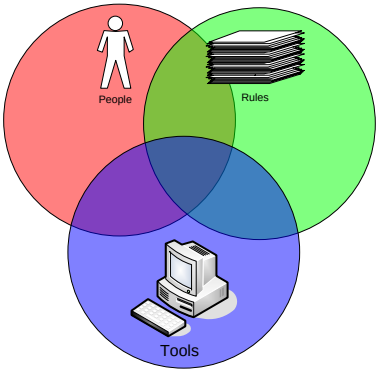
ABC's of Hardening the Network

June 2019

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Bottom Line Up Front



- Why do you have it?
- What is it supposed to do?

- Turn off the components you don't need
- Change the defaults
- Train your people
- Manage, Tune, and Monitor the systems

Federal Financial Institutions Examination Council (FFIEC) Guidelines

- FFIEC provides a handbooks for guidelines on information security
  - https://ithandbook.ffiec.gov/it-booklets/information-security/

- Cybersecurity Assessment Tool
  - CAT helps financial institutions identify risks and determine cyber attack preparedness
  - https://www.ffiec.gov/cyberassessmenttool.htm

Federal Financial Institutions Examination Council (FFIEC) Guidelines

II.C.9 Network Controls

Action Summary

Management should secure access to computer networks through multiple layers of access controls by doing the following:

- Establishing zones (e.g., trusted and untrusted) according to the risk profile and criticality of assets contained within the zones and appropriate access requirements within and between each security zone.
- Maintaining accurate network diagrams and data flow charts.
- Implementing appropriate controls over wired and wireless networks.

Networks should be protected by a secure boundary, identifying "trusted" and "untrusted" zones. Internal zones, typically trusted, should segregate various components into distinct areas, each with the level of controls appropriate to the content and function of the assets within the zone. The institution's trusted network should be protected through appropriate configuration and patch management, privileged access controls, segregation of duties, implementation of effective security policies, and use of perimeter devices and systems to prevent and detect unauthorized access. Tools used to enforce and detect perimeter protection include routers, firewalls, intrusion detection systems (IDS) and intrusion prevention systems, proxies, gateways, jump boxes,[25] demilitarized zones, virtual private networks (VPN), virtual LANs (VLAN), log monitoring and network traffic inspecting systems, data loss prevention (DLP) systems, and access control lists.

The trusted network should be further segregated into internal layers, including production, staging, and development environments. Within those environments, management should

[25] A jump box, or jump server, provides administrators with access to or control of other servers or devices in the network. Because of this capability, additional security measures should be implemented.

II.C.10(d) *Patch Management*

Frequently, security vulnerabilities are discovered in operating systems and other software after deployment. Hackers often will attempt to exploit these known vulnerabilities to try to gain access to the institution's systems. Third parties issue patches to address vulnerabilities found on institution systems and applications.[33] Management should implement automated patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) are appropriately updated. In addition, management should use vulnerability scanners periodically to identify vulnerabilities in a timely manner.

As part of the institution's patch management process, management should establish and implement the following:

- A monitoring process that identifies the availability of software patches.
- A process to evaluate the patches against the threat and network environment.
- A prioritization process to determine which patches to apply across classes of computers and applications.
- A process for obtaining, testing, and securely installing patches, including in the institution's virtual environments.
- An exception process, with appropriate documentation, for patches that management decides to delay or not apply.
- A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment in a timely manner.
- A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied.

The institution should have procedures that include how to implement patches to mitigate risks of changing systems and address systems with unique configurations. Before applying a patch, management should back up the production system. Additionally, management should define appropriate patch windows and, whenever possible, restrict the implementation of patches to defined time frames to minimize business impact or potential down time.

FFIEC Network Controls Handbook Example

Center for Internet Security (CIS) Benchmarks

- The Center for Internet Security (CIS) Benchmarks provides documented standards for internet security, CIS Benchmarks and Controls are recognized globally as a best practice for securing IT infrastructure.

