Center for Internet Security®

Prioritizing the CIS Controls

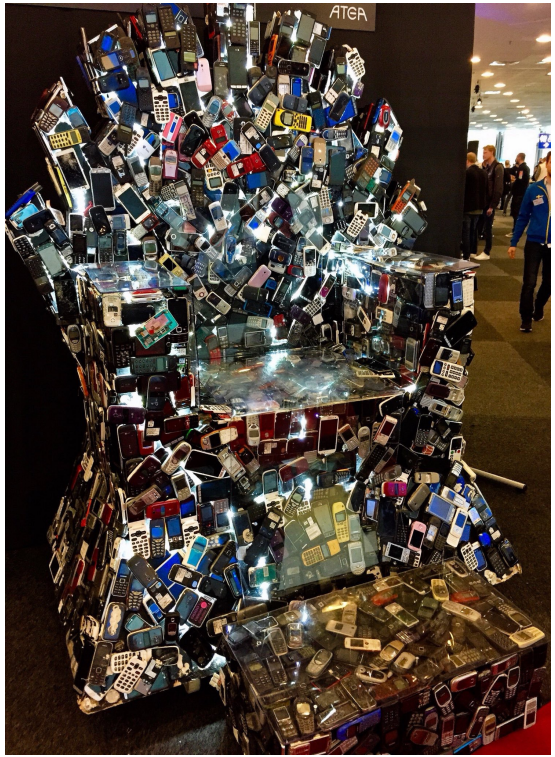
Making the Critical Security Controls Work for You

Joshua M Franklin
Senior Cybersecurity Engineer, Controls

June 21, 2019

About Me

- Joshua M Franklin
- Product owner of the CIS Controls
- Cybersecurity standardization
- Telecommunications security, mobile security, mobile app vetting
- Campaign and election security
- NIST
- Election Assistance Commission



Game of Phones

The Defender's Dilemma

1. What's right thing to do, and how much do I need to do?
2. How do I actually do it?
3. How can I demonstrate to others that I have done the right thing?

CIS Controls Introduction

- Globally recognized cybersecurity standard
- Over 150,000 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***

What Are the CIS Controls?

The CIS Controls are a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber attacks. The Controls are developed, refined, and validated by a community of leading experts from around the world.

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

New: CIS Controls Version 7.1

- 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 cyber hygiene with limited resources and expertise
  - Prioritize cybersecurity activities
  - Implement security best practices, regardless of resources
  - Ensure a standard duty of care

NSA/DoD Project

The Consensus Audit Guidelines (CSIS)

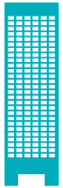
“The SANS Top 20” (the SANS Institute)

The Critical Security Controls (CCS/CIS)

Mapping to Other Frameworks

- CIS is committed to interoperability with other industry frameworks:
  - NIST CSF mapping available now: https://www.cisecurity.org/white-papers/cis-controls-v7-1-mapping-to-nist-csf/
- Look out for more CIS v7.1 mappings later this year!
  - NIST SP 800-53
  - NIST SP 800-171
  - ISO 27000
  - COBIT
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Payment Card Industry Data Security Standard (PCI DSS)

Implementation Groups



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

Definitions	1	2	3
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.			●

CIS defines Implementation Group 1 as Basic Cyber Hygiene

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

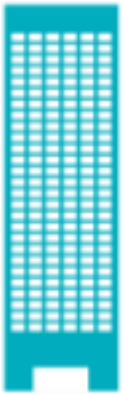
- 43 Sub-Controls out of the 171 total
- Combination of procedural and technical mitigations
  - Heavily leans procedural
- Represents the essential sub-controls that mitigate the most common attacks
- May sub-controls may require an IT contractor for smaller organizations

- Defined as cyber hygiene
- Impact on usability should be low

Implementation Group 2

- Includes an additional 97 Sub-Controls meaning 140 total in IG2
- Combination of procedural and technical mitigations
  - Leans towards more technical mitigations
- Represents the next step after the security *essentials*
- Contains the largest number of mitigations
- Examples include:
  - formal vulnerability management process,
  - advanced logging,
  - monitoring for deviations from approved configuration baseline

