CIS Controls and the HPH

09/03/2020
Agenda

• Introduction
• Center for Internet Security (CIS)
• CIS Communities
• CIS Controls
• Conclusion
• Reference Materials
• Questions

Slides Key:

- Non-Technical: managerial, strategic and high-level (general audience)
- Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
CIS Controls:

- Provide a quick security win for the Healthcare and Public Health (HPH) Sector
- They offer an initial starting point for execution of a cyber security strategy
- They are scalable to meet the needs of the smallest to largest organizations
- Execution of the initial 43 sub-controls can defend against the five major cyber attacks and mitigates 62% of Mitre ATT&CK Techniques
Center for Internet Security (CIS)

- Community-driven nonprofit
- Maintains the CIS Controls and CIS Benchmarks
- Provides cloud-based CIS Hardened Images
- Home to MS-ISAC and EI-ISAC

The CIS Vision:

- “Leading the global community to secure our ever-changing connected world.”

The CIS Mission:

- “Our mission is to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.”

Figure source: Center for Internet Security
CIS Communities

**CIS Benchmarks™ Community**

- Over 100 configuration guidelines
  - Operating Systems
  - Server Software
  - Cloud Providers
  - Mobile Devices
  - Network Devices
  - Desktop Software
  - Multi-function Print Devices
- Across 25+ vendor product families
- Maintained by community volunteers

**CIS Controls® Community**

- 20 Security Controls
  - Six Basic Controls
  - Ten Foundational Controls
  - Four Organizational Controls
  - 171 sub-controls
- Initial application recommended according to organization’s Implementation Group (IG)
  - IG1, IG2, and IG3
- Maintained by community volunteers

Figure source: Center for Internet Security
Mission:
- “The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.”

Mission:
- “The mission of the EI-ISAC is to improve the overall cybersecurity posture of state, local, territorial, and tribal election offices, through collaboration and information sharing among members, the U.S. Department of Homeland Security and other federal partners, and private sector partners are the keys to success.”
### CIS Controls (cont.)

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>Tony Sager led release of NSA security guidance to public</td>
</tr>
<tr>
<td>2008</td>
<td>Sager led small group at NSA to determine where to get started with security</td>
</tr>
</tbody>
</table>
| 2009 | Picked up the Center for Strategic and International Studies and SANS Institute  
|      | Originally “The Consensus Audit Guidelines” => “SANS Top 20” |
| 2012 | Sager retires from NSA – Takes over SANS Top 20 at SANS |
| 2013 | Maintenance of Controls transferred to the Council on Cyber Security |
| 2015 | Maintenance of Controls transferred to the Center for Internet Security |
| 2019 | Current version 7.1 of Controls released in April 2019 |
## CIS Controls (cont.)

### Basic
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

### Foundational
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

### Organizational
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Figure source: Center for Internet Security
CIS Control 10: Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Why Is This CIS Control Critical?
When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker’s presence on the machine.
### CIS Control 10: Data Recovery Capabilities

<table>
<thead>
<tr>
<th>Sub-Control</th>
<th>Asset Type</th>
<th>Security Function</th>
<th>Control Title</th>
<th>Control Descriptions</th>
<th>Implementation Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Data</td>
<td>Protect</td>
<td>Ensure Regular Automated Backups</td>
<td>Ensure that all system data is automatically backed up on a regular basis.</td>
<td>1</td>
</tr>
<tr>
<td>10.2</td>
<td>Data</td>
<td>Protect</td>
<td>Perform Complete System Backups</td>
<td>Ensure that all of the organization’s key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.</td>
<td>2</td>
</tr>
<tr>
<td>10.3</td>
<td>Data</td>
<td>Protect</td>
<td>Test Data on Backup Media</td>
<td>Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.</td>
<td>3</td>
</tr>
<tr>
<td>10.4</td>
<td>Data</td>
<td>Protect</td>
<td>Protect Backups</td>
<td>Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.</td>
<td>1</td>
</tr>
<tr>
<td>10.5</td>
<td>Data</td>
<td>Protect</td>
<td>Ensure All Backups Have at Least One Offline Backup Destination</td>
<td>Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.</td>
<td>2</td>
</tr>
</tbody>
</table>

Figure source: Center for Internet Security
**CIS Control 10: Procedures and Tools**

Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

**CIS Control 10: System Entity Relationship Diagram**

Figure source: Center for Internet Security
IG1: Family-owned business with ten employees
IG2: Regional organization with hundreds of employees
IG3: Large corporation with thousands of employees

IG1 = 43 sub-controls
IG2 = 128 sub-controls
IG3 = 171 sub-controls

- Data Sensitivity / Criticality of Services
- Level of staff technical expertise
- Available resources

Figure source: Center for Internet Security
CIS Controls (cont.)

