LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Laying a Strong Cyber Foundation for the HPH

01/21/2021

TLP: WHITE, ID# ***202101211030***

Agenda

- Introduction
- Center for Internet Security (CIS)
- CIS Controls
- Implementation Groups
- Conclusion
- Reference Materials
- Questions

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Introduction

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 were lost in breaches
- 3.8 million employee-related incidents affected patient data

Source: gettyimages.com

CynergisTek 2020 Report:

- Assessed almost 300 healthcare facilities
- Only 45 percent conformed to the NIST Cybersecurity Framework

Healthcare cybersecurity budgets:

- 4 to 7 percent compared to as much as 15 percent in the Finance industry

CIS Controls:

- Offer an initial starting point for execution of a cyber security strategy, and are scalable
- Provide a quick security win for the HPH Sector

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:

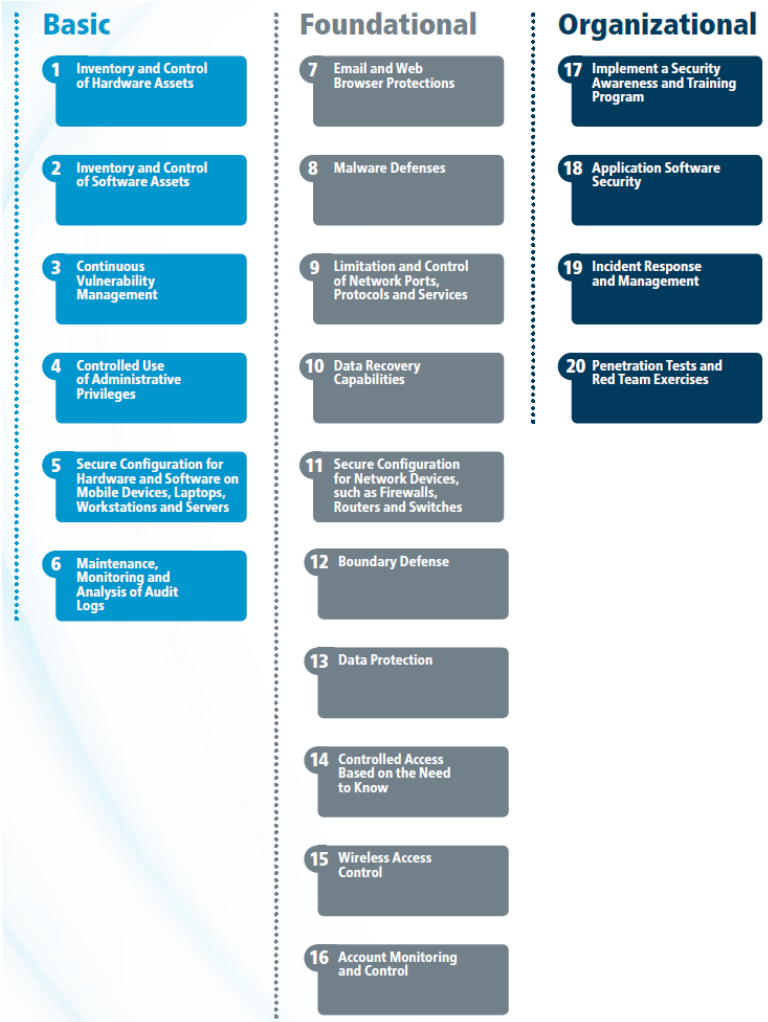
- "Our mission is to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats."

Source: Center for Internet Security

CIS Controls® Community

Source: Center for Internet Security

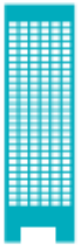
- 20 Security Controls
  - Six Basic Controls
  - Ten Foundational Controls
  - Four Organizational Controls
  - 171 sub-controls
- Maintained by community volunteers
- They offer an initial starting point for execution of a cyber security strategy
- They are scalable to meet the needs of the smallest to largest organizations



Source: Center for Internet Security

Implementation Groups

- IG1: Family-owned business with ten employees
- IG2: Regional organization with hundreds of employees
- IG3: Large corporation with thousands of employees



Implementation Group 3
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

Implementation Group 2
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 1
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

Source: Center for Internet Security

- IG1 = 43 sub-controls
- IG2 = 128 sub-controls (+85)
- IG3 = 171 sub-controls (+43)

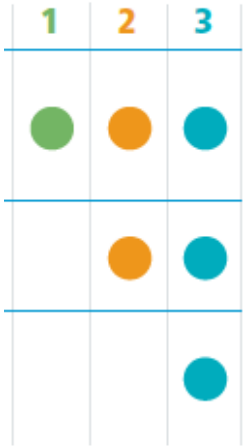
- Data Sensitivity / Criticality of Services
- Level of staff technical expertise
- Available resources

Implementation Groups (cont.)

