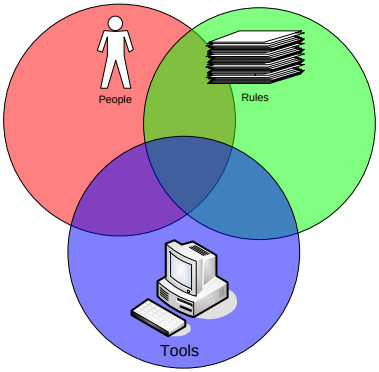
June 2019

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Understanding the CIS Critical Controls

Policies and Standards



- People, Rules and Tools
  - What do we expect to occur?
  - How do we conduct business?
- Standards based operations from a governance or compliance framework:
  - GLBA, FFIEC, state laws, etc…
  - PCI – DSS
  - **CIS Critical Controls**, NIST
- Disciplined exception management

Standards Based Operations

- Standards for your in-house systems that your IT staff manages and maintains.
- Standards for the the in-house systems provided by and/or managed by your service providers.
- Standards for your systems hosted at a third party (cloud/service bureau).

- NIST
  National Institute of Standards and Technology
- FFIEC
  Federal Financial Institutions Examination Council IT Examination Handbook InfoBase
- CIS
  Center for Internet Security CIS controls
- PCI
  Payment Card Industry Security Standards council
- CSA
  Cloud Security Allowance

Standards Based Operations

AuditScripts enclave SECURITY

Critical Security Control	NIST CSF v1.1	PCI DSS 3.2	FFIEC Information Security Booklet (2016)	FFIEC Examiners Handbook	FFIEC Cybersecurity Assessment Tool (CAT)	Cloud Security Alliance
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices	ID.AM-1 ID.AM-3 ID.AM-4 PR.DS-3	2.4	II.C.5	Host Security User Equipment Security (Workstation, Laptop, Handheld)	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	DCS-01 MOS-09 MOS-15
Critical Security Control #2: Inventory of Authorized and Unauthorized Software	ID.AM-2 PR.DS-6	2.4		Host Security User Equipment Security (Workstation, Laptop, Handheld)	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	CCC-04 MOS-3 MOS-04 MOS-15
Critical Security Control #3: Continuous Vulnerability Assessment and Remediation	ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.AN-5	6.1 6.2 11.2		Host Security User Equipment Security (Workstation, Laptop, Handheld)	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	IVS-05 MOS-15 MOS-19 TVM-02
Critical Security Control #4: Controlled Use of Administrative Privileges	PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3	2.1 7.1 - 7.3 8.1 - 8.3 8.7		Authentication and Access Controls	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	IAM-09 - IAM-13 MOS-16 MOS-20
Critical Security Control #5: Secure Configurations for Hardware and Software	PR.IP-1	2.2 2.3 6.2 11.5		Host Security User Equipment Security (Workstation, Laptop, Handheld)	Domain 3: Cybersecurity Controls - Preventative Controls Domain 3: Cybersecurity Controls - Detective Controls	IVS-07 MOS-15 MOS-19 TVM-02

Summary | NIST 800-53 rev4 | NIST CSF 1.1 | NIST CSF 1.0 | NIST 800-82 rev2 | NIST SMB Guide | DHS CDM Program | ISO 27002-2013 | ISO 27002-2005 | IEC 62443-3-3-2013 | NIST 800-171 | NSA MNT | Australian Essential 8 | Australian Top