Figure source: Center for Internet Security
### CIS RAM: Risk Assessment Criteria

<table>
<thead>
<tr>
<th>Impact Score</th>
<th>Impact to Mission</th>
<th>Impact to Objectives</th>
<th>Impact to Obligations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Patients continue to access helpful information, and outcomes are on track.</td>
<td>Profits are on target.</td>
<td>Patients do not experience loss of service or protection.</td>
</tr>
<tr>
<td>2</td>
<td>Some patients may not get all the information they need as they request it.</td>
<td>Profits are off target, but are within planned variance.</td>
<td>Patients can experience financial losses, but not harm.</td>
</tr>
<tr>
<td>3</td>
<td>Some patients cannot access the information they need to maintain good health outcomes.</td>
<td>Profits are off planned variance and may take a fiscal year to recover.</td>
<td>Some patients may be harmed financially or reputationally after compromise of information or services.</td>
</tr>
<tr>
<td>4</td>
<td>Many patients consistently cannot access beneficial information.</td>
<td>Profits may take more than a fiscal year to recover.</td>
<td>Many patients may be harmed financially or reputationally.</td>
</tr>
<tr>
<td>5</td>
<td>We can no longer provide helpful information to remote patients.</td>
<td>The organization cannot operate profitably.</td>
<td>Some patients may be harmed financially, reputationally, or physically up to and including death.</td>
</tr>
</tbody>
</table>

#### Likelihood Score

<table>
<thead>
<tr>
<th>Score</th>
<th>Foreseeability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Not foreseeable. This is not plausible in the environment.</td>
</tr>
<tr>
<td>2</td>
<td>foreseeable. This is plausible, but not expected.</td>
</tr>
<tr>
<td>3</td>
<td>Expected. We are certain this will eventually occur.</td>
</tr>
<tr>
<td>4</td>
<td>Common. This happens repeatedly.</td>
</tr>
<tr>
<td>5</td>
<td>Current. This may be happening now.</td>
</tr>
</tbody>
</table>

Figure source: Center for Internet Security
CIS Controls (cont.)

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Figure source: Center for Internet Security
CIS Controls (cont.)

Identified 5 most important attack types:
• Web-Application Hacking
• Insider and Privilege Misuse
• Malware
• Ransomware
• Targeted Intrusions

Implementing only the 43 sub-controls in IG1 mitigated:
• All 5 attack types
• 62% of all Mitre ATT&CK Techniques

Definitions

CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3.

Figure source: Center for Internet Security
## CIS Controls (cont.)

