Cyber-Hygiene for All: 
An Introduction to the CIS Controls

Phyllis Lee
Senior Director of CIS Controls
Center for Internet Security
Overview

- Introductions
- CIS Control Basics
- Implementation Groups
- Other Available Tools and Resources
- Feedback on the Controls
- Future Directions
Introductions

- Phyllis Lee
  - 20 years in the US Federal Government
  - Security Automation Lead for the Information Assurance Directorate (IAD) at the NSA
  - Focus on virtualization and malware analysis

- Joshua M Franklin
  - 10 years in the US Federal Government
    - 7 of those years at NIST
  - Focus on telecommunications, mobile, and election security
  - Cybersecurity standards (e.g., NIST, CIS, IEEE, OASIS, 3GPP)
CIS Introduction

- US-based forward-thinking, non-profit entity that harnesses the power of a global IT community
- Goal of safeguarding private & public organizations against cyber threats
- CIS Vision: Leading the global community to secure our connected world
- CIS Mission:
  - Identify, develop, validate, promote, and sustain best practice solutions for cyber defense
  - Build and lead communities to enable an environment of trust in cyberspace
The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation’s state, local, tribal, and territorial governments.
The CIS Controls

- Globally recognized cybersecurity standard
- Over 228,000 downloads since CIS took the reigns
- 20 top-level controls followed by 171 sub-controls
- Prioritized set of actions that’s designed to scale
- Provides a logical path to build a foundation and gradually improve your cybersecurity posture
- Version 7.1 released in April 2019
- Developed by cybersecurity experts - *like you*
Goals of the CIS Controls

- Concise
- Prioritized
- Attack-driven
- Measurable
- Defensible
- Consensus-based
7.1 Update

- Guiding principles for the 7.1 update:
  - Provide a new prioritization scheme (Implementation Groups)
  - Enhance the clarity and readability of the Controls
  - Refrain from modifying the spirit of any Controls

- Aimed as a way to:
  - Practice **basic cyber hygiene** with limited resources and expertise
  - Prioritize cybersecurity activities
  - Implement security best practices, regardless of resources
  - Ensure a standard duty of care
CIS Controls History

NSA/DoD Project

CSIS The Consensus Audit Guidelines (CSIS)

SANS “The SANS Top 20” (the SANS Institute)

CIS Critical Security Controls (CCS/CIS)

CIS Controls®
The CIS Controls

**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
Staying Fresh with Basic Cyber Hygiene

- Comparing your organization against best practice helps you take stock of your cybersecurity health
  - Often nebulously defined as **basic cyber hygiene**

- Commonly used term but what does it mean?

- CIS defines Implementation Group 1 as **basic cyber hygiene**
  - 43 specific tasks to ensure your organization is performing the baseline
Implementation Groups

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

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

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

Definitions

Implementation Group 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.

Implementation Group 2
CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.

Implementation Group 3
CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.
What Group Are You?

- That’s for you to decide
- Methodology for deciding your Implementation Group is provided based on the following:
  - Data sensitivity and criticality of services offered by the organization
  - Expected level of technical expertise exhibited by staff or on contract
  - Resources available and dedicated towards cybersecurity activities
Implementation Group 1 Topics

Procedural
- Maintaining an asset inventory
- Password management
- 1 offsite backup
- Network boundary inventory
- Incident response planning
- Isolating personal devices

Technical
- Automated patching
- Secure configuration
- Audit logging
- DNS filtering
- Dedicated admin workstations
- Account management
Other Tools to Help Along the Way

Supplementing the CIS Controls
Guides & Tools

- CIS provides domain specific guidance for the CIS Controls
  - Cloud
  - Internet of Things (IoT)
  - Mobile
  - Industrial Control System (ICS)

- CIS provides a detailed Cyber Hygiene guide for Windows 10

- CIS provides an automated method to assess some CIS Controls on Windows 10 called the Controls Assessment Module
Mappings to Other Frameworks

