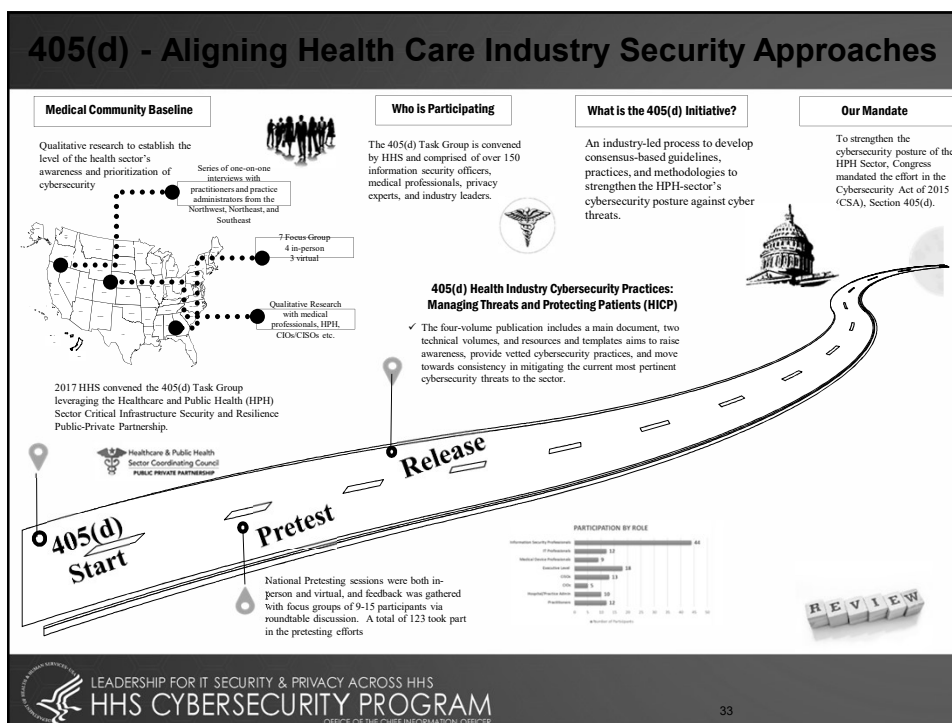
1. **NIST CSF for leadership and governance**
2. **Security and resilience increased**
 - ❖ medical devices & Health IT
3. **Improve information sharing**
 - ❖ threats, weaknesses, and mitigations
4. **Cybersecurity training & awareness**
5. **Develop workforce**
6. **Protect R&D and Intellectual Property**



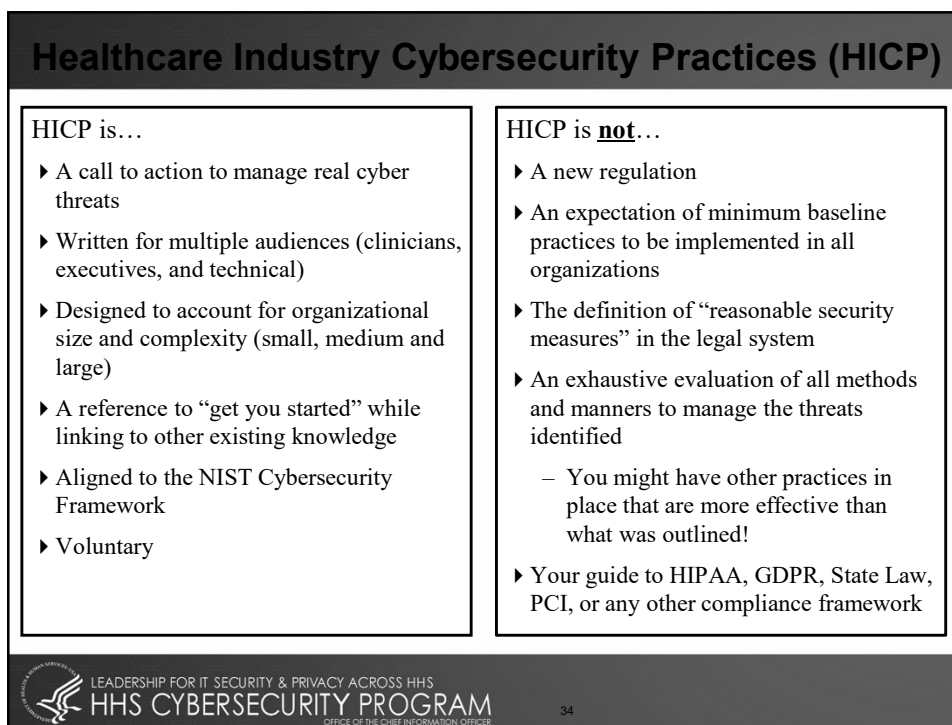
LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

