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

IN PARTNERSHIP

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

HICP
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

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
Agenda

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

Why consider HICP?
cute name for a serious tool
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**

<table>
<thead>
<tr>
<th>Culpability</th>
<th>Minimum penalty/ violation</th>
<th>Maximum penalty/ violation</th>
<th>Annual limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Knowledge</td>
<td>$100</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>1,000</td>
<td>50,000</td>
<td>1,500,000</td>
</tr>
<tr>
<td>Wilful Neglect—Corrected</td>
<td>10,000</td>
<td>50,000</td>
<td>1,500,000</td>
</tr>
<tr>
<td>Wilful Neglect—Not Corrected</td>
<td>50,000</td>
<td>50,000</td>
<td>1,500,000</td>
</tr>
</tbody>
</table>

**Table 2—Penalty Tiers Under Notification of Enforcement Discretion**

<table>
<thead>
<tr>
<th>Culpability</th>
<th>Minimum penalty/ violation</th>
<th>Maximum penalty/ violation</th>
<th>Annual limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Knowledge</td>
<td>$100</td>
<td>$50,000</td>
<td>$25,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>1,000</td>
<td>50,000</td>
<td>100,000</td>
</tr>
<tr>
<td>Wilful Neglect—Corrected</td>
<td>10,000</td>
<td>50,000</td>
<td>250,000</td>
</tr>
<tr>
<td>Wilful Neglect—Not Corrected</td>
<td>50,000</td>
<td>50,000</td>
<td>1,500,000</td>
</tr>
</tbody>
</table>
Healthcare Industry
we have serious challenges

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.”
Cost of a Data Breach – per record

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

Churn Rates – loss of business

6.7%
**Identify & Contain – 358 days**

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

Healthcare Breach Notification Rule - 60 days (most states less)

2018 Cost of a Data Breach: Ponemon Institute

**Healthcare Breach and Incident Volumes**

General Statistics

Number of Reported Data Breaches (2009-2018)

Hacking/IT Incidents

Unauthorized Access/Disclosure Incidents

Theft/Loss Incidents

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
Healthcare Breaches

01/2017 – 07/2019

Cumulative Sum of Breaches By Month

- Theft
- Loss
- Hacking/IT Incident
- Improper Disposal
- Unauthorized Access/ Disclosure
- Other
- Unknown
- Not Categorized
- Total

Healthcare Records Lost

2019 already double 2018 total – 32 Million Records

Cumulative Sum of Records Lost by Month

- Theft
- Loss
- Hacking/IT Incident
- Improper Disposal
- Unauthorized Access/ Disclosure
- Other
- Unknown
- Not Categorized
- Total
**Healthcare Breach and Incident Volumes**

Jan – July 2019

- **NUMBER OF BREACHES:** 276
- **RECORDS LOST BY BUSINESS ASSOCIATES:** 23,269,686

**Number of Healthcare Breaches by Type**

- Hacking/Incident: 276
- Improper Disposal
- Loss
- Theft
- Unauthorized Access/Disclosure

**Was the Breach Caused by a Business Associate?**

- Yes: 74.3%
- No: 25.7%

**Healthcare Breach and Incident Volumes**

**Total HIPAA Penalty Amounts by Year**

- 2008: $0
- 2009: $0
- 2010: $0
- 2011: $0
- 2012: $0
- 2013: $0
- 2014: $0
- 2015: $0
- 2016: $0
- 2017: $5,000,000
- 2018: $35,000,000
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

Medical Device Vulnerabilities

Siemens Medical Products Affected by Wormable Windows Flaw

By Eduard Kavacs on May 28, 2019

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.
**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

**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)
Healthcare Industry
we face serious dangers

Outrunning the Bear
Healthcare Industry
we need serious solutions
Senate panel eyes mandating use of NIST cyber framework following Equifax investigation

March 06, 2019 | Rick Weber

NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY

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

HHS supports to increase compliance

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

NIST CSF
- Confidentiality: data being stored is safe from unauthorized access and use
- Integrity: data is reliable and accurate
- Availability: data is available for use when it is needed