<table>
<thead>
<tr>
<th>CIS Controls</th>
<th>Sub Controls</th>
<th>Asset Type</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.4</td>
<td>Devices</td>
<td>Maintain Detailed Asset Inventory</td>
</tr>
<tr>
<td>1</td>
<td>1.6</td>
<td>Devices</td>
<td>Address Unauthorized Assets</td>
</tr>
<tr>
<td>2</td>
<td>2.1</td>
<td>Applications</td>
<td>Maintain Inventory of Authorized Software</td>
</tr>
<tr>
<td>2</td>
<td>2.2</td>
<td>Applications</td>
<td>Ensure Software is Supported by Vendor</td>
</tr>
<tr>
<td>2</td>
<td>2.6</td>
<td>Applications</td>
<td>Address unapproved software</td>
</tr>
<tr>
<td>3</td>
<td>3.4</td>
<td>Applications</td>
<td>Deploy Automated Operating System Patch Management Tools</td>
</tr>
<tr>
<td>3</td>
<td>3.5</td>
<td>Applications</td>
<td>Deploy Automated Software Patch Management Tools</td>
</tr>
<tr>
<td>4</td>
<td>4.2</td>
<td>Users</td>
<td>Change Default Passwords</td>
</tr>
<tr>
<td>4</td>
<td>4.3</td>
<td>Users</td>
<td>Ensure the Use of Dedicated Administrative Accounts</td>
</tr>
<tr>
<td>5</td>
<td>5.1</td>
<td>Applications</td>
<td>Establish Secure Configurations</td>
</tr>
<tr>
<td>6</td>
<td>6.2</td>
<td>Network</td>
<td>Activate audit logging</td>
</tr>
<tr>
<td>7</td>
<td>7.1</td>
<td>Applications</td>
<td>Ensure Use of Only Fully Supported Browsers and Email Clients</td>
</tr>
<tr>
<td>7</td>
<td>7.7</td>
<td>Network</td>
<td>Use of DNS Filtering Services</td>
</tr>
<tr>
<td>8</td>
<td>8.2</td>
<td>Devices</td>
<td>Ensure Anti-Malware Software and Signatures are Updated</td>
</tr>
<tr>
<td>CIS Controls</td>
<td>Sub Controls</td>
<td>Asset Type</td>
<td>Title</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>8</td>
<td>8.4</td>
<td>Devices</td>
<td>Configure Anti-Malware Scanning of Removable Devices</td>
</tr>
<tr>
<td>8</td>
<td>8.5</td>
<td>Devices</td>
<td>Configure Devices Not To Auto-Run Content</td>
</tr>
<tr>
<td>9</td>
<td>9.4</td>
<td>Devices</td>
<td>Apply Host-Based Firewalls or Port Filtering</td>
</tr>
<tr>
<td>10</td>
<td>10.1</td>
<td>Data</td>
<td>Ensure Regular Automated BackUps</td>
</tr>
<tr>
<td>10</td>
<td>10.2</td>
<td>Data</td>
<td>Perform Complete System Backups</td>
</tr>
<tr>
<td>10</td>
<td>10.4</td>
<td>Data</td>
<td>Ensure Protection of Backups</td>
</tr>
<tr>
<td>10</td>
<td>10.5</td>
<td>Data</td>
<td>Ensure Backups Have At least One Non-Continuously Addressable Destination</td>
</tr>
<tr>
<td>11</td>
<td>11.4</td>
<td>Network</td>
<td>Install the Latest Stable Version of Any Security-Related Updates on All Network Devices</td>
</tr>
<tr>
<td>12</td>
<td>12.1</td>
<td>Network</td>
<td>Maintain an Inventory of Network Boundaries</td>
</tr>
<tr>
<td>12</td>
<td>12.4</td>
<td>Network</td>
<td>Deny Communication over Unauthorized Ports</td>
</tr>
<tr>
<td>13</td>
<td>13.1</td>
<td>Data</td>
<td>Maintain an Inventory of Sensitive Information</td>
</tr>
<tr>
<td>13</td>
<td>13.2</td>
<td>Data</td>
<td>Remove Sensitive Data or Systems Not Regularly Accessed by Organization</td>
</tr>
<tr>
<td>13</td>
<td>13.6</td>
<td>Data</td>
<td>Encrypt the Hard Drive of All Mobile Devices.</td>
</tr>
<tr>
<td>14</td>
<td>14.6</td>
<td>Data</td>
<td>Protect Information through Access Control Lists</td>
</tr>
<tr>
<td>CIS Controls</td>
<td>Sub Controls</td>
<td>Asset Type</td>
<td>Title</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>15</td>
<td>15.7</td>
<td>Network</td>
<td>Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data</td>
</tr>
<tr>
<td>15</td>
<td>15.1</td>
<td>Network</td>
<td>Create Separate Wireless Network for Personal and Untrusted Devices</td>
</tr>
<tr>
<td>16</td>
<td>16.8</td>
<td>Users</td>
<td>Disable Any Unassociated Accounts</td>
</tr>
<tr>
<td>16</td>
<td>16.9</td>
<td>Users</td>
<td>Disable Dormant Accounts</td>
</tr>
<tr>
<td>16</td>
<td>16.11</td>
<td>Users</td>
<td>Lock Workstation Sessions After Inactivity</td>
</tr>
<tr>
<td>17</td>
<td>17.3</td>
<td>N/A</td>
<td>Implement a Security Awareness Program</td>
</tr>
<tr>
<td>17</td>
<td>17.5</td>
<td>N/A</td>
<td>Train Workforce on Secure Authentication</td>
</tr>
<tr>
<td>17</td>
<td>17.6</td>
<td>N/A</td>
<td>Train Workforce on Identifying Social Engineering Attacks</td>
</tr>
<tr>
<td>17</td>
<td>17.7</td>
<td>N/A</td>
<td>Train Workforce on Sensitive Data Handling</td>
</tr>
<tr>
<td>17</td>
<td>17.8</td>
<td>N/A</td>
<td>Train Workforce on Causes of Unintentional Data Exposure</td>
</tr>
<tr>
<td>17</td>
<td>17.9</td>
<td>N/A</td>
<td>Train Workforce Members on Identifying and Reporting Incidents</td>
</tr>
<tr>
<td>19</td>
<td>19.1</td>
<td>N/A</td>
<td>Document Incident Response Procedures</td>
</tr>
<tr>
<td>19</td>
<td>19.3</td>
<td>N/A</td>
<td>Designate Management Personnel to Support Incident Handling</td>
</tr>
<tr>
<td>19</td>
<td>19.5</td>
<td>N/A</td>
<td>Maintain Contact Information For Reporting Security Incidents</td>
</tr>
<tr>
<td>19</td>
<td>19.6</td>
<td>N/A</td>
<td>Publish Information Regarding Reporting Computer Anomalies and Incidents</td>
</tr>
</tbody>
</table>
Conclusion

HPH Sector:
• Comprised of organizations of various sizes, budgets, IT-experience, and data

• According to the Verizon DBIR, in 2019:
  • Over 41 million patient records lost in breaches
  • 3.8 million employee-related incidents affecting patient data

CIS Controls:
• They offer an initial starting point for execution of a cyber security strategy

• They are scalable to meet the needs of the smallest to largest organizations

• Execution of the initial 43 sub-controls can defend against the five major cyber attacks and mitigates 62% of Mitre ATT&CK Techniques

• Provide a quick security win for the Healthcare and Public Health (HPH) Sector

Figure source: Center for Internet Security
Reference Materials
References

- Center for Internet Security
  - https://www.cisecurity.org/
- Cybersecurity Best Practices
  - https://www.cisecurity.org/cybersecurity-best-practices/
- CIS Communities
  - https://www.cisecurity.org/communities/
- CIS Benchmarks
  - https://www.cisecurity.org/cis-benchmarks/
- The 20 CIS Controls & Resources
  - https://www.cisecurity.org/controls/cis-controls-list/
- MS-ISAC
  - https://www.cisecurity.org/ms-isac/
- EI-ISAC
  - https://www.cisecurity.org/ei-isac/
- Cleaning Up a Definition of Basic Cyber Hygiene
  - https://www.cisecurity.org/blog/cleaning-up-a-definition-of-basic-cyber-hygiene/
- CIS Blog
  - https://www.cisecurity.org/resources/?type=post
References (cont.)

• Verizon 2020 Data Breach Investigations Report (DBIR)

• Tony Sager of CIS on the Origin and Importance of Critical Security Controls
  • https://www.youtube.com/watch?v=SyLSA8kxV8Q

• Cleaning Up Our Cyber Hygiene
  • https://www.sans.org/webcast/recording/citrix/115955/252745

• CIS RAM Webinar
Questions
Questions

Upcoming Briefs

• Fileless Malware (9/10)
• Malspam (9/17)

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.
HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

**Products**

**Sector & Victim Notifications**
Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

**White Papers**
Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

**Threat Briefings & Webinar**
Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to [HC3@HHS.GOV](mailto:HC3@HHS.GOV) or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Visit us at: [www.HHS.Gov/HC3](http://www.HHS.Gov/HC3)
Contact

www.HHS.GOV/HC3  (202) 691-2110  HC3@HHS.GOV