32

32



33



34

Documentation Overview

► Main Document

- Industry cybersecurity threats and vulnerabilities
- Explores five (5) current threats
- Presents ten (10) practices to mitigate those threats

► Technical Volume 1

- Small healthcare organization
- Ten (10) detailed cybersecurity mitigation practices
- Nineteen (19) detailed sub-practices

► Technical Volume 2

- Medium and Large healthcare organizations
- Ten (10) detailed cybersecurity mitigation practices
- Seventy (70) detailed sub-practices

► Resources and Templates

- Mappings to the NIST Cybersecurity Framework
- An HICP assessment process
- Sample Templates
- Acknowledgements for its development.

5 Current Threats

1. Email Phishing 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



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

<https://www.cyberdygr.com/Resource.html>

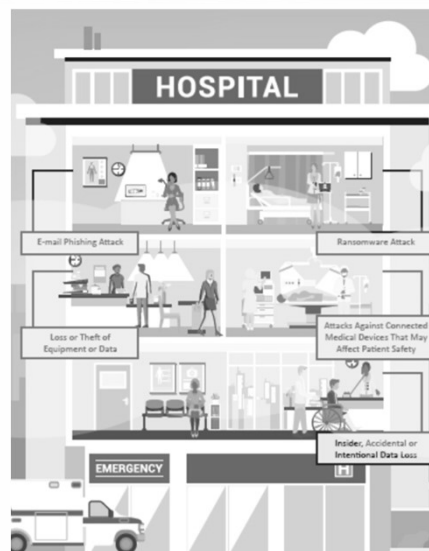
<https://www.phe.gov/405d>

35

35

Ten (10) Cybersecurity Mitigation Practices

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



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

36

36

Sub-Practices for Small Organizations

Cybersecurity Practice	Sub-Practice for Small Organizations	Page
E-mail Protection Systems	1.S.A E-mail System Configuration	6
	1.S.B Education	7
	1.S.C Phishing Simulation	7
Endpoint Protection Systems	2.S.A Basic Endpoint Protection	9
Access Management	3.S.A Basic Access Management	11
Data Protection and Loss Prevention	4.S.A Policy	13
	4.S.B Procedures	14
	4.S.C Education	15
Asset Management	5.S.A Inventory	16
	5.S.B Procurement	17
	5.S.C Decommissioning	17
Network Management	6.S.A Network Segmentation	18
	6.S.B Physical Security and Guest Access	18
	6.S.C Intrusion Prevention	19
Vulnerability Management	7.S.A Vulnerability Management	20
Incident Response	8.S.A Incident Response	21
	8.S.B ISAC/ISAO Participation	22
Medical Device Security	9.S.A Medical Device Security	23
Cybersecurity Policies	10.S.A Policies	24



A Thousand Words


[Main Document](#)

[Technical Volume 1](#)

[Technical Volume 2](#)

[Resources and Templates](#)





LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM


OFFICE OF THE CHIEF INFORMATION OFFICER

THREAT #1

E-Mail Phishing Attack & Mitigating Practices

39

Email Phishing – Small Organization



Cybersecurity Practice #1: E-mail Protection Systems

E-mail system configuration

Education

Phishing simulations

Cybersecurity Practice #8 Incident Response

ISAC/ISAO Participation

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.