https://www.auditscripts.com/free-resources/critical-security-controls/

Standards Based Operations

CIS Controls™

V7

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

https://www.cisecurity.org/controls/

Basic Controls

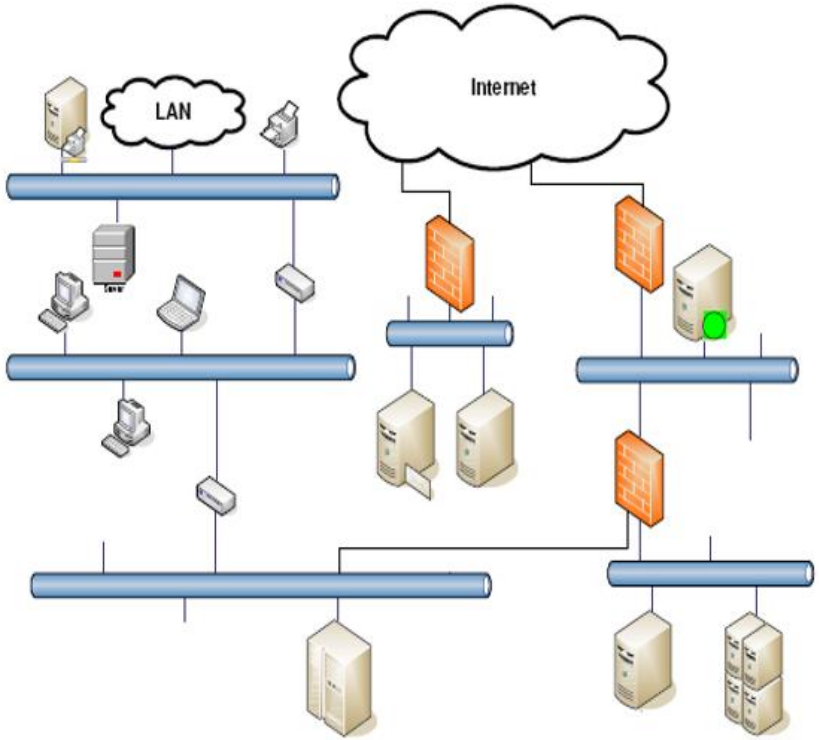
Low Hanging Fruit

Apply The CIS Critical Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets

"Inventory"…

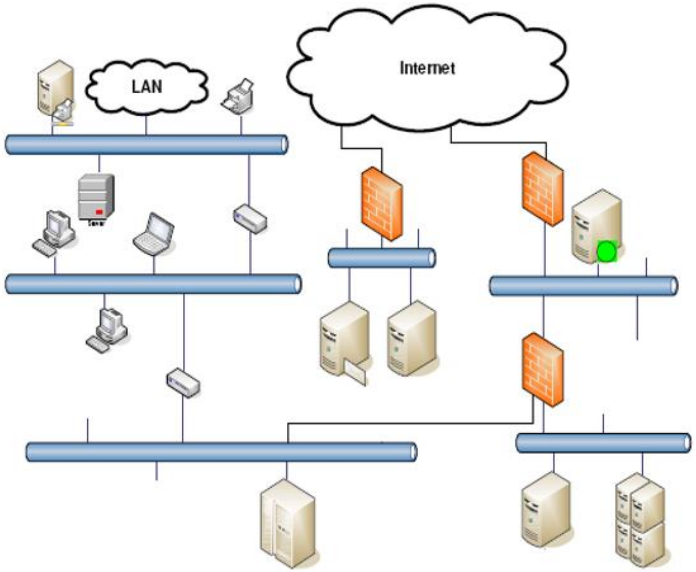
- Set the standard for "Normal"
- Sets the stage for the rest of the controls



Vulnerability Management

3 Continuous Vulnerability Management

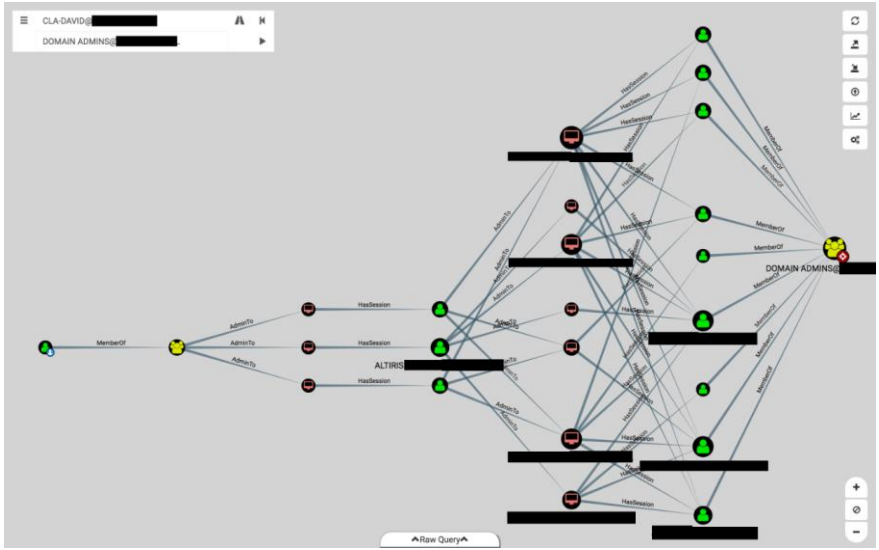
- Monitoring (built in) and scanning (independent) for vulnerabilities
  - "Patch Tuesday" and vulnerability scanning
  - Rogue devices