- CIS is committed to interoperability with other industry frameworks
- CIS maps to a variety of security standards and frameworks
  - Available in a machine-readable format
- Available mappings:
  - NIST CSF
  - ISO 27000
  - NIST 800-53
  - NIST 800-171
- Upcoming:
  - HIPAA
  - PCI DSS
  - COBIT
  - MARS-E
- External:
  - Microsoft Azure Security Benchmark
  - NIST Online Informative Reference (OLIR)
# Evolving a Cybersecurity Standard

## Evolving the CIS Controls Selection Process

<table>
<thead>
<tr>
<th>LOWER</th>
<th>Leverage, Scalability, Repeatability</th>
<th>HIGHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Five schmucks in a room</td>
<td>Five thousand friends on a mailing list</td>
<td>Mapping to authoritative problem summaries</td>
</tr>
</tbody>
</table>

---

**RSAC**

Center for Internet Security

18

RSAC Conference 2020
Community Attack Model Version 1

- CIS effort to analyze pertinent information relating to real-world attacks in the wild
- Goal: help enterprises make good choices about the most effective defensive actions they can take
- Released via Blackhat in 2016
- Leverages additional frameworks such as NIST CSF and Lockheed Martin Cyber Kill Chain
- Updating this model based on publicly available attack data
Community Defense Model

• Revamp and update the *Community Attack Model*

• Standard method of expression

• General methodology:
  – Analyze data sources
  – Identify key attack paths
  – Identify mitigations for key attacks
  – Map mitigations to CIS Controls

• Expected outputs:
  – Mapping of the CIS Controls to MITRE ATT&CK
  – Mappings of the CIS Controls to MITRE ATT&CK Mitigations
  – Data-backed attack patterns that the CIS Controls defend against
Define What Attacks the CIS Controls Defend Against

- No other security standard or defensive framework does this.
Controls Assessment Specification

- Open specification allowing organizations to measure implementation of the CIS Controls
- CAS is focused on “what to measure” rather than “how to measure”
- Platform agnostic method allowing external tooling vendors to implement as best for their appropriate use cases
Feedback on the CIS Controls

What’s the community saying and doing?
State Adoption of the CIS Controls

- States have adopted the CIS Controls in different ways
- **Nevada** defines the CIS Controls as a reasonable definition of security for state government agencies (NV S.B. 302)
- **Ohio** Data Protection Act provides legal protections for organizations voluntary implementing the CIS Controls or other defined frameworks
- **California** 2016 Data Breach Report warns that failing to implement the CIS Controls “constitutes a lack of reasonable security”
- **Idaho** Governor’s executive order requires executive branch agencies to implement the first 5 CIS Controls (EXECUTIVE ORDER NO. 2017-02)
Feedback

- Where do I start?
  - Many organizations get very bogged down in Control 1
- What isn’t [my_favorite_technology] reflected within the Controls?
- Where is my guidance for performing a risk assessment?
- Why don’t the Controls tell me what specific policies to use?
CIS Security Assessment Tool (CSAT)

- Web application allowing security professionals to track the implementation of the CIS Controls
  - At the Sub-Control level
  - Recent inclusion of CIS Implementation Groups
- Essentially a GRC tool designed to ease implementation of the CIS Controls
- Allows users to compare their scores against others in their industry
## Top 10 Sub-Control Scores