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

40

E-Mail Phishing Mitigation Matrix Small Organization

Practice	Sub-Practice	To Consider	NIST Reference
<i>E-mail Protection Systems</i>	(1.S.A): E-mail System Configuration	<ul style="list-style-type: none"> 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
<i>Email Protection Systems</i>	(1.S.B): Education	<ul style="list-style-type: none"> 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
<i>Email Protection Systems</i>	(1.S.C): Phishing Simulations	<ul style="list-style-type: none"> Implement proven and tested response procedures when employees click on phishing e-mails 	NIST FRAMEWKORK REF: PR.AT
<i>Incident Response</i>	(8.S.B): ISAC/ISAO Participation	<ul style="list-style-type: none"> Establish cyber threat information sharing with other health care organizations 	NIST: DETECT - ID.RA-2



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

41

41

Email Phishing Medium/Large Organization

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



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

42

42

E-Mail Phishing Matrix Medium/Large Organization

Practice	Sub-Practice	To Consider	NIST Reference
<i>Email Protection Systems</i>	<i>(1.L.A): Advanced and Next-Generation Tooling</i>	<ul style="list-style-type: none"> Implement advanced technologies for detecting and testing e-mail for malicious content or links 	NIST FRAMEWORK REF: PR.DS-2, DE.CM-5, DE.CM-7
<i>Access Management</i>	<i>(3.M.D): Multifactor Authentication for Remote Access</i>	<ul style="list-style-type: none"> Implement multifactor authentication (MFA) 	NIST FRAMEWORK REF: PR.AC-3, PR.AC-7
<i>Incident Response</i>	<i>(8.M.A): Security Operations Center</i>	<ul style="list-style-type: none"> Implement incident response plays to manage successful phishing attacks 	NIST FRAMEWORK REF: RS.RP
<i>Incident Response</i>	<i>(8.M.C): Information Sharing and ISACs/ISAOs</i>	<ul style="list-style-type: none"> Establish cyber threat information sharing with other health care organizations 	NIST FRAMEWORK REF: ID.RA-2



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

43

43

Email Phishing - Mitigation Practice Metrics

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**:

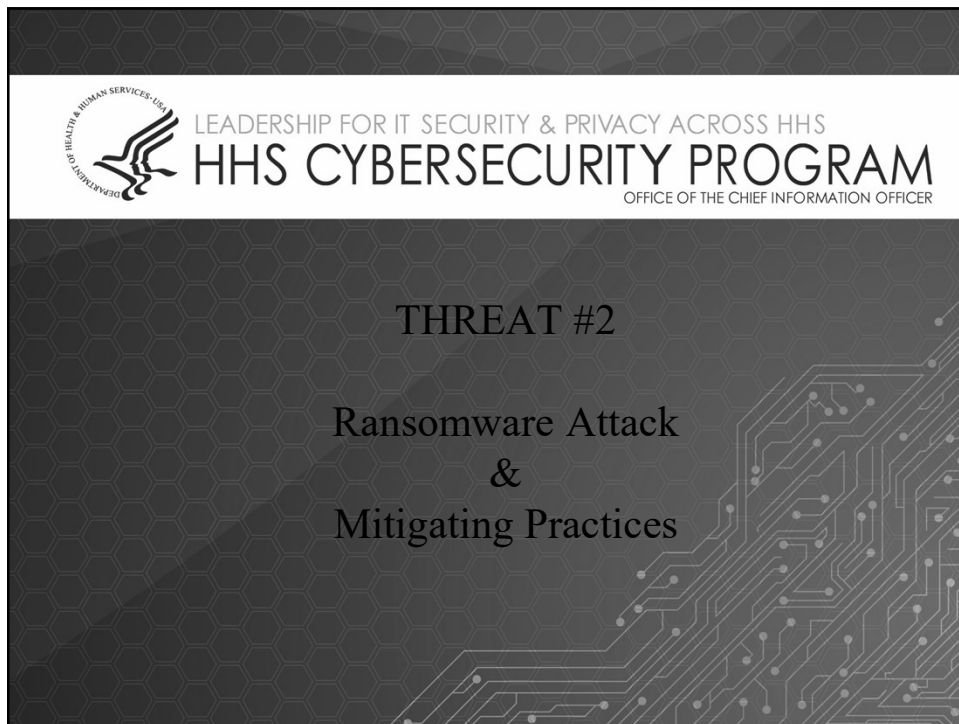
Malicious Phishing Attacks	Malicious URLs	Susceptible to Phishing	Malicious Websites
<ul style="list-style-type: none"> Number of malicious phishing attacks prevented on a weekly basis. The goal is to ensure that systems are working. A reduction in attacks prevented indicates system misconfiguration. Sudden changes in the rate of phishing attacks should trigger operational checks of to ensure that systems are still operating as intended. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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