NIST Privacy Framework
- Manageability: granular alteration, deletion and selective disclosure of PII
- Predictability: reliable assumptions about PII processing
- Disassociability: enable PII processing w/o association to individuals or devices

Privacy Risks
- arise as a byproduct of authorized data processing

Security Risks
- arise from unauthorized activity

Protection of PII
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.
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

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
Our Mandate

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

2017 HHS convened the 405(d) Task Group leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership.

An industry-led process to develop consensus-based guidelines, practices, and methodologies to strengthen the HPH-sector’s cybersecurity posture against cyber threats.

What is the 405(d) Initiative?

Qualitative Research with medical professionals, HPH, CIOs/CISOs etc.

Medical Community Baseline

- Qualitative research to establish the level of the health sector’s awareness and prioritization of cybersecurity
- States of one-on-one interviews, focus groups, surveys, and panel discussions with executives, operators, and industry leaders.

2017 HHS convened the 405(d) Task Group leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership.

Who is Participating

The 405(d) Task Group is comprised of over 150 information security officers, medical professionals, privacy experts, and industry leaders.

The four-volume publication includes a main document, two technical volumes, and resources and templates aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in mitigating the current most pertinent cybersecurity threats to the sector.

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

The four-volume publication includes a main document, two technical volumes, and resources and templates aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in mitigating the current most pertinent cybersecurity threats to the sector.

Healthcare Industry Cybersecurity Practices (HICP)

HICP is...

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

HICP is not...

- A new regulation
- An expectation of minimum baseline practices to be implemented in all organizations
- The definition of “reasonable security measures” in the legal system
- An exhaustive evaluation of all methods and manners to manage the threats identified
  - You might have other practices in place that are more effective than what was outlined!
- Your guide to HIPAA, GDPR, State Law, PCI, or any other compliance framework
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

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
### Sub-Practices for Small Organizations

<table>
<thead>
<tr>
<th>Cybersecurity Practice</th>
<th>Sub-Practice for Small Organizations</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail Protection Systems</td>
<td>1.5.A E-mail System Configuration</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>1.5.B Education</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>1.5.C Phishing Simulation</td>
<td>7</td>
</tr>
<tr>
<td>Endpoint Protection Systems</td>
<td>2.5.A Basic Endpoint Protection</td>
<td>9</td>
</tr>
<tr>
<td>Access Management</td>
<td>3.5.A Basic Access Management</td>
<td>11</td>
</tr>
<tr>
<td>Data Protection and Loss Prevention</td>
<td>4.5.A Policy</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>4.5.B Procedures</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>4.5.C Education</td>
<td>15</td>
</tr>
<tr>
<td>Asset Management</td>
<td>5.5.A Inventory</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>5.5.B Procurement</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>5.5.C Decommissioning</td>
<td>17</td>
</tr>
<tr>
<td>Network Management</td>
<td>6.5.A Network Segmentation</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>6.5.B Physical Security and Guest Access</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>6.5.C Intrusion Prevention</td>
<td>19</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>7.5.A Vulnerability Management</td>
<td>20</td>
</tr>
<tr>
<td>Incident Response</td>
<td>8.5.A Incident Response</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>8.5.B ISAC/ISAO Participation</td>
<td>22</td>
</tr>
<tr>
<td>Medical Device Security</td>
<td>9.5.A Medical Device Security</td>
<td>23</td>
</tr>
<tr>
<td>Cybersecurity Policies</td>
<td>10.5.A Policies</td>
<td>24</td>
</tr>
</tbody>
</table>
THREAT #1

E-Mail Phishing Attack & Mitigating Practices

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.
## E-Mail Phishing Mitigation Matrix

