Health Industry Cybersecurity Practices
Managing Threats and Protecting Patients
HCCA - New Orleans Region
50,000 Hackers in Attendance
Medical Device Hackathon

Take part in finding vulnerabilities in these connected medical devices. Simply ask the staff to help you with a device and start working on it. Any vulnerabilities found should be disclosed to the vendor.
2017
• Windows Vulnerability
• 300,000 computers shut down
• One fifth of the UK Health System Shut Down

2020
• Urgent 11 – Sept 2019 (CVSS 9.8)
• BlueKeep – Wormable like Wannacry
• 49 Windows Vulnerabilities – Jan 2020
• Many more........
• COVID 19 – Healthcare Industry (Critical)

Lower Health Care Costs Act – Section 502

• Senate Bill 1895
• Recognition of Security Practices
  • Approaches promulgated under section 405(d) of the Cybersecurity Act 2015
• Reduce Breach Exposure
  • Mitigate fines
  • Early favorable termination of an audit
  • Limit remedies from HHS
• Documentation for 12 months
Healthcare – #1 Target

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

- Most costly across industry - $408
- Most valuable record for hackers - $500
- Highest “Churn Rate” due to breach
- Longest “Identify and Contain” times – 358 days
- Records breached in 2019 increased 300% - 41 million
- Fines and Fees hit $28m in 2019
- Least investment in cybersecurity
- Medical Devices Security = Patient Safety
“We’ve narrowed our security risks down to these two groups.”
Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients
“HICP”

• Co-founder Cyber Tygr
• 30 years experience in HIM
• Henry Ford Health System – Most Innovative Technology of the Year
• Healthcare Information Systems & Privacy Practitioner (HCISPP) ISC²
• HHS Joint Cybersecurity Workgroup
• NCHICA Biomedical Security Taskforce
• HHS led CISA 405(d) task group member
Agenda

- Top 5 Current Threats
- 10 Mitigation Practices
- Traveling the 405
- Resources and Templates
- Where is the 405 going
- Questions

Cybersecurity Act (CSA) 2015

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
CSA 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
4. Cybersecurity training & awareness
5. Develop workforce
6. Protect R&D and Intellectual Property

CSA 405(d)
Aligning Health Care Industry Security Approaches
• **HICP - Main Document**
  * Industry cybersecurity threats and vulnerabilities
  * Explores five (5) current threats
  * Presents ten (10) practices to mitigate those threats

• **HICP - Technical Volume 1**
  * Small healthcare organization
  * Ten (10) detailed cybersecurity mitigation practices
  * Nineteen (19) detailed sub-practices

• **HICP - Technical Volume 2**
  * Medium and Large healthcare organizations
  * Ten (10) detailed cybersecurity mitigation practices
  * Seventy (70) detailed sub-practices

• **HICP - Resources and Templates**
  * Mappings to the NIST Cybersecurity Framework
  * An HICP assessment process
  * Sample Templates

---

### Top 5 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**

---

### 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**
Top 5 Threats

Email Phishing Attack

- Spear Phishing
- Executive Whaling
- Social Engineering
- Malvertising

CURRENT ATTACK VECTOR:
COVID 19
#2 Threat

Ransomware

- Email
- Drive by Download
- Free Software
- Remote Desktop Protocol (RDP)
- Ransom - Bitcoin
- Held Hostage

Ransomware-As-A-Service
#3 Threat

**Loss or Theft of Equipment or Data**

- Laptops, drives, etc.
- Data sensitivity
- Business disruption

#4 Threat

**Insider – Accidental or Intentional Data Loss**

- Accidental Insider
  - Honest mistakes
  - Procedural errors
  - Emailing sensitive data

- Intentional Insider
  - Personal gain
  - Inflict harm
  - Impersonating staff
  - Disgruntled employee
Medical Device Security: Patient Safety

- Inventory control
- Software patches
- Device monitoring
- Remote access
- Anti-malware
- Urgent 11 – VxWorks OS
Top 10 Cybersecurity Practices

Doctors and nurses know that hand sanitizing is critical to prevent the spread of germs. That does not mean healthcare workers wash up as often as they should.

Similarly, cybersecurity practices reduce the risk of cyber-attacks and data breaches. Just as we are able to protect our patients from infection, we should all work towards protecting patient data to allow physicians and caregivers to trust the data and systems that enable delivery of quality health care.