44

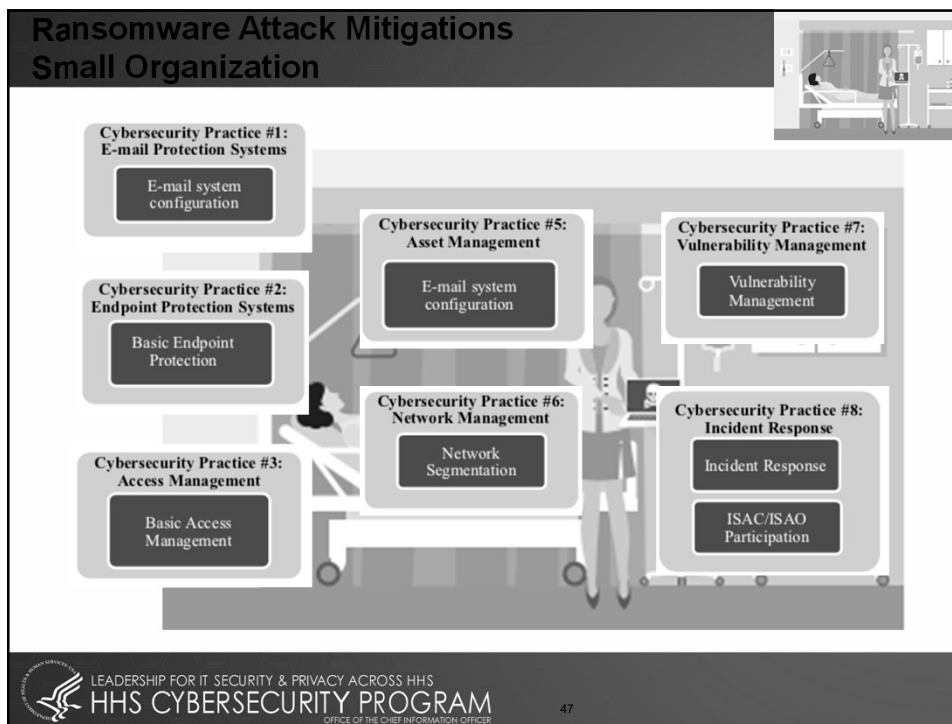
44



45



46



47

Ransomware Attack Mitigating Practices – Small Organizations

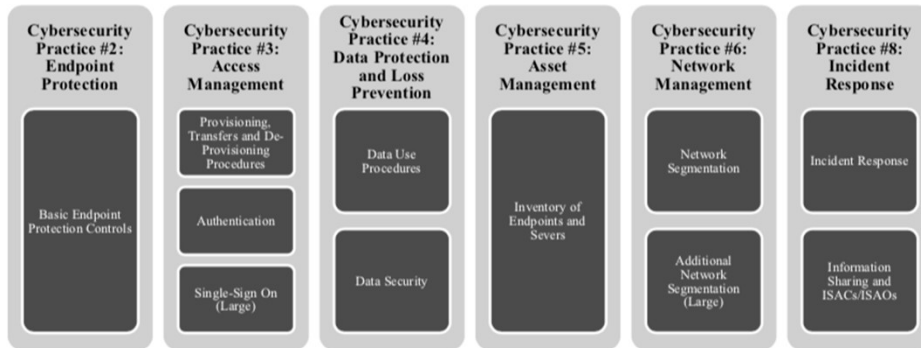
Threat 2: Ransomware Attack Sub-Practices for Small Organizations			
Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
1 – E-mail Protection Systems	1.S.A E-mail System Configuration	<ul style="list-style-type: none"> Use strong/unique username and passwords with MFA 	PR.DS-2, PR.IP-1, PR.AC-7
2 – Endpoint Protection Systems	2.S.A Basic Endpoint Protection	<ul style="list-style-type: none"> Deploy anti-malware detection and remediation tools 	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-3
3 – Access Management	3.S.A Basic Access Management	<ul style="list-style-type: none"> Limit users who can log in from remote desktops 	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-7
5 – Asset Management	5.S.A Inventory	<ul style="list-style-type: none"> Maintain a complete and updated inventory of assets 	ID.AM-1
6 – Network Management	6.S.A Network Segmentation	<ul style="list-style-type: none"> Separate critical or vulnerable systems from threats 	PR.AC-5, PR.AC-3, PR.AC-4, PR.PT-3
7 – Vulnerability Management	7.S.A Vulnerability Management	<ul style="list-style-type: none"> Ensure that users understand authorized patching procedures Patch software according to authorized procedures 	PR.IP-12
8 – Incident Response	8.S.A Incident Response	<ul style="list-style-type: none"> Implement proven and tested incident response procedures 	PR.IP-9
	8.S.B ISAC/ISAO Participation	<ul style="list-style-type: none"> Establish cyber threat information sharing with other health care organizations 	ID.RA-2

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

48

Ransomware Attack Mitigating Practices - Medium/Large Organizations

Ransomware Attack Practices in *Technical Volume 2* can be found in **Cybersecurity #2, #3, #4, #5, #6, & #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 is interested in adopting them.




