Addressing the Internet of Things (IoT) Challenge

John M. Gilligan
Interim CEO & Chairman of the Board

21 June 2017
Who is CIS?

CIS delivers
Confidence in the Connected World

- Not-for-profit, independent, objective, and international in scope.
- We operate the Multi-State Information Sharing and Analysis Center (MS-ISAC).
- We develop and support best practices for effective defenses against cyber attacks.
- We mobilize and organize volunteers in a community model.
The Isolated Enterprise – the “Good Old Days”

INTERNET

Corp. IT

Contractors & Guests

PHYSICAL SECURITY

BUILDING MANAGEMENT

MEDICAL DEVICES

PAYMENT SYSTEMS
The Connected Enterprise – Internet of (Evil) Things (IoT)

- Corp. IT
- Contractors & Guests
- PHYSICAL SECURITY
- MEDICAL DEVICES
- BUILDING MANAGEMENT
- PAYMENT SYSTEMS
New Devices Interactions – New Risk

Uncontrolled interactions of connected devices and networks introduces risk to **physical safety, revenue, public perception, and customer experience.**
Challenges in Securing IoT Devices

• **The Devices: “Volume, Variety, Velocity”**
  – Formerly stand-alone, and smarter devices coming on-line
  – Lack of visibility, central management, and “situational awareness”

• **The Players:**
  – manufacturers, decision-makers, end users, regulators…..

• **The Environment:**
  – Mobile Devices? ”Mobile Users and Data” with fixed devices!
  – IT/Security shifts from “Gatekeeper” to “Orchestrator”
  – Distributed oversight and control

• **The Risks: A fresh look in the context of mission/business priorities**
  – beyond **Confidentiality / Integrity / Availability**
  – Risk = $f \{ \text{vulnerability, threat, consequence} \} / \text{controls}$
How Do You Manage IoT Device Risk?

Discover, fingerprint and track all devices in your environment

Identify vulnerable and high-risk devices putting critical systems at risk

Mitigate high-risk devices
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 the MS-ISAC to ensure access to advisories and support and consider use of MS-ISAC managed security services

• Visit CIS web site (www.cisecurity.org) for additional information and materials regarding securing the IoT
The CIS Controls – A Practical Guide to Security (for IoT)

First 5 CIS Controls
Eliminate the vast majority of your organization’s vulnerabilities

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges

6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Applications
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment & Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Leverage IoT Companion for CIS Controls
Contact Information:

John M. Gilligan
Interim CEO & Chairman of the Board
Center for Internet Security (CIS)
John.Gilligan@cisecurity.org
703-395-1561
Thank You