CIS Sub-Control / CIS Control Title	Implementation Groups 1	2	3
CIS Control 1: Inventory and Control of Hardware Assets			
1.1 Utilize an Active Discovery Tool		●	●
1.2 Use a Passive Asset Discovery Tool			●
1.3 Use DHCP Logging to Update Asset Inventory		●	●
1.4 Maintain Detailed Asset Inventory	●	●	●
1.5 Maintain Asset Inventory Information		●	●
1.6 Address Unauthorized Assets	●	●	●
1.7 Deploy Port Level Access Control		●	●
1.8 Utilize Client Certificates to Authenticate Hardware Assets			●
CIS Control 2: Inventory and Control of Software Assets			
2.1 Maintain Inventory of Authorized Software	●	●	●
2.2 Ensure Software Is Supported by Vendor	●	●	●
2.3 Utilize Software Inventory Tools		●	●
2.4 Track Software Inventory Information		●	●
2.5 Integrate Software and Hardware Asset Inventories			●
2.6 Address Unapproved Software	●	●	●
2.7 Utilize Application Whitelisting			●
2.8 Implement Application Whitelisting of Libraries			●
2.9 Implement Application Whitelisting of Scripts			●
2.10 Physically or Logically Segregate High Risk Applications			●

1-6 Basic

Source: Center for Internet Security



Source: Center for Internet Security

CIS Controls™ V7.1

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

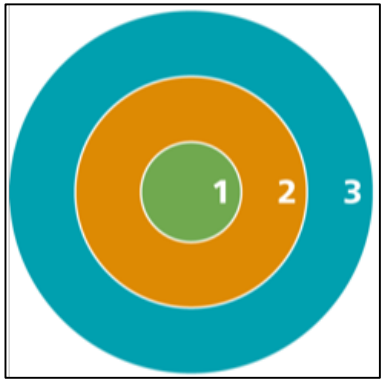
Foundational

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

Source: Center for Internet Security



Source: Center for Internet Security

Definitions

1

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.

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

Implementing all 171 CIS sub-controls is effective in mitigating 83% of all Mitre ATT&CK Techniques.

CIS Control 1 – Inventory and Control of Hardware Assets

Sub-Controls	Asset Type	Security Function	Title	Control Description
1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.
1.6	Devices	Identify	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.

CIS Control 2 – Inventory and Control of Software Assets

Sub-Controls	Asset Type	Security Function	Title	Control Description
2.1	Apps	Identify	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.
2.2	Apps	Identify	Ensure Software Is Supported by Vendor	Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
2.6	Apps	Respond	Address Unapproved Software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.

CIS Control 3 – Continuous Vulnerability Management

Sub-Controls	Asset Type	Security Function	Title	Control Description
3.4	Apps	Protect	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.
3.5	Apps	Protect	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

CIS Control 4 – Controlled Use of Administrative Privileges

Sub-Controls	Asset Type	Security Function	Title	Control Description
4.2	Users	Protect	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
4.3	Users	Protect	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities.

CIS Control 5 – Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Sub-Controls	Asset Type	Security Function	Title	Control Description
5.1	Apps	Protect	Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.

Sub-Controls	Asset Type	Security Function	Title	Control Description
6.2	Network	Detect	Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.

Sub-Controls	Asset Type	Security Function	Title	Control Description
7.1	App	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.
7.7	Network	Protect	Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.

Sub-Controls	Asset Type	Security Function	Title	Control Description
8.2	Devices	Protect	Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
8.4	Devices	Detect	Configure Anti-Malware Scanning of Removable Media	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
8.5	Devices	Protect	Configure Devices to Not Auto-Run Content	Configure devices to not auto-run content from removable media.

Sub-Controls	Asset Type	Security Function	Title	Control Description
9.4	Devices	Protect	Apply Host-Based Firewalls or Port-Filtering	Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

CIS Control 10 – Data Recovery Capabilities

Sub-Controls	Asset Type	Security Function	Title	Control Description
10.1	Data	Protect	Ensure Regular Automated Backups	Ensure that all system data is automatically backed up on a regular basis.
10.2	Data	Protect	Perform Complete System Backups	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.
10.4	Data	Protect	Protect Backups	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.
10.5	Data	Protect	Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

CIS Control 11 – Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

Sub-Controls	Asset Type	Security Function	Title	Control Description
11.4	Network	Protect	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.