49

Ransomware Attack 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. For example, the metrics for **Cybersecurity Practice #2: Endpoint Protection** can be found directly following the Sub-Practices for Large Organizations. Here are a few examples of the metrics discussed for Endpoint Protection Systems:

Percentage of Endpoints Encrypted 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 Nonhardened Images Each Month
<ul style="list-style-type: none"> The first goal is to achieve a high percentage of encryption, somewhere around 99 percent. Achieving 100 percent encryption is nearly impossible, because defects always exist. Additionally, the percentage of endpoints encrypted will vary as you discover new assets, which is why you should measure it weekly. 	<ul style="list-style-type: none"> The first goal is to achieve a high percentage of success. Secondary goals are to ensure that there are practices to patch endpoints for third-party and OS-level application vulnerabilities, and to be able to determine the effectiveness of those patches. Without the metric, there might not be checks and balances in place to ensure satisfactory compliance with expectations. 	<ul style="list-style-type: none"> The goal is to ensure that practices are in place to respond to AV alerts that are not automatically quarantined or protected. Such alerts indicate that there could be active malicious action on an endpoint. An endpoint with an active threat should be reimaged using general IT practices and managed using a ticketing system. 	<ul style="list-style-type: none"> The goal is to check assets for compliance with the full set of IT management practices, identifying assets that do not comply. To do this, place a key or token on the asset indicating that it is managed through a corporate image. Separate practices are necessary for assets that are not managed this way to ensure that they are properly hardened.