---

Email Protection Systems

- Education
- Phishing Simulation
- E-mail Protection Controls
- Domain Key Identified Mail (DKIM)
- E-mail Encryption

#1 Practice
Endpoint Protection Systems

- Micro-segmentation
- Mobile Device Management
- Host Based Intrusion Detection/Prevention Systems
- Endpoint Detection and Response
- Application Whitelisting

#2 Practice

Access Management

- Identity
- Automate Provisioning
- Authentication
- Multifactor Authentication for Remote Access
- Single-Sign On

#3 Practice
Data Protection and Loss Prevention

- Policies & Procedures
- Classification of Data
- Data Use Procedures
- Data Security
- Backup Strategies
- Data Loss Prevention
- Mapping of Data Flows

#4 Practice

Asset Management

- Inventory Details
- Decommissioning
- Automated Discovery and Maintenance
- Procurement – HIC-SCRiM

https://healthsectorcouncil.org/hic-scrim/

#5 Practice
Network Management

#6 Practice

- Network Segmentation
- Physical Security
- Intrusion Prevention
- Network Profiles and Firewalls
- Network Access Control

Vulnerability Management

- Scanning
- Data Classification
- Patch Management
- Configuration Management
- Penetration Testing

#6 Practice
Incident Response

- Incident Response
- ISAC/ISAO Participation
- Security Operations Center (SOC)
- Baseline Network Traffic
- User Behavior Analytics
- Deception Technologies

#8 Practice

Medical Device Security

- Procurement and Security Evaluations
- Practice #2
- Practice #3
- Practice #5
- Practice #6
- Practice #7
- Practice #8
- Practice #10
- Contacting the FDA

#9 Practice
Cybersecurity Policies

- Policies

#10 Practice

Mitigating Email Phishing Recipe

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

Preheat your email system with some basic email protection controls, building a foundation for your dish. Mix in MFA for remote access, protecting against potential credential theft. Place in oven at high temp for incident response plan testing.

When finished baking sprinkle with additional tooling to provide next level protection to taste. Let cool several hours while providing the workforce training on reporting phishing attacks in the new system. Garnish with education on how digital signatures demonstrate authenticity of the sender.

Just like with any cookbook, the recipes provide the basic ingredients to making a meal. It does not instruct you how to cook, instruct you on what recipes to use or limit your ability for substitutions. The skill of the cook is what makes the dish!
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

What Size is My Organization?

Factors Determining Size:
– Health Information Exchanges
– IT Capability
– Cybersecurity Investment
– Size (provider)
– Size (acute/post-acute)
– Size (hospital)
– Complexity
Prioritization Tool

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

<table>
<thead>
<tr>
<th>Factor</th>
<th>Priority</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select your organization size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prioritize the threats (5 being highest priority, 1 being lowest priority)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A Email Phishing Attack</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>B Ransomware Attack</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>C Loss or Theft of Equipment or Data</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>D Insider; Accidental or Intentional Data Loss</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>E Attacks Against Connected Medical Devices that may affect Patient Safety</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

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

- Glossary of Terms
- NIST Cybersecurity Framework Crosswalk
- Assessment Methodology
- Toolkits

Examples
- Portable devices policy
- Incident response policy
- Access control procedure
- Security incident report sample
- Onboarding and Offboarding policy
- TECFA Do’s and Don’ts

405(d) Awareness Materials
The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! These 5 threat posters were created in support of Cybersecurity Awareness Month in October 2019 to be used in hospitals, doctor’s offices and even in email threads!

405(d) Outreach
The 405(d) Program produces Bi-monthly Newsletters and Spotlight Webinars to increase cybersecurity awareness. They also present on new emerging cybersecurity news and topics, to include highlighting the HICP Publication!

405(d) Social Media
The 405(d) Program is now live on Twitter, Instagram, and Facebook at @ask405d. Follow us to receive up to date 405(d) News and cybersecurity tips and practices!

Request materials – cisa405d@hhs.gov
HHS 405(d) Group

- 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)
- Executive Leadership’s role
- Impactful metrics

Resources and Solutions


Business Case for Medical Device Security
Free Medical Device Security ROI
https://cybertygr.com/connectedmd.html

Automatically Document Security Efforts
Governance, Risk & Compliance Software
https://cybertygr.com/hipaamanage.html

Ty Greenhalgh – Ty@CyberTygr.com