Passwords

- Controlled use of administrative privileges
  - Standard users should not have admin rights
  - Administrators should have two sets of credentials
- Do NOT log into workstations with administrator privileges

4 Controlled Use of Administrative Privileges



Secure Configurations (standards…)

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

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

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Why Is This CIS Control Critical?
As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared towards ease-of-deployment and ease-of-use – not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, pre-installation of unneeded software – all can be exploitable in their default state.

Developing configuration settings with good security properties is a complex task beyond the ability of individual users, requiring analysis of potentially hundreds or thousands of options in order to make good choices (the Procedures and Tools section on page 17 provides resources for secure configurations). Even if a strong initial configuration is developed and installed, it must be continually managed to avoid security "decay" as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked" to allow the installation of new software or support new operational requirements. If not, attackers will find opportunities to exploit both network accessible services and client software.

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

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions
5.1	Applications	Protect	Establish Secure Configurations	Maintain documented, standard security configuration standards for all authorized operating systems and software.
5.2	Applications	Protect	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
5.3	Applications	Protect	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
5.4	Applications	Protect	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
5.5	Applications	Detect	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

Benchmarks

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

- Secure Standard Builds
- Hardening Checklists

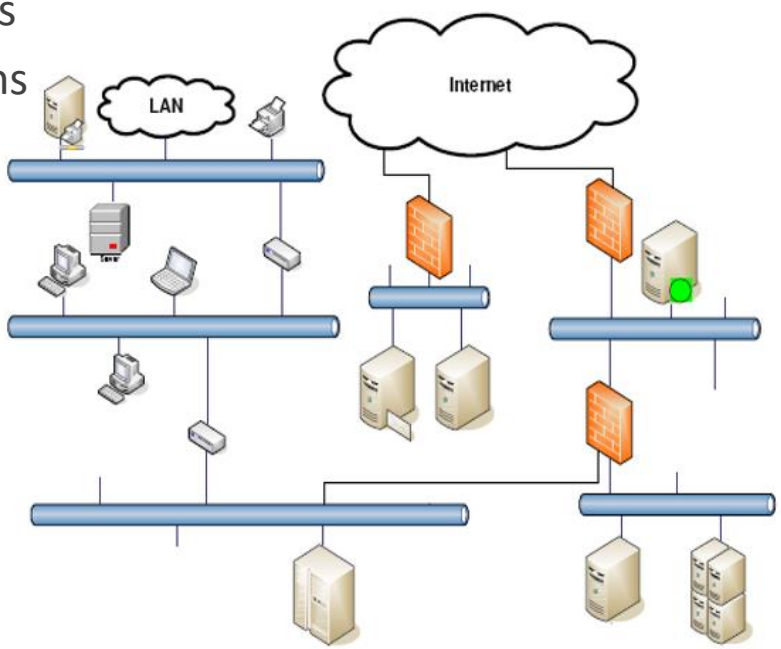
- Microsoft Windows 10 Benchmarks
- Microsoft Windows Server 2000 Benchmarks
- Microsoft Windows Server 2003 Benchmarks
- Microsoft Windows Server 2008 Benchmarks
- Microsoft Windows Server 2012 Benchmarks
- Microsoft Windows 7 Benchmarks
- Microsoft Windows 8 Benchmarks
- Microsoft Windows NT Benchmarks
- Microsoft Windows XP Benchmarks

Log Files

Centralization and Correlation of event logs

- System and application logs
- Critical data systems/files
- Key system configurations
- Data activity and flow
- Accounts