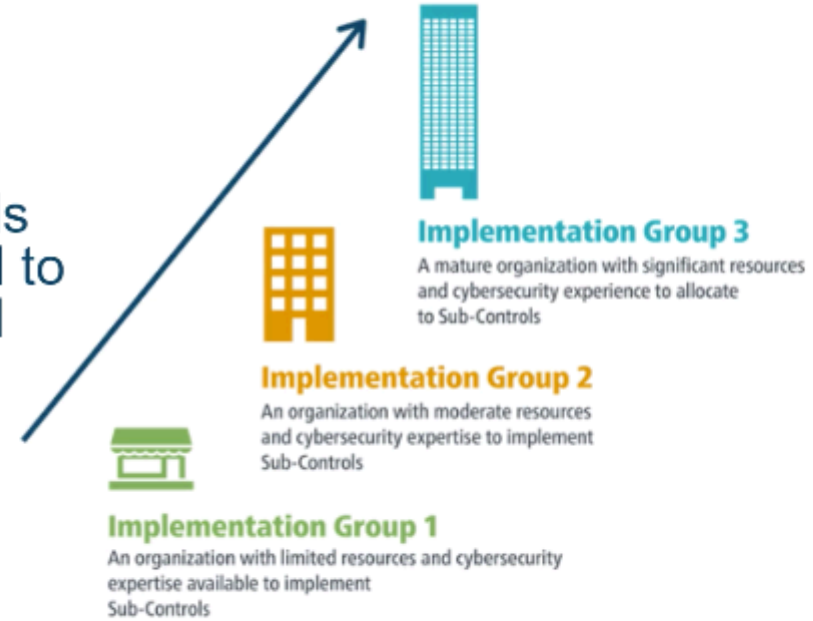
Implementation Group 3



- Includes an additional 31 Sub-Controls meaning 171 total in IG3
- Combination of procedural and technical mitigations
  - Heavily leans technical
- Represents mitigations to mitigate zero days and targeted attacks
- Requires extensive resources and knowledge to implement
- Primarily focuses on security automation
- Usability impacts will likely occur
- Examples include whitelisting and application level firewalls

Building Groups

The number of Sub-Controls an organization is expected to implement increases based on which group an organization falls into



CIS RAM

For "Reasonable" Implementation of the CIS Controls

CIS Risk Assessment Methodology

Step-by-step instructions to demonstrate when your CIS Controls implementation is enough …

- for security
- for business
- for regulators
- for litigation

CIS RAM

- Detailed instructions for conducting cyber security risk assessments.
- Instructions for defining acceptable risk.
- Aligned with judicial and regulatory understanding of “reasonable” and “appropriate.”
- Workbook with templates and examples.
- Based on new Duty of Care Risk Analysis (“DoCRA”) standard.
- Everyone needs a risk assessment

IG1 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

Prioritization via Data

- IG1 is meant to focus on real threats affecting organizations
- Threat data sources are often scarce, under NDA, or unable to be compared to each other
- CIS used publicly available threat reports to develop IG1
  - Useful lens to explore IG1
- Examples of high-profile threats mitigated by IG1:
  - Malicious email attachments
  - Spearphishing
  - Accidental errors and incidents
  - Ransomware

Malicious Email Attachments

- Verizon states that there were 1,192 incidents and 236 confirmed data breaches using this attack pattern in 2018 *[Verizon, 2018]*
- Mitigated by the following IG1 Sub-Controls:
  - 1.4: Maintain detailed asset inventory
  - 1.6: Address unauthorized assets
  - 2.1: Maintain inventory of authorized software
  - 2.2: Ensure software is supported by vendor
  - 2.6: Address unapproved software
  - 3.4, 3.5: Update with recent security updates provided by software vendor
  - 5.1: Maintain documented, standard security configuration
  - 17.3: Implement a Security Awareness Program
  - 17.6: Train Workforce on Identifying Social Engineering Attacks

Spearphishing

- Symantec reports that Spear-phishing is used by 71 percent of hacking groups *[Symantec, 2018]*
- IBM states that "…phishing attacks continue to be one of the most successful means of making unknowing insiders open the door to malicious attackers" [*IBM, 2018*]
- Mitigated by the following IG1 Sub-Controls:
  - 17.3: Implement a Security Awareness Program
  - 17.6: Train Workforce on Identifying Social Engineering Attacks

Accidental Errors and Incidents

- Verizon states that 17% of breaches in 2018 had errors as causal events [*Verizon, 2018*]
- Mitigated by the following IG1 Sub-Controls:
  - 10.1: Ensure Regular Automated Back Ups
  - 10.2: Perform Complete System Backups
  - 10.5: Ensure Backups Have At least One Non-Continuously Addressable Destination
  - 13.1: Maintain an Inventory of Sensitive Information
  - 13.2: Remove Sensitive Data or Systems Not Regularly Accessed by Organization

Stolen Credentials

- Verizon listed stolen credentials as the most common reason for a publicly confirmed data breach, with 399 breaches utilizing this “threat action” *[Verizon, 2018]*
- Mitigated by the following IG1 Sub-Controls:
  - 4.2: Change default passwords
  - 4.3: Ensure the Use of Dedicated Administrative Accounts
  - 14.6: Protect Information through Access Control Lists
  - 16.8: Disable Any Unassociated Accounts
  - 16.9: Disable Dormant Accounts
  - 17.3: Implement a Security Awareness Program
  - 17.6: Train Workforce on Identifying Social Engineering Attacks

Conclusions

- CIS provides free tools and guidance for all organizations:
  - https://www.cisecurity.org
- Get involved and join one of our communities:
  - https://workbench.cisecurity.org/ to get a workbench account
- Download CIS Controls v7.1
  - https://workbench.cisecurity.org/
- Measure your Windows 10 implementation of IG1 soon
- Automated assessment via the Controls Assessment Module

Thank You

References

- Symantec, *Internet Security Threat Report, Symantec Corporation*, Volume 23, March 2018. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf
- Verizon, *2018 Data Breach Investigations Report, Verizon*, 11th Edition, 2018. https://enterprise.verizon.com/resources/reports/dbir/
- IBM, *X-Force Threat Intelligence Index 2018*, IBM, March 2018. https://www.ibm.com/security/data-breach/threat-intelligence (Direct link to report)