- CIS Benchmark list Includes:
  - Desktop and Web Browsers
  - Mobile Devices
  - Network Devices
  - Servers and Operating Systems
  - Cloud and Virtualization Platforms
    - ◊ Amazon Web Services
    - ◊ Microsoft Suite
    - ◊ VMware
    - ◊ Google

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

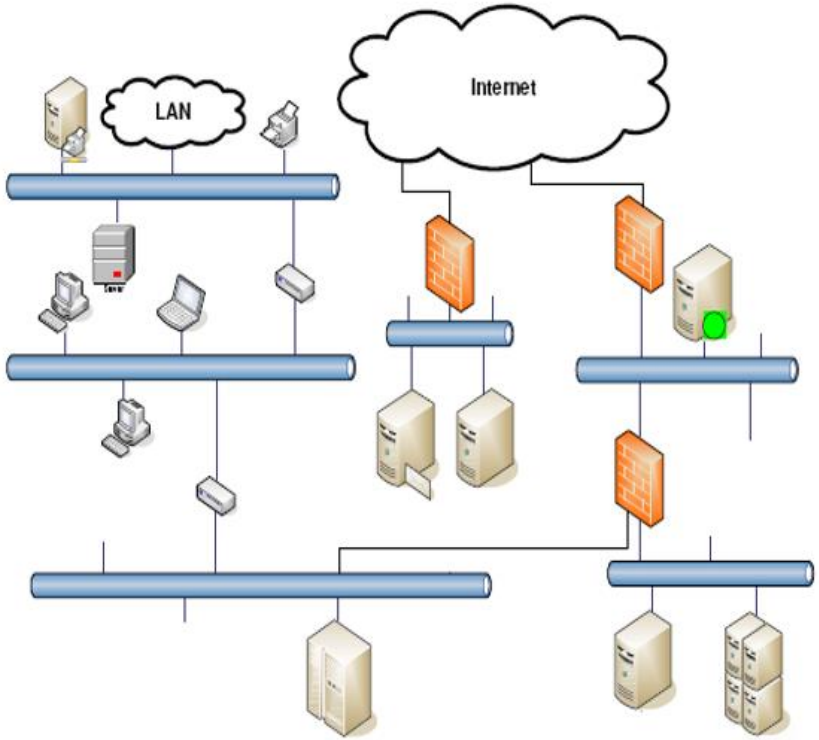
https://www.cisecurity.org/controls/

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



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

Center for Internet Security (CIS) Benchmarks

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Domain Controller**

  Items in this profile apply to Domain Controllers and intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 1 - Member Server**

  Items in this profile apply to Member Servers and intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

  Items in this profile also apply to Member Servers that have the following Roles enabled:

  - AD Certificate Services
  - DHCP Server
  - DNS Server
  - File Server
  - Hyper-V
  - Network Policy and Access Services
  - Print Server
  - Remote Access Services
  - Remote Desktop Services
  - Web Server

1.2.2 (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to `0` does not conform to the benchmark as doing so disables the account lockout threshold.

The recommended state for this setting is: `10 or fewer invalid logon attempt(s), but not 0`.

Rationale:

Setting an account lockout threshold reduces the likelihood that an online password brute force attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `10 or fewer invalid login attempt(s), but not 0`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold
```

Microsoft Windows Server 2016 CIS Benchmark example

Hardening the Network - Workstations

- Configuration hardening
  - CIS benchmarks as guidelines
- Account Controls
  - Limit local administrative privileges
  - Enforce use of strong passwords
    - Microsoft LAPS
  - Perform periodic audit scans on workstations, to ensure best practices are being followed
- Utilize local protection IE, fire-walling/anti-virus
  - Enable Host Intrusion Prevention (HIPS) if anti-virus supports
  - Ensure anti virus definitions are kept up to date
- Patching
  - Keep all systems up to date
  - Validate patching effectiveness with authenticated vulnerability scans
- Third party software should be update to date or removed

Hardening the Network – Firewalls

- Configuration hardening
  - CIS benchmarks keep all firewalls operating systems up to date
- Configure strong non default passwords
- Harden/tune your rules
  - Document the business need
- Document configuration changes and exceptions
- SSL/Egress filtering
- Web content filtering
- Enable SSL Inspection
  - Palo Alto
- Enabling intrusion prevention
  - Palo Alto/Checkpoint

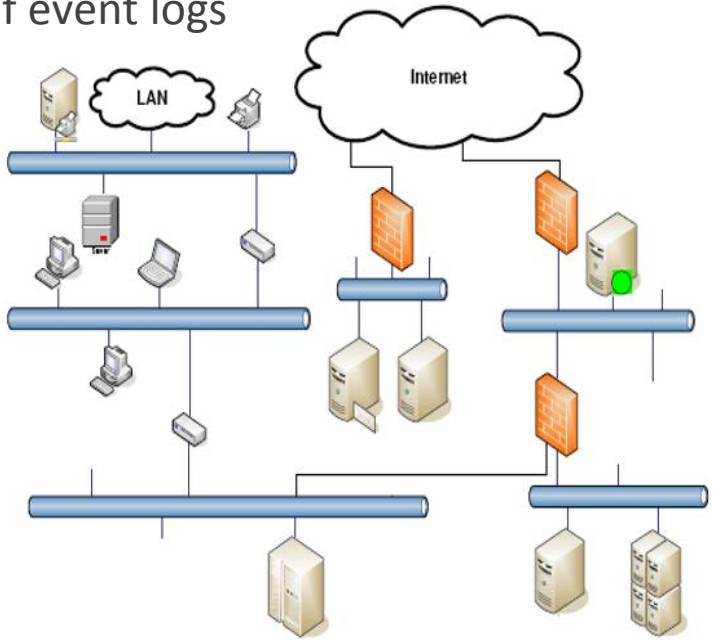
Hardening the Network – Internet of Things (IoT)

- Inventory authorized devices and software
- Secure configurations
  - Understand connectivity and data “collection”