- Retention…



6 Maintenance, Monitoring and Analysis of Audit Logs

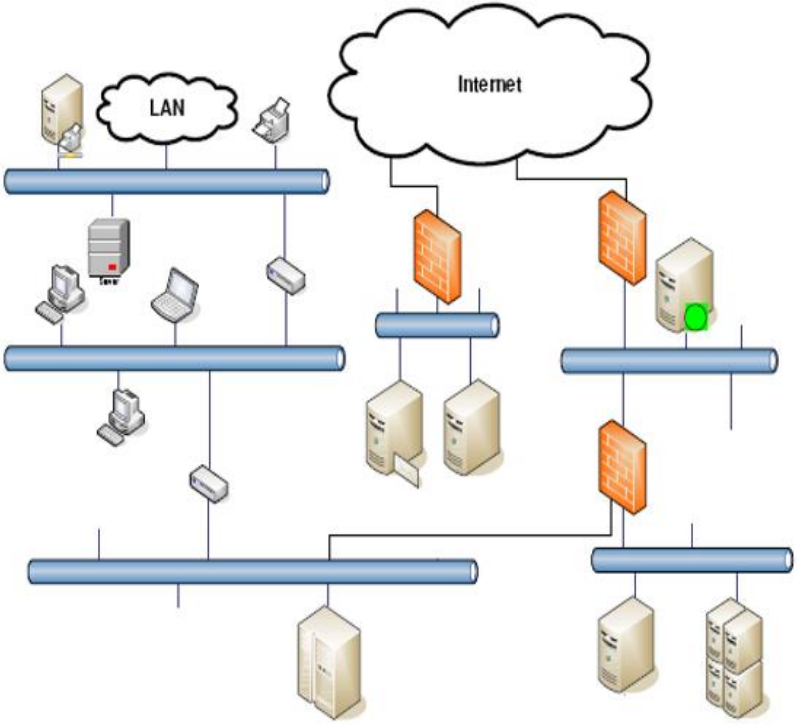
Foundational Controls

Layered Defenses and Operational Maturity

Foundational Controls

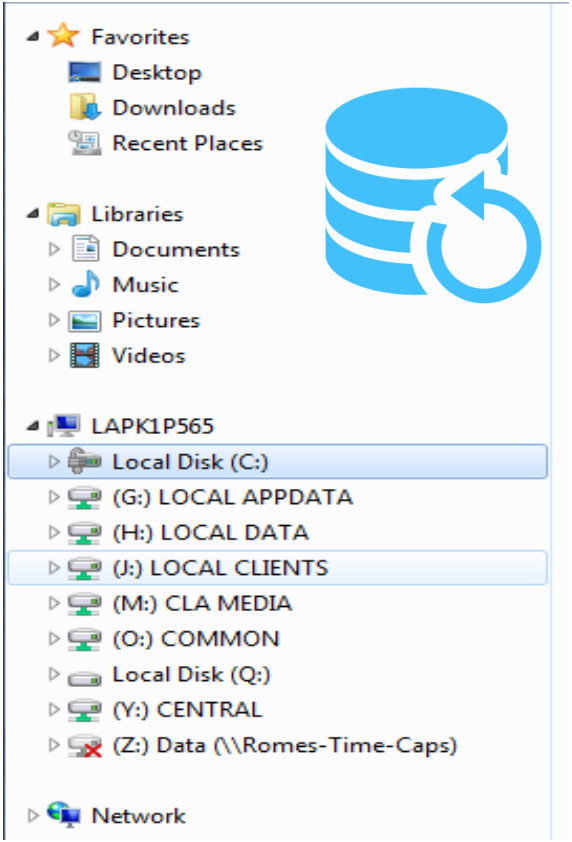
Foundational

- 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



Resilience
Back up and Restore

- Secure the backup process
  - Backups should be done with a service account.
  - Storage location of back ups should be very restrictive – read only access even for most administrators.
  - Identify which users could encrypt backups if they were to become infected.
  - You could also restrict the backup network access temporally similar to a bank vault.
- Working backup and restore capabilities
  - *PRACTICE*