CIS Control 12 – Boundary Defense

Sub-Controls	Asset Type	Security Function	Title	Control Description
12.1	Network	Identify	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.
12.4	Network	Protect	Deny Communication Over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic, to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

CIS Control 13 – Data Protection

Sub-Controls	Asset Type	Security Function	Title	Control Description
13.1	Data	Identify	Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.
13.2	Data	Protect	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.
13.6	Data	Protect	Encrypt Mobile Device Data	Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.

Sub-Controls	Asset Type	Security Function	Title	Control Description
14.6	Data	Protect	Protect Information Through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

CIS Control 15 – Wireless Access Control

Sub-Controls	Asset Type	Security Function	Title	Control Description
15.7	Network	Protect	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.
15.10	Network	Protect	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.

CIS Control 16 – Account Monitoring and Control

Sub-Controls	Asset Type	Security Function	Title	Control Description
16.8	Users	Respond	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.
16.9	Users	Respond	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.
16.11	Users	Protect	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.

CIS Control 17 – Implement a Security Awareness and Training Program

Sub-Controls	Asset Type	Security Function	Title	Control Description
17.3	N/A	N/A	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.
17.5	N/A	N/A	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.
17.6	N/A	N/A	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.

CIS Control 17 (cont.) – Implement a Security Awareness and Training Program

Sub-Controls	Asset Type	Security Function	Title	Control Description
17.7	N/A	N/A	Train Workforce on Sensitive Data Handling	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information.
17.8	N/A	N/A	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to *autocomplete* in email.
17.9	N/A	N/A	Train Workforce Members on Identifying and Reporting Incidents	Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.

CIS Control 19 – Incident Response and Management

Sub-Controls	Asset Type	Security Function	Title	Control Description
19.1	N/A	N/A	Document Incident Response Procedures	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.
19.3	N/A	N/A	Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.
19.5	N/A	N/A	Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.
19.6	N/A	N/A	Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.

Source: Center for Internet Security

Implementation Group 1:

- They offer an initial starting point for execution of a cyber security strategy and provide for a Strong Cyber Foundation
- They are scalable to meet the needs of the smallest to largest organizations
- Execution of the 43 sub-controls in Implementation Group 1 can defend against the five major cyber attacks, and mitigates 62 percent of Mitre ATT&CK Techniques
- Provide a quick security win for the Healthcare and Public Health (HPH) Sector

Implementation Groups 2 and 3:

- Implementing all 171 CIS sub-controls is effective in mitigating 83 percent of all Mitre ATT&CK Techniques

Reference Materials

References

- “CIS – Center for Internet Security,” Center for Internet Security. Accessed January 7, 2021. https://www.cisecurity.org/
- “CIS Controls and the HPH,” Department of Health and Human Services. September 3, 2020. https://www.hhs.gov/sites/default/files/cis-controls-and-the-hph.pdf
- “The 20 CIS Controls & Resources,” Center for Internet Security. Accessed January 7, 2021. https://www.cisecurity.org/controls/cis-controls-list/
- Sager, Tony. “Cleaning Up a Definition of Basic Cyber Hygiene,” Center for Internet Security. Accessed January 8, 2021. https://www.cisecurity.org/blog/cleaning-up-a-definition-of-basic-cyber-hygiene/
- “Verizon 2020 Data Breach Investigations Report (DBIR),” Verizon. Accessed January 11, 2021. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
- “Framework for Improving Critical Infrastructure Cybersecurity,” NIST. Accessed January 11, 2021. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- “Moving Forward: Setting the Direction | 2020 Annual Report,” CynergisTek. Accessed January 13, 2021. https://insights.cynergistek.com/reports/2020-annual-report
- Morgan, Steve. “Healthcare Industry To Spend $125 Billion On Cybersecurity From 2020 To 2025,” Cybercrime Magazine. September 8, 2020. https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025
- Anderson, Ginger, et al. “CIS Community Defense Model,” Center for Internet Security. Accessed January 12, 2021. https://www.cisecurity.org/white-papers/cis-community-defense-model/

Questions

Upcoming Briefs

- ATT&CK for Emotet (1/28)
- Threats in Healthcare Cloud Computing (2/4)

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.

HC3 Customer Feedback

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

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current 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 presentations that provide 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,or call us Monday-Friday between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV