From Security Vulnerabilities to Better Practices: Version 7 of the CIS Controls

Curtis Dukes
Executive VP & General Manager,
Security Best Practices & Automation Group
June 11, 2018

Cyber Adversaries a changing landscape

6 Cyber Threats for 2018

- More huge data breaches (Equifax part deux)
- Ransomware in the cloud
- The weaponization of AI (machine learning)
- Cyber-physical attacks
- Mining cryptocurrencies
- Hacking elections (again!)

Courtesy, MIT Technology Review

New Devices = New Risk

Traditional IT

Traditional devices and infrastructure owned, and managed by IT

Employee

Transient devices that connect to corporate networks

Operational

Business critical devices that now have IP addresses

Public

Neighboring wireless networks and devices

Uncontrolled interactions of connected devices and networks introduces risk to **physical safety**, **revenue**, **public perception**, and **customer experience**

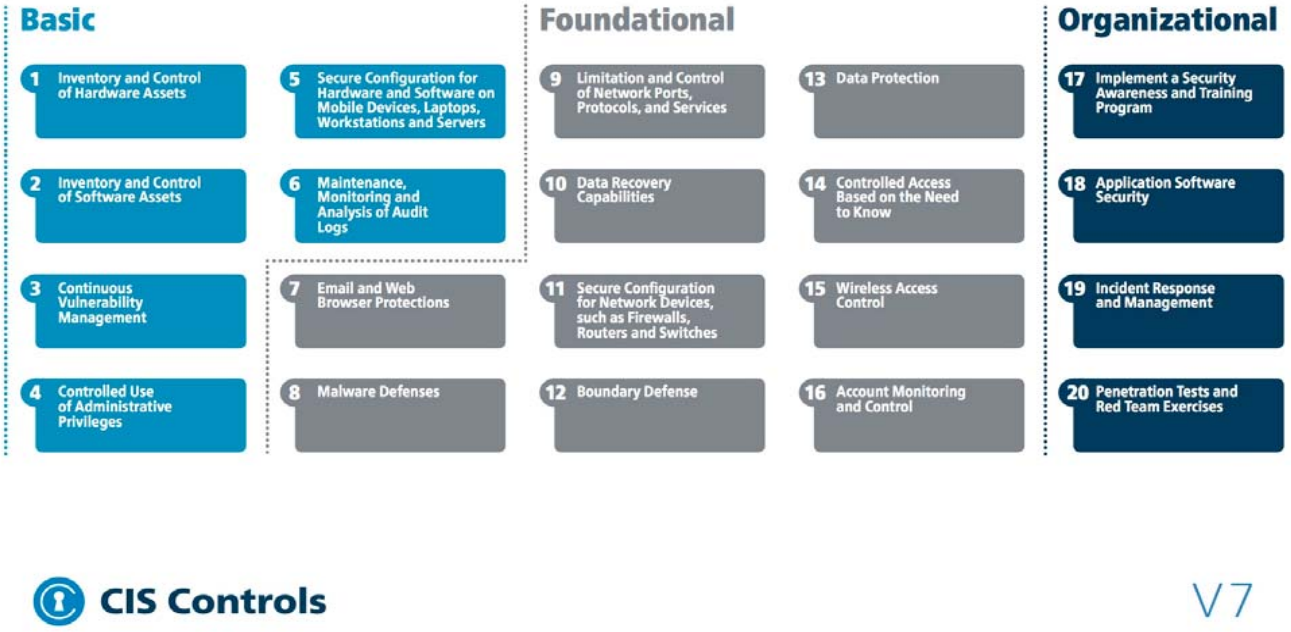
Some Unfortunate Facts

- The vast majority of compromises are based on known problems that have known solutions
- 85% of the incidents managed by the US-CERT come down to the same five basic defenses
- Very few attackers use “stealth” techniques
- Very few defenders have automated workflow

The Defender's Dilemma

1. What's the 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?

Incremental Approach to Cyber Defense



Focus on the first 6 Controls

- Know what you are protecting
  - ✓ CIS Control #1: Inventory and Control of Hardware Assets
  - ✓ CIS Control #2: Inventory and Control of Software Assets
- Define Secure Configuration Baseline
  - ✓ CIS Control #3: Continuous Vulnerability Management
- Continuously Monitor Vulnerability of Resources
  - ✓ CIS Control #4: Controlled Use of Administrative Privileges
- Limit and Monitor Administrative Privileges
  - ✓ CIS Control #5: Secure Configuration for HW and SW on Mobile Devices, Laptops, Workstations and Servers
- Continuous Monitoring/Situational Awareness
  - ✓ CIS Control #6: Maintenance, Monitoring, and Analysis of Audit Logs

Recommendations

- Revisit organizational IT governance model
  - Extend security policies to IoT devices and all organization elements
  - Include IoT as a part of the enterprise architecture
  - Establish enterprise-wide standards and best practices for IoT devices
- Develop and enforce a BYOD policy
- Evolve procurement policies
  - Disclosure of device technical characteristics
  - Unique passwords for every device
  - Purchased devices must meet technical standards (longer term)
- Join an ISAC to ensure access to advisories and support

- Website: www.cisecurity.org
- Email: Controlsinfo@cisecurity.org
- Twitter: @CISecurity
- Facebook: Center for Internet Security
- LinkedIn Groups:
  - Center for Internet Security
  - 20 Critical Security Controls