### Small Organization

<table>
<thead>
<tr>
<th>Practice</th>
<th>Sub-Practice</th>
<th>To Consider</th>
<th>NIST Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E-mail Protection Systems</strong></td>
<td>(1.S.A): E-mail System Configuration</td>
<td>• Tag external e-mails to make them recognizable to staff</td>
<td>NIST FRAMEWORK REF: PR.DS-2, PR.IP-1, PR.AC-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Implement multifactor authentication (MFA)</td>
<td></td>
</tr>
<tr>
<td><strong>Email Protection Systems</strong></td>
<td>(1.S.B): Education</td>
<td>• 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</td>
<td>NIST FRAMEWORK REF: PR.AT-1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Train staff to recognize suspicious e-mails and to know where to forward them</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Never open e-mail attachments from unknown senders</td>
<td></td>
</tr>
<tr>
<td><strong>Email Protection Systems</strong></td>
<td>(1.S.C): Phishing Simulations</td>
<td>• Implement proven and tested response procedures when employees click on phishing e-mails</td>
<td>NIST FRAMEWORK REF: PR.AT</td>
</tr>
<tr>
<td><strong>Incident Response</strong></td>
<td>(8.S.B): ISAC/ISAO Participation</td>
<td>• Establish cyber threat information sharing with other health care organizations</td>
<td>NIST: DETECT-ID.RA-2</td>
</tr>
</tbody>
</table>

### 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
## E-Mail Phishing Matrix
### Medium/Large Organization

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

---

### 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:

<table>
<thead>
<tr>
<th>Malicious Phishing Attacks</th>
<th>Malicious URLs</th>
<th>Susceptible to Phishing</th>
<th>Malicious Websites</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Number of malicious phishing attacks prevented on a weekly basis. The goal is to ensure that systems are working. A reduction in attacks prevents misconfiguration. Sudden changes in the rate of phishing attacks should trigger operational checks of to ensure that systems are still operating as intended.</td>
<td>• Number of malicious URLs discovered and prevented on a weekly basis. The goal is to measure the effectiveness of advanced tools, like click protection or attachment protection.</td>
<td>• 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 decrease the number of susceptible users with the number of malicious websites visited or the number of malicious URLs opened.</td>
<td>• 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.</td>
</tr>
</tbody>
</table>
THREAT #2
Ransomware Attack & Mitigating Practices

Ransomware Challenges
Ransomware-As-A-Service

Ransom Note Creator
Ransomware Attack Mitigations
Small Organization

Cybersecurity Practice #1: E-mail Protection Systems
- E-mail system configuration

Cybersecurity Practice #2: Endpoint Protection Systems
- Basic Endpoint Protection

Cybersecurity Practice #3: Access Management
- Basic Access Management

Cybersecurity Practice #4: Asset Management
- E-mail system configuration

Cybersecurity Practice #5: Asset Management
- E-mail system configuration

Cybersecurity Practice #6: Network Management
- Network Segmentation

Cybersecurity Practice #7: Vulnerability Management
- Vulnerability Management

Cybersecurity Practice #8: Incident Response
- Incident Response
- ISAC-ISAO Participation

Ransomware Attack Mitigating Practices – Small Organizations

<table>
<thead>
<tr>
<th>Cybersecurity Practice</th>
<th>Sub-Practice</th>
<th>To Consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - E-mail Protection Systems</td>
<td>1.5.A E-mail System Configuration</td>
<td>Use strong, unique passwords with MFA</td>
</tr>
<tr>
<td>2 - Endpoint Protection Systems</td>
<td>2.5.A Basic Endpoint Protection</td>
<td>Deploy anti-malware detection and remediation tools</td>
</tr>
<tr>
<td>3 - Access Management</td>
<td>3.3.A Basic Access Management</td>
<td>Limit users who can log in from remote devices</td>
</tr>
<tr>
<td>4 - Asset Management</td>
<td>5.5.A Inventory</td>
<td>Maintain a complete and updated inventory of assets</td>
</tr>
<tr>
<td>5 - Network Management</td>
<td>6.5.A Network Segmentation</td>
<td>Separate critical and vulnerable systems from threats</td>
</tr>
<tr>
<td>6 - Vulnerability Management</td>
<td>7.5.A Vulnerability Management</td>
<td>Ensure that users understand authorized patching procedures</td>
</tr>
<tr>
<td>7 - Incident Response</td>
<td>8.5.A Incident Response</td>
<td>Implement proven and tested incident response procedures</td>
</tr>
<tr>
<td>8 - ISAC-ISAO Participation</td>
<td>8.5.B ISAC-ISAO Participation</td>
<td>Establish cyber threat information sharing with other healthcare organizations</td>
</tr>
</tbody>
</table>
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.

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**
  - 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.

- **Percentage of Endpoints that Meet All Patch Requirements Each Month**
  - 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.

- **Percentage of Endpoints with Active Threats Each Week**
  - 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 remaged using general IT practices and managed using a ticketing system.

- **Percentage of Endpoints that Run Standardized Images Each Month**
  - 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.
THREAT #3

Loss or Theft of Equipment or Data
&
Mitigating Practices

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

THREAT #4
Insider: Accidental or Intentional Data Loss & Mitigating Practices
Insider: Accidental or Intentional Attack Mitigations
Medium/Large Organization

Cybersecurity Practice #1: E-mail Protection Systems
- Workforce Education

Cybersecurity Practice #3: Access Management
- Provisioning, Transfers, and De-Provisioning Procedures
- Authentication

Cybersecurity Practice #4: Data Protection and Loss Prevention
- Data Loss Prevention
- Advanced Data Loss Prevention (Large)

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:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of encrypted e-mail messages, trended by week</td>
<td>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).</td>
</tr>
<tr>
<td>Number of blocked e-mail messages, trended by week</td>
<td>The goal is to detect large numbers of blocked messages, which could indicate potential malicious data exfiltration or user training.</td>
</tr>
<tr>
<td>Number of files with excessive access on the file systems, trended by week</td>
<td>The goal is to enact actions that limit access on the file storage systems to sensitive data, create tickets, and deliver to access management.</td>
</tr>
<tr>
<td>Number of unencrypted devices with access attempts, trended by week</td>
<td>The goal is to use this information to educate the workforce on the risks of removable media.</td>
</tr>
</tbody>
</table>
THREAT # 5
Medical Device Security
& Mitigating Practices

Perspectives on the Medical Device Security

“The glass is half full”

“The glass is half empty”

“Who are you drinking with?”

“More dishes to wash?”

“We purchased 50% too much glass”
Hacking Medical Devices

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

- Do not know: 44%
- Attacker took control of the device: 37%
- Additional software installed on the device: 40%
- Denial of services: 21%
- Theft of records: 19%
- Inappropriate therapy/treatment delivered to the patient: 36%
- Ransomware: 9%

- Device Maker
- Healthcare Delivery Org.

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)
Resources and Templates

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

Table 1: Selecting the "Best Fit" for Your Organization
Prioritization Tool

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

### Select

<table>
<thead>
<tr>
<th>Threat</th>
<th>Practice</th>
<th>Sub-Practice</th>
<th>Relevant</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Email</td>
<td>Phishing</td>
<td>Medium</td>
<td>1</td>
</tr>
<tr>
<td>B</td>
<td>Ransomware</td>
<td>Attack</td>
<td>Medium</td>
<td>4</td>
</tr>
<tr>
<td>C</td>
<td>Loss</td>
<td>Theft of</td>
<td>Equipment</td>
<td>Medium</td>
</tr>
<tr>
<td>D</td>
<td>Insider</td>
<td>Accidental</td>
<td>or</td>
<td>Medium</td>
</tr>
<tr>
<td>E</td>
<td>Attacks</td>
<td>Against</td>
<td>Medical</td>
<td>Devices</td>
</tr>
</tbody>
</table>