  - IoT devices typically lack the range of configuration changes that workstations and servers offer, when configuration options are available, they should be reviewed and a baseline of these controls as a best practice.
- Isolation and segmentation
- Vulnerability Assessments
  - Perform regular vulnerability assessments, as if any other device on the network

Log Files

Centralization and Correlation of event logs

- Centralize
- Secure
- Programmatically process
- Retention
  - System and application logs
  - Critical data systems/files
  - Key system configurations
  - Data activity and flow
  - Accounts



6 Maintenance, Monitoring and Analysis of Audit Logs

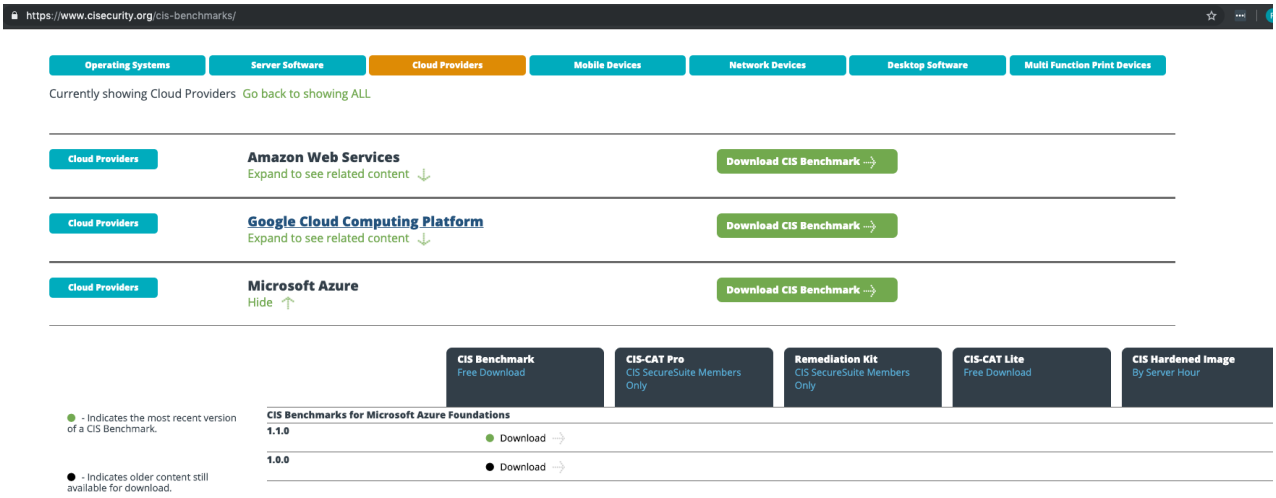
Common Security Issues

- Default credentials
- Legacy protocols in use
- SIEMs, HIPS, end-point controls not being utilized
- Excessive user account permissions
- Little to no segmentation in place
- Insecurely configured services and software
- Password polices not meeting best practice
- Missing critical security patches

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 iLinkP2P-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.

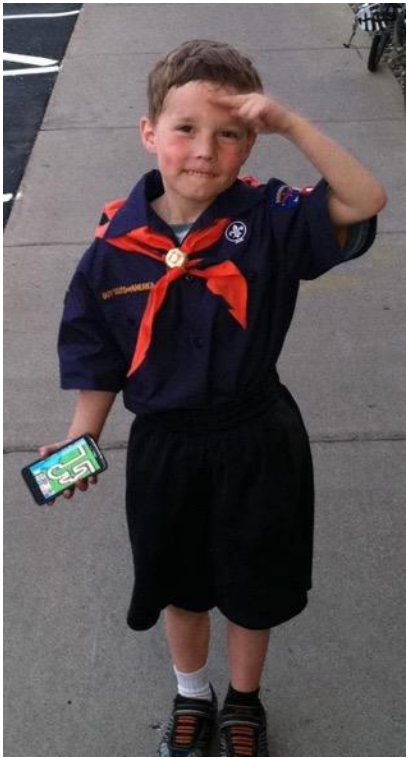
iLnkP2P is designed to allow users of these devices to quickly and easily access them remotely from anywhere in the world, without having to tinker with one's firewall: Users simply download a mobile app, scan a barcode or enter the six-digit ID stamped onto the bottom of the device, and the P2P software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

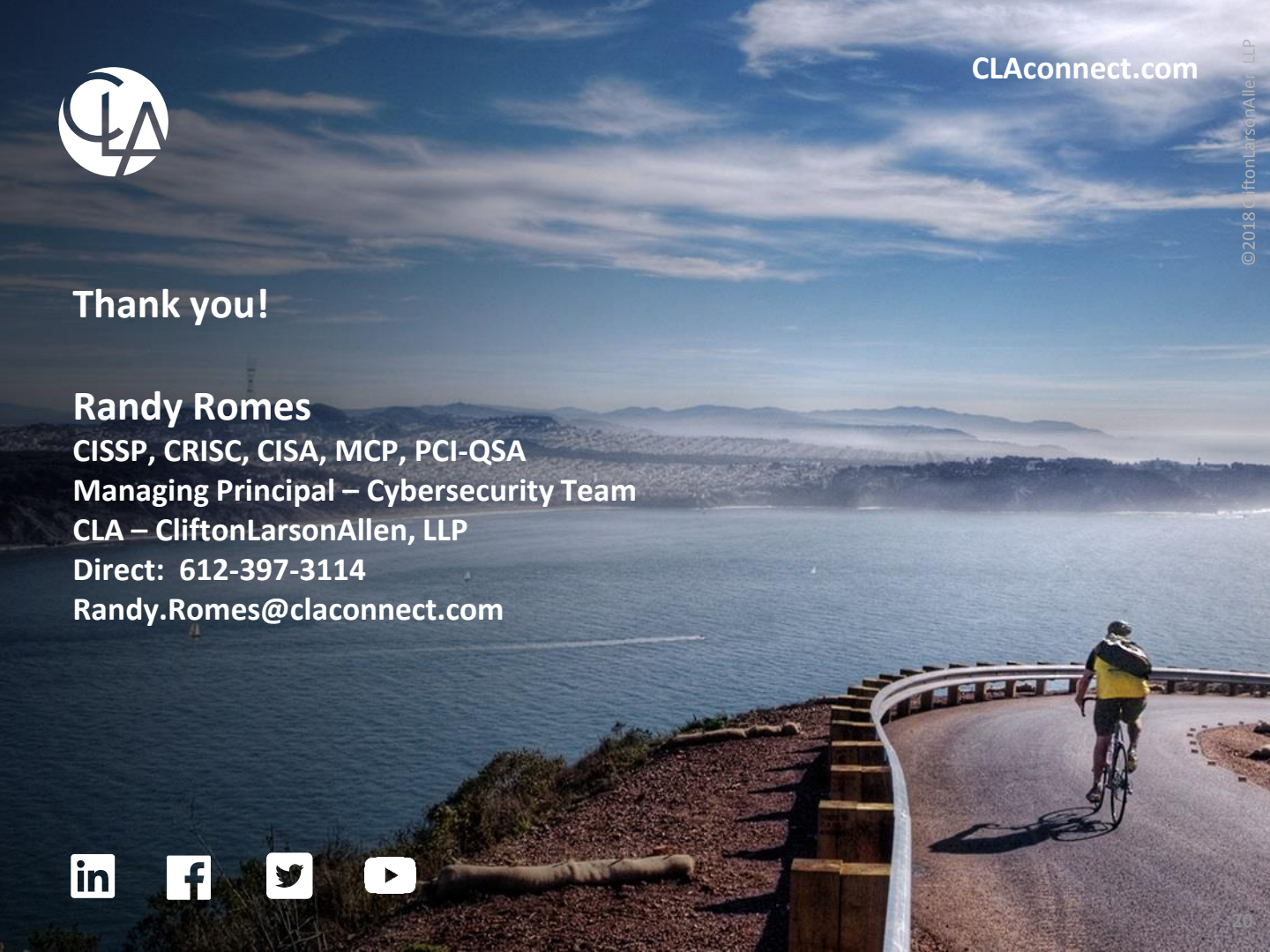
https://krebsonsecurity.com/2019/04/p2p-weakness-exposes-millions-of-iot-devices/

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

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