Organizational Controls

Improvement Processes and Resilience

Standards Based Operations

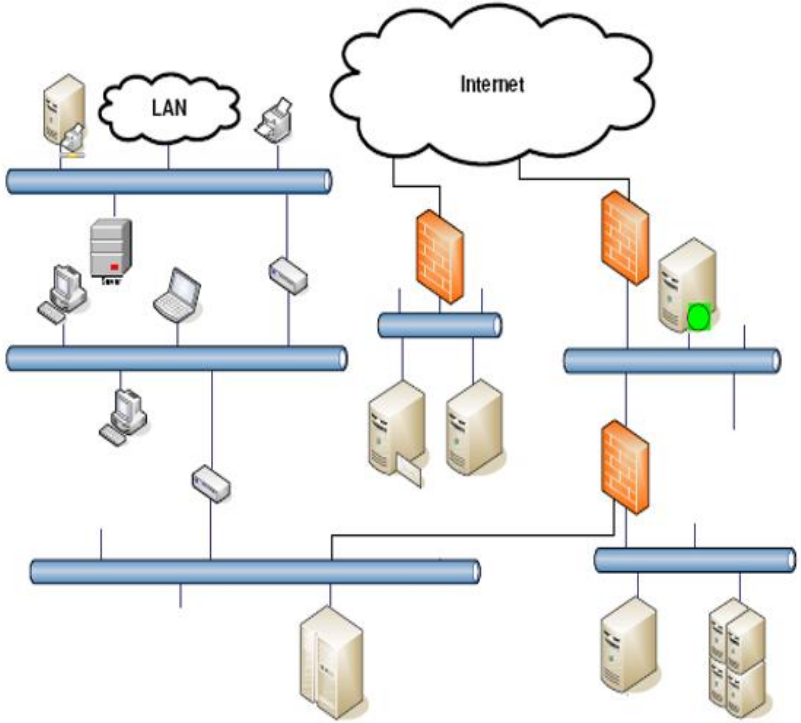
Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