50



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM


OFFICE OF THE CHIEF INFORMATION OFFICER

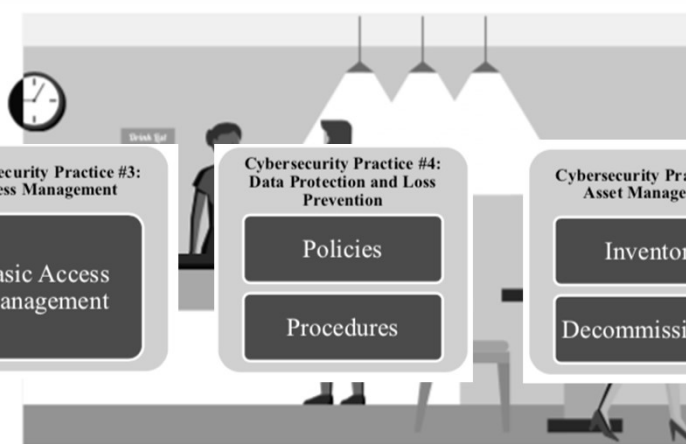
THREAT #3

Loss or Theft of Equipment or Data & Mitigating Practices

51

Loss or Theft of Data or Equipment Mitigating Practices – Small Organization





**Cybersecurity Practice #3:
Access Management**

Basic Access Management

**Cybersecurity Practice #4:
Data Protection and Loss Prevention**


Policies

Procedures

**Cybersecurity Practice #5:
Asset Management**

Inventory

Decommissioning



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

52

Loss or Theft of Data or Equipment Mitigating Practices – Small Organization

Cybersecurity Practice #3: Access Management

Basic Access Management

Basic Access Management

- Establish a unique account for each user
 - Assign a separate user account to each user in your organization. Train and regularly remind users that they must never share their passwords.
- Limit the use of shared or generic accounts
 - The use of shared or generic accounts should be avoided. If shared accounts are required, train and regularly remind users that they must sign out upon completion of activity or whenever they leave the device, even for a moment. Passwords should be changed after each use.
- Tailor access to the needs of each user
 - Tailor access for each user based on the user's specific workplace requirements. Most users require access to common systems, such as e-mail and file servers. Implementing tailored access is usually called *provisioning*.
- Terminate user access as soon as the user leaves the organization
 - When an employee leaves your organization, ensure that procedures are executed to terminate the employee's access immediately. This is very important for organizations that use cloud-based systems where access is based on credentials, rather than physical presence at a particular computer.
- Provide Role-Based access
 - Consider following the "minimum necessary" principle associated with the HIPAA Privacy Rule. Allow each user access only to the computers and programs required to accomplish that user's job or role in the organization.

53

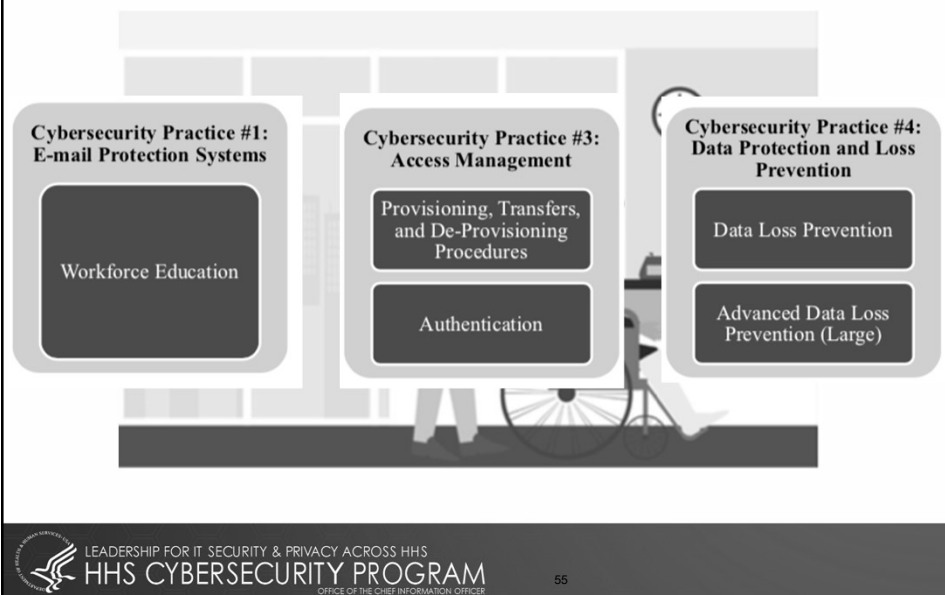


THREAT #4

Insider: Accidental or Intentional Data Loss & Mitigating Practices

54

Insider: Accidental or Intentional Attack Mitigations Medium/Large Organization




55

Insider, Accidental or Intentional Data Loss 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 **Cybersecurity Practice #4 Data Protection and Loss Prevention** can be found directly following the Sub-Practices for Large Organizations. Here are a few examples of the metrics discussed for Ransomware Attack:

Number of encrypted e-mail messages, trended by week	Number of blocked e-mail messages, trended by week	Number of files with excessive access on the file systems, trended by week	Number of unencrypted devices with access attempts, trended by week
<ul style="list-style-type: none"> The goal is to establish a baseline of encrypted messages sent. Be on the lookout for spikes of encryption (which could indicate data exfiltration) and no encryption (which could indicate that encryption is not working properly). 	<ul style="list-style-type: none"> The goal is to detect large numbers of blocked messages, which could indicate potential malicious data exfiltration or user training. 	<ul style="list-style-type: none"> The goal is to enact actions that limit access on the file storage systems to sensitive data, create tickets, and deliver to access management. 	<ul style="list-style-type: none"> The goal is to use this information to educate the workforce on the risks of removable media.

56



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM


OFFICE OF THE CHIEF INFORMATION OFFICER

THREAT # 5


Medical Device Security & Mitigating Practices

57

Perspectives on the Medical Device Security




"The glass is half full"




Info Technology

"The glass is half empty"




Info Security

"Who are you drinking with?"




Privacy Officer

"More dishes to wash?"




Clinical Engineering

"We purchased 50% too much glass"



CFO



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

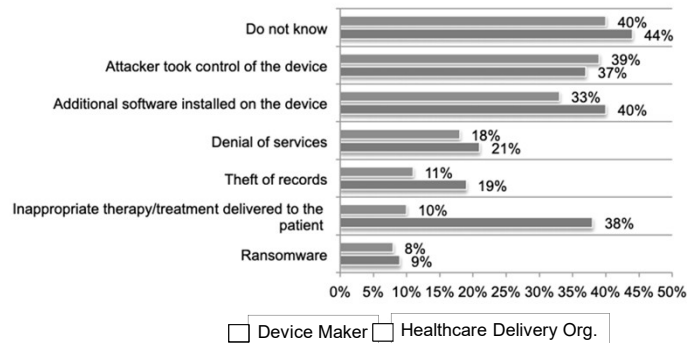
58

Hacking Medical Devices



Medical Device Security: An Industry Under Attack and Unprepared to Defend

Figure 3. If you are aware of an adverse event or harm, what was the cause?
More than one choice permitted



59

Medical Device Security Mitigating Practices for Medium/Large Organizations

Cybersecurity Practice #1: Email Protection

Advanced and Next
Generation Tooling

Cybersecurity Practice #9: Medical Device Security

Endpoint Protections

Identity and Access Management

Asset Management

Network Management

Vulnerability Management (Large)

Security Operations and Incident Response
(Large)

Procurement and Security Evaluations
(Large)

60

60



61

What Size is My Organization?

Implement resources and practices tailored and cost effective

Factors Determining Size:

- Health Information Exchanges
- IT Capability
- Cybersecurity Investment
- Size (provider)
- Size (acute/post-acute)
- Size (hospital)
- Complexity

Main Document – page 11

	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) ²⁵	1–50 beds	51–299 beds	Over 300 beds
Other Org Types	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated delivery networks Participate in accountable care organization or clinically integrated network
			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

DEPARTMENT OF HEALTH & HUMAN SERVICES USA

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

62

Prioritization Tool

► Approach

- Threat - apply combination of Practices and Sub-Practices
- Practice - applicable to multiple Threats

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

63

Assessment Methodology

Step	Analysis	Outcome
Step 1: Threat Assessment	Reviewed all threats. Threat most likely to occur is Phishing.	Determined that phishing attacks could cause the most damage to the organization. Start here.
Step 2: Review Practices	Reviewed all 10 Practices.	Identified three practices that would help mitigate this threat: Email Phishing Protection, Security Operations Center / Incident Response (SOC/IR), Policies and Procedures
Step 3: Determine Gaps	Reviewed the sub-practices identified within the three practices.	Email phishing protection controls are sufficient. No education or phishing simulation conducted.
Step 4: Identify Improvement Opportunities and Implement	Phishing education comes with no direct costs. Phishing simulations would be too expensive for the small practice.	Deferred the implementation of Phishing simulation. Established a workforce phishing education program and implemented.
Step 5: Repeat	Reviewed additional 4 threats, determined next most critical is ransomware.	Start the process anew.

64

Self Assessment - Practices & Sub Practices

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
2.M.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	Encryption at 80%, AV in place, baseline image, all users with admin rights	Encryption gaps and admin rights	Finish encryption, remove admin rights	High
3.M.A	Identity	Establish a unique identifier for all users, leveraging systems of record	All users provided accounts, not tied to ERP	No identity, can allow for orphaned accounts and failure to term	Establish identity program	Me
3.M.B	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination	User accounts created directly into Active Directory manually, when requested	Access rights might cumulate and administrators might fail to terminate access	Establish accounts based upon identity, automate provisioning and de-provisioning	Med
3.M.C	Authentication	Implement and monitor secure authentication for users and privileged accounts	Authentication bound to central authentication source	No gaps	No gaps	N/A
3.M.D	Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources	VPN access available, no MFA	No MFA enabled, which can allow for a theft of credentials to access sensitive data	Implement MFA	Med
8.M.A	Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks	Dedicated team to manage and respond to cyber incidents	No gaps	No Gaps	N/A
8.M.B	Incident Response	Establish formal incident response playbooks for responding to cyber attacks	Playbooks exist, but no playbook for lost/stolen device	In the case of a stolen device teams might not execute investigation properly	Establish playbook for stolen devices, get approval from leadership	High
8.M.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information	Not a current member of an ISAC/ISAO	By not participating in ISAC/ISAOs cyber teams might be missing out on leading practices	Join ISAC/ISAO	High

Cybersecurity Practices Assessment Toolkit



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

65

65

Resources - examples

My entity just experienced a cyber-attack! What do we do now? A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)

- **Link:** <https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf>
- **Description:** A checklist of things to do if your organization experiences a cyber-attack.
- **# of pages:** 2

Cyber-Attack Quick Response

- **Link:** <https://www.hhs.gov/sites/default/files/cyber-attack-quick-response-infographic.gif>
- **Description:** An infographic on responding to a cyber-attack.
- **# of pages:** 1

FACT SHEET: Ransomware and HIPAA

- **Link:** <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es>
- **Description:** A fact sheet on ransomware and HIPAA.
- **# of pages:** 8

Cybersecurity Awareness Training

- **Link:** <https://www.hhs.gov/sites/default/files/fy18-cybersecurityawarenesstraining.pdf>
- **Description:** Cybersecurity awareness training leveraged by HHS employees, contractors, interns, and other.
- **# of pages:** 61



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

66

66

HICP is a Cookbook!



So you want a recipe for Medium to Large Phish?

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)

The publication does not:

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

THE COOK MAKES THE DISH

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

CSA 405(d) - Looking Forward

- **Leading collaboration center for HHS Office of the CIO**
- **HICP**
 - **Update current information**
 - **Add additional detail**
- **405(d) Communications**
 - **Videos**
 - **Newsletter**
 - **How to guides (S,M,L)**
- **Enterprise Cybersecurity Risk Management**
 - **Leaderships role and impactful metrics**





Karen Greenhalgh:
Karen@CyberTygr.com

Erik Decker:
Erik.Decker@uchospitals.edu



Thank you for joining

Contact 405(d):
CISA405d@hhs.gov
phe.gov/405d

Proud Member of
HHS 405(d)
Aligning Health Care
Industry Security Approaches