<table>
<thead>
<tr>
<th>Rank</th>
<th>Sub-Control #</th>
<th>Sub-Control Title</th>
<th>Average</th>
<th>IG</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8.2</td>
<td>Ensure Anti-Malware Software and Signatures Are Updated</td>
<td>81.42</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>8.1</td>
<td>Utilize Centrally Managed Anti-Malware Software</td>
<td>80.00</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>15.7</td>
<td>Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data</td>
<td>79.69</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>15.10</td>
<td>Create Separate WiFi Network for Untrusted Devices</td>
<td>78.53</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>15.1</td>
<td>Maintain an Inventory of Authorized Wireless Access Points</td>
<td>76.75</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>10.1</td>
<td>Ensure Regular Automated Backups</td>
<td>76.12</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>4.2</td>
<td>Change Default Passwords</td>
<td>75.35</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>7.9</td>
<td>Block Unnecessary File Types</td>
<td>69.80</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>10.2</td>
<td>Perform Complete System Backups</td>
<td>69.67</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>16.11</td>
<td>Lock Workstation Sessions After Inactivity</td>
<td>69.10</td>
<td>1</td>
</tr>
</tbody>
</table>
## Bottom 10 Sub-Control Scores

<table>
<thead>
<tr>
<th>Rank</th>
<th>Sub-Control #</th>
<th>Sub-Control Title</th>
<th>Average</th>
<th>IG</th>
</tr>
</thead>
<tbody>
<tr>
<td>171</td>
<td>20.5</td>
<td>Create a Test Bed for Elements Not Typically Tested in Production</td>
<td>12.50</td>
<td>2</td>
</tr>
<tr>
<td>170</td>
<td>14.5</td>
<td>Utilize an Active Discovery Tool to Identify Sensitive Data</td>
<td>13.78</td>
<td>3</td>
</tr>
<tr>
<td>169</td>
<td>4.6</td>
<td>Use Dedicated Workstations For All Administrative Tasks</td>
<td>14.92</td>
<td>3</td>
</tr>
<tr>
<td>168</td>
<td>14.7</td>
<td>Enforce Access Control to Data Through Automated Tools</td>
<td>15.05</td>
<td>3</td>
</tr>
<tr>
<td>167</td>
<td>20.3</td>
<td>Perform Periodic Red Team Exercises</td>
<td>15.33</td>
<td>3</td>
</tr>
<tr>
<td>166</td>
<td>15.9</td>
<td>Disable Wireless Peripheral Access to Devices</td>
<td>15.84</td>
<td>2</td>
</tr>
<tr>
<td>165</td>
<td>2.9</td>
<td>Implement Application Whitelisting of Scripts</td>
<td>15.99</td>
<td>3</td>
</tr>
<tr>
<td>164</td>
<td>2.8</td>
<td>Implement Application Whitelisting of Libraries</td>
<td>16.13</td>
<td>3</td>
</tr>
<tr>
<td>163</td>
<td>5.5</td>
<td>Implement Automated Configuration Monitoring Systems</td>
<td>16.88</td>
<td>2</td>
</tr>
<tr>
<td>162</td>
<td>11.6</td>
<td>Use Dedicated Workstations for All Network Administrative Tasks</td>
<td>17.59</td>
<td>2</td>
</tr>
</tbody>
</table>
Future of the Controls

- Looking to release version 8 of the CIS Controls in 2021
- Primary tasks: *simplification, decrease of cost and time to implement the Controls*
- Integrate the Community Defense Model into the CIS Controls
- Integrate CSAT data into the CIS Controls
- Will also be reflective of cloud technologies
- New approach to identity, authentication, and authorization
Apply What You’ve Learned Today

- Next week you should:
  - Review Implementation Group 1
  - Verify your organization is implementing basic cyber hygiene

- In the first three months following this presentation you should:
  - Assess whether your organization is Implementation Group 1, 2, or 3
  - Develop a plan for prioritize CIS Sub-Controls in your Implementation Group

- Within six months you should:
  - Review other free CIS resources such as Mobile, Cloud, and IoT Guides
  - Consider assessing your organization’s via CSAT
Conclusions

- CIS provides free tools and guidance for all organizations:
  - https://www.cisecurity.org

- Share your cybersecurity expertise, join a community:
  - Visit https://workbench.cisecurity.org to participate

- The CIS Community Defense Model releasing soon

- Download CIS Controls v7.1
  - Fun web application to view, filter, and relate the Controls
Unused unless we need to