### Assessment Methodology

<table>
<thead>
<tr>
<th>Step</th>
<th>Analysis</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Threat Assessment</td>
<td>Reviewed all threats. Threat most likely to occur is Phishing.</td>
<td>Determined that phishing attacks could cause the most damage to the organization. Start here.</td>
</tr>
<tr>
<td>Step 3: Determine Gaps</td>
<td>Reviewed the sub-practices identified within the three practices.</td>
<td>Email phishing protection controls are sufficient. No education or phishing simulation conducted.</td>
</tr>
<tr>
<td>Step 4: Identify Opportunities and Implement Improvement</td>
<td>Phishing education comes with no direct costs. Phishing simulations would be too expensive for the small practice.</td>
<td>Deferred the implementation of Phishing simulation. Established a workforce phishing education program and implemented.</td>
</tr>
<tr>
<td>Step 5: Repeat</td>
<td>Reviewed additional 4 threats, determined next most critical is ransomware.</td>
<td>Start the process anew.</td>
</tr>
</tbody>
</table>
## Self Assessment - Practices & Sub Practices

<table>
<thead>
<tr>
<th>Sub Practice Title</th>
<th>Short Description</th>
<th>Current State</th>
<th>Gaps</th>
<th>Action Plan</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.M.A Basic Endpoint Controls</td>
<td>Basic endpoint security controls to enable encryption of PHI data, baseline image, all users with admin rights</td>
<td>Encryption gaps and admin rights</td>
<td>Finish encryption, remove admin rights</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>3.M.A Identity</td>
<td>Establish a unique identifier for all users, leveraging systems of record</td>
<td>No identity, can allow for orphaned accounts and failure to term</td>
<td>Establish identity program</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>3.M.B Provisioning, Transfer, and De-provisioning Procedures</td>
<td>Provision user accounts based on identity, ensure de-provisioning upon termination</td>
<td>Access rights might cumulate and administrators might fail to terminate access</td>
<td>Establish accounts based upon identity, automate provisioning and de-provisioning</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>3.M.C Authentication</td>
<td>Implement and monitor secure authentication for users and privileged accounts</td>
<td>Authentication based on control authentication source</td>
<td>No gaps</td>
<td>No gaps</td>
<td>N/A</td>
</tr>
<tr>
<td>3.M.D Multi-Factor Authentication for Remote Access</td>
<td>Implement multi-factor authentication for remote access to resources</td>
<td>MFA access enabled, which can allow for a theft of credentials to access sensitive data</td>
<td>Implement MFA</td>
<td>Med</td>
<td></td>
</tr>
<tr>
<td>3.M.A Security Operations Center</td>
<td>Establish a SOC to prevent, discover and respond to cyber attacks</td>
<td>Dedicated team to manage and respond to cyber incidents</td>
<td>No gaps</td>
<td>No Gaps</td>
<td>N/A</td>
</tr>
<tr>
<td>3.M.B Incident Response</td>
<td>Establish formal incident response playbook for responding to cyber attacks</td>
<td>Playbooks exist, but no playbook for the organization</td>
<td>Establish playbook for stolen devices, get approval from leadership</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>3.M.C Information Sharing and M2M/I2I</td>
<td>Join security communities to share best practices and threat information</td>
<td>Not a current member of an IAC/I2I</td>
<td>Join IAC/I2I</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

Cybersecurity Practices Assessment Toolkit

---

## 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)

- **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](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=en](https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=en)
- **Description:** A fact sheet on ransomware and HIPAA.
- **# of pages:** 8

### Cybersecurity Awareness Training

- **Link:** [https://www.hhs.gov/sites/default/files/gy18-cybersecurityawarenesstraining.pdf](https://www.hhs.gov/sites/default/files/gy18-cybersecurityawarenesstraining.pdf)
- **Description:** Cybersecurity awareness training leveraged by HHS employees, contractors, interns, and other.
- **# of pages:** 61
HICP is a Cookbook!

So you want a recipe for Medium to Large Phish?
1. 5 oz of Basic Email 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
Thank you for joining

Karen Greenhalgh:
Karen@CyberTygr.com

Erik Decker:
Erik.Decker@uchospitals.edu

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