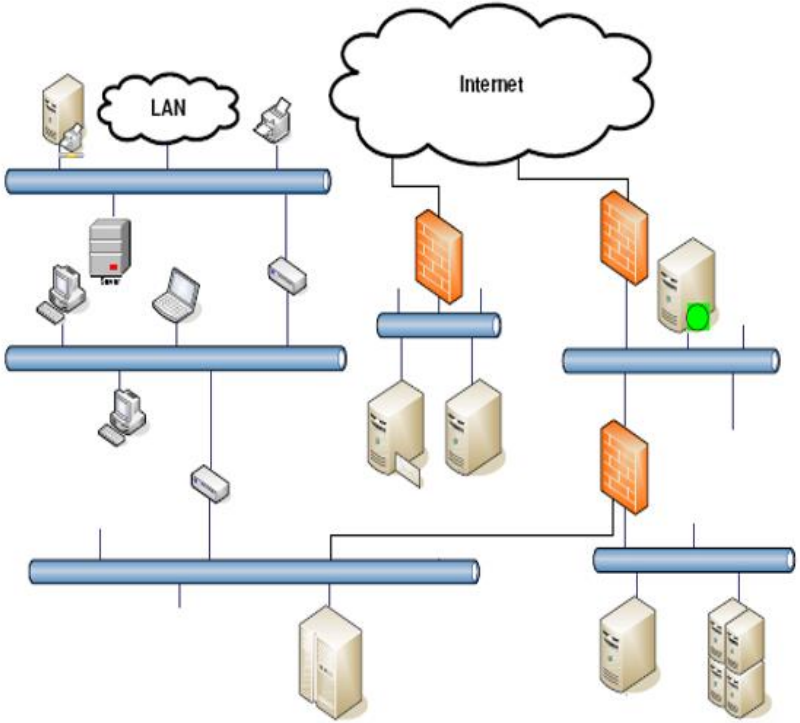
19 Incident Response and Management

20 Penetration Tests and Red Team Exercises



Know Your Network
Know What "Normal" Looks Like

- Infrastructure
- Servers & Applications
- Data Flows
- Archiving vs. Reviewing

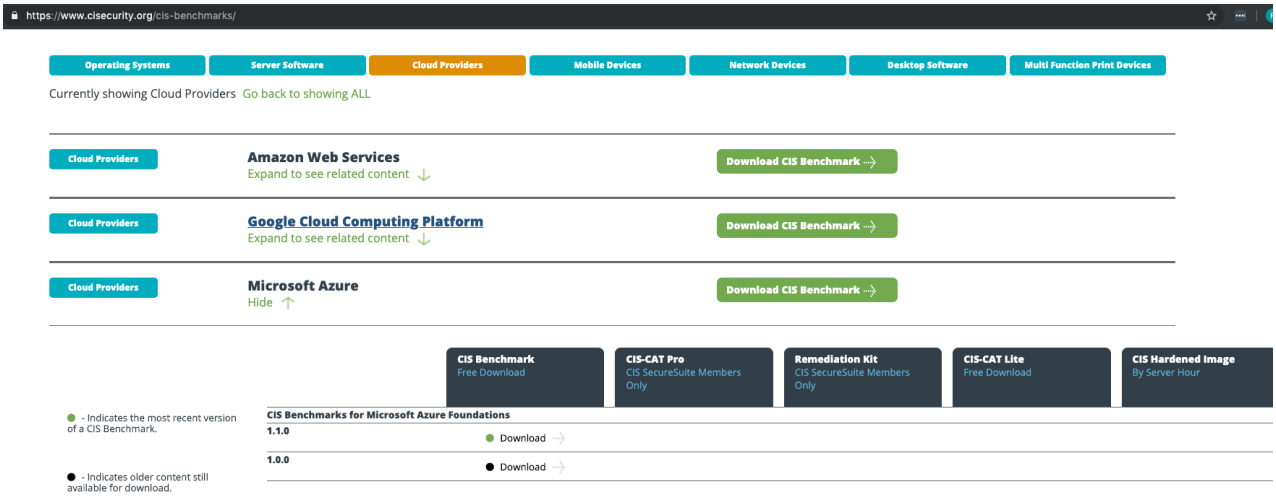


- System inventory
- Application inventory
- Data inventory

Cloud and Internet of Things (IoT)

Extend the controls to service providers

- "Traditional" 3rd party service providers
- Cloud hosting services
- IoT systems and service providers



Internet of Things (IoT)

- These “Things” are “computers”
- They have software that needs to be updated
- They provide remote access and control
- They have presence and sensing
- They are sending and receiving data
- Examples include:
- _____
- _____

26 P2P Weakness Exposes Millions of IoT Devices

APR 19

A peer-to-peer (P2P) communications technology built into millions of security cameras and other consumer electronics includes several critical security flaws that expose the devices to eavesdropping, credential theft and remote compromise, new research has found.

A map showing the distribution of some 2 million iLnkP2P-enabled devices that are vulnerable to eavesdropping, password theft and possibly remote compromise, according to new research.

The security flaws involve **iLnkP2P**, software developed by China-based **Shenzhen Yunni Technology**. iLnkP2p is bundled with millions of Internet of Things (IoT) devices, including security cameras and Webcams, baby monitors, smart doorbells, and digital video recorders.

iLnkP2P is designed to allow users of these devices to quickly and easily access them remotely from anywhere in the world, without having to tinker with one's firewall: Users simply download a mobile app, scan a barcode or enter the six-digit ID stamped onto the bottom of the device, and the P2P software handles the rest.

https://krebsonsecurity.com/2019/04/p2p-weakness-exposes-millions-of-iot-devices/

Cloud and Internet of Things (IoT)

- Cloud Security Alliance:
  https://cloudsecurityalliance.org/
- FFFIEC:
  https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf
- CIS:
  https://www.cisecurity.org/cis-benchmarks/
- NIST:
  https://www.nist.gov/topics/internet-things-iot

Summary

- Standards Based IT Operations
  - Framework based operations aligned with accepted standards:
    - CIS Critical Controls
    - FFIEC
    - NIST
  - Manage, Monitor, and Test controls

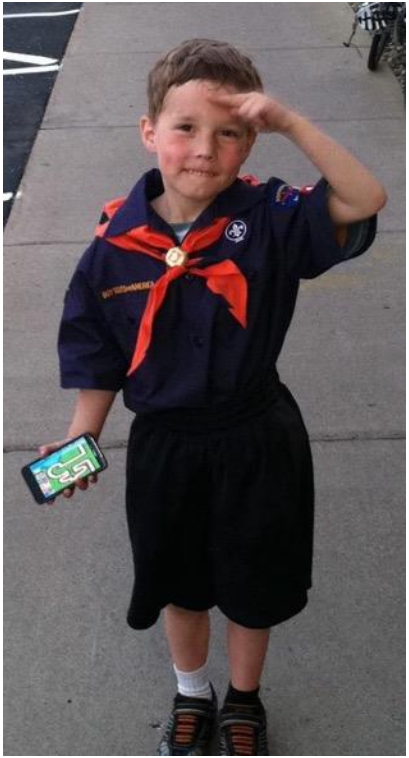
➢PRACTICE

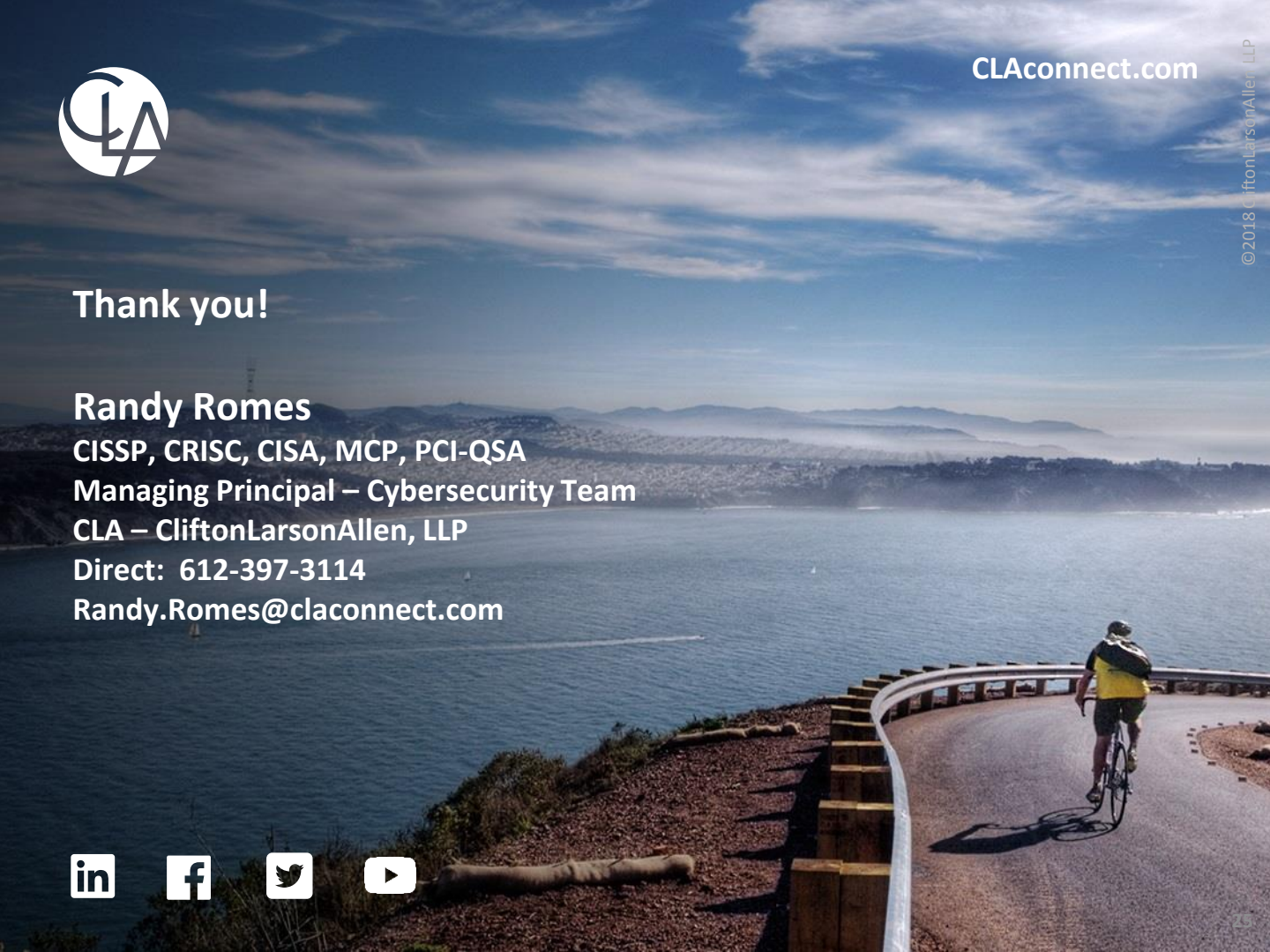
Summary

- Apply Standards and Required Controls to Your Service Providers
  - In-house/on-prem systems provided by third parties
  - Hosted/Cloud based systems and service providers
  - Awareness of IoT devices
  - Manage, Monitor and Test the systems

➢PRACTICE

Questions?





CLAconnect.com

Thank you!

Randy Romes
CISSP, CRISC, CISA, MCP, PCI-QSA
Managing Principal – Cybersecurity Team
CLA – CliftonLarsonAllen, LLP
Direct: 612-397-3114
Randy.Romes@claconnect.com