June 2019

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

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

Cloud Cyber Security

Create Opportunities

We promise to know you and help you.

CLA – A Professional Services Firm

- A professional services firm with three distinct business lines
  - Wealth Advisory
  - Outsourcing
  - Audit, Tax, and Consulting

- More than 6,500 employees
- Offices coast to coast
- Serve more than 1,500 financial institutions

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.

Cyber Security Capabilities

Information Security offered as specialized service offering for over 20 years

- Largest Credit Union Service Practice*

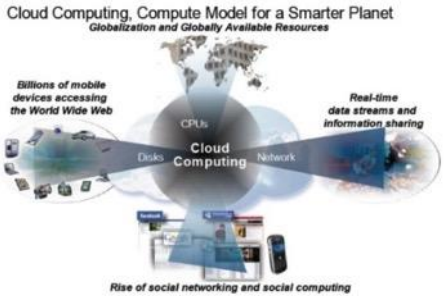
- Penetration Testing and Vulnerability Assessment
  - Red Team, Black Box, and Collaborative Assessments
- IT/Cyber security risk assessments
- IT audit and compliance (GLBA, FFIEC, CIS, etc…)
- PCI-DSS Readiness and Compliance Assessments
- Incident response and forensics
- Cybersecurity architecture
- Independent security consulting
- Internal audit support

*Callahan and Associates 2018 Guide to Credit Union CPA Auditors.

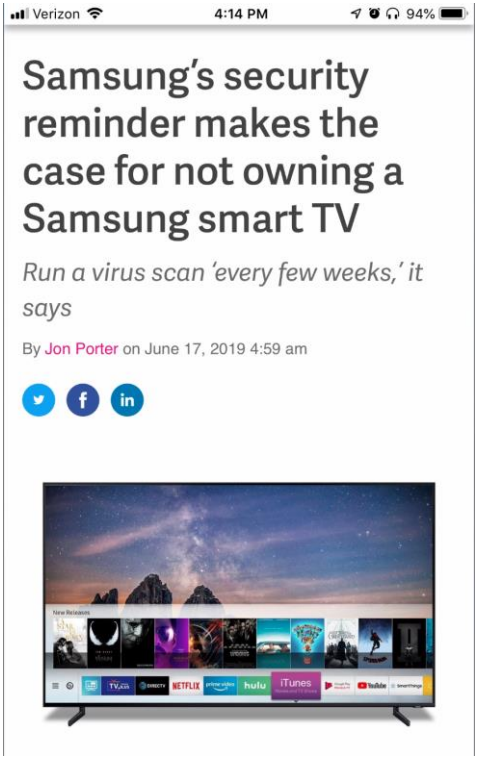
C:\whoami

- “Professional Student”
- Science Teacher/Self Taught Computer Guy
- IT Consultant - Project Manager → IT Staff/Help Desk → Hacker
- Assistant Scout Master (Boy Scouts)

Raise Your Hand If…



When a TV is NOT a TV…

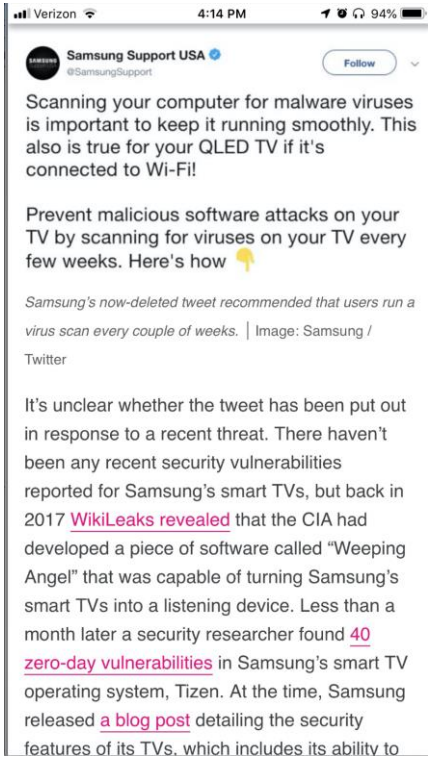


Verizon 4:14 PM 94%

Samsung's security reminder makes the case for not owning a Samsung smart TV

Run a virus scan 'every few weeks,' it says

By Jon Porter on June 17, 2019 4:59 am



Verizon 4:14 PM 94%

Samsung Support USA
@SamsungSupport
Follow

Scanning your computer for malware viruses is important to keep it running smoothly. This also is true for your QLED TV if it's connected to Wi-Fi!

Prevent malicious software attacks on your TV by scanning for viruses on your TV every few weeks. Here's how 👇

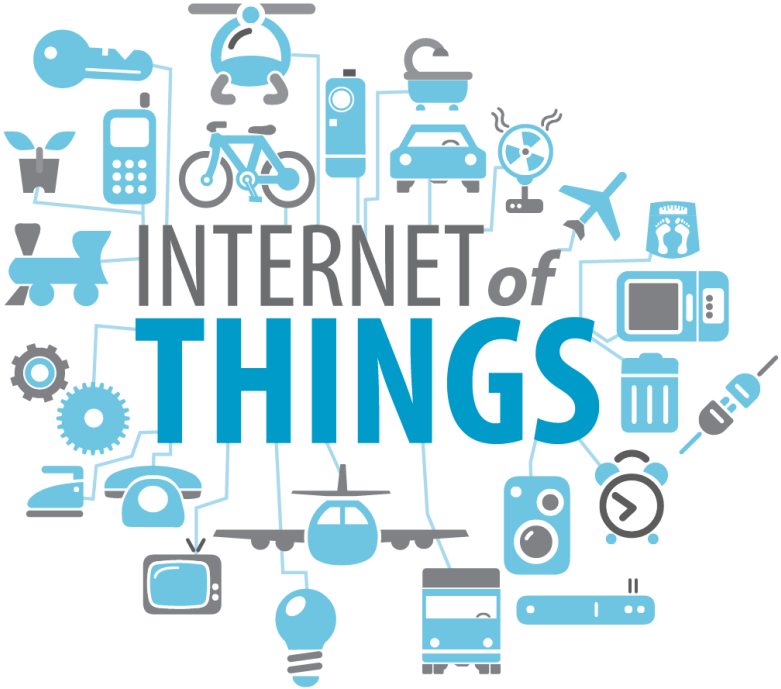
Samsung's now-deleted tweet recommended that users run a virus scan every couple of weeks. | Image: Samsung / Twitter

It's unclear whether the tweet has been put out in response to a recent threat. There haven't been any recent security vulnerabilities reported for Samsung's smart TVs, but back in 2017 WikiLeaks revealed that the CIA had developed a piece of software called "Weeping Angel" that was capable of turning Samsung's smart TVs into a listening device. Less than a month later a security researcher found 40 zero-day vulnerabilities in Samsung's smart TV operating system, Tizen. At the time, Samsung released a blog post detailing the security features of its TVs, which includes its ability to

https://www.theverge.com/2019/6/17/18681683/samsung-smart-tv-virus-scan-malware-attack-tweet

Everything Can Talk to Everything….

- Security cameras
- HVAC systems
- Door sensors and proximity readers
- "Chrome wants to remember your location…"
- "Hey Alexa, what's my balance?"
- ➢ **"Presence"**



Sun Tzu:

"Know your enemy and know yourself and you can fight a hundred battles without disaster"

The Current State of Cybercrime

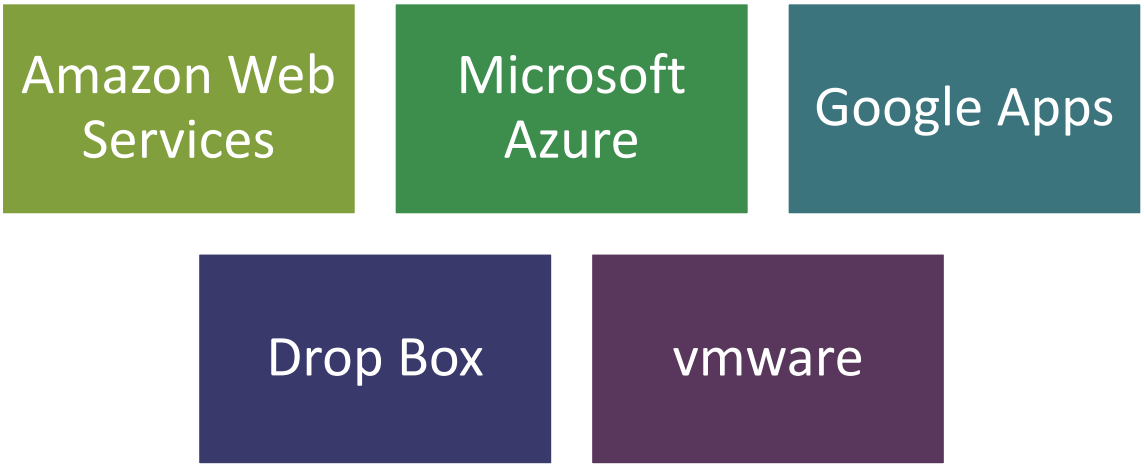
WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

What is the Cloud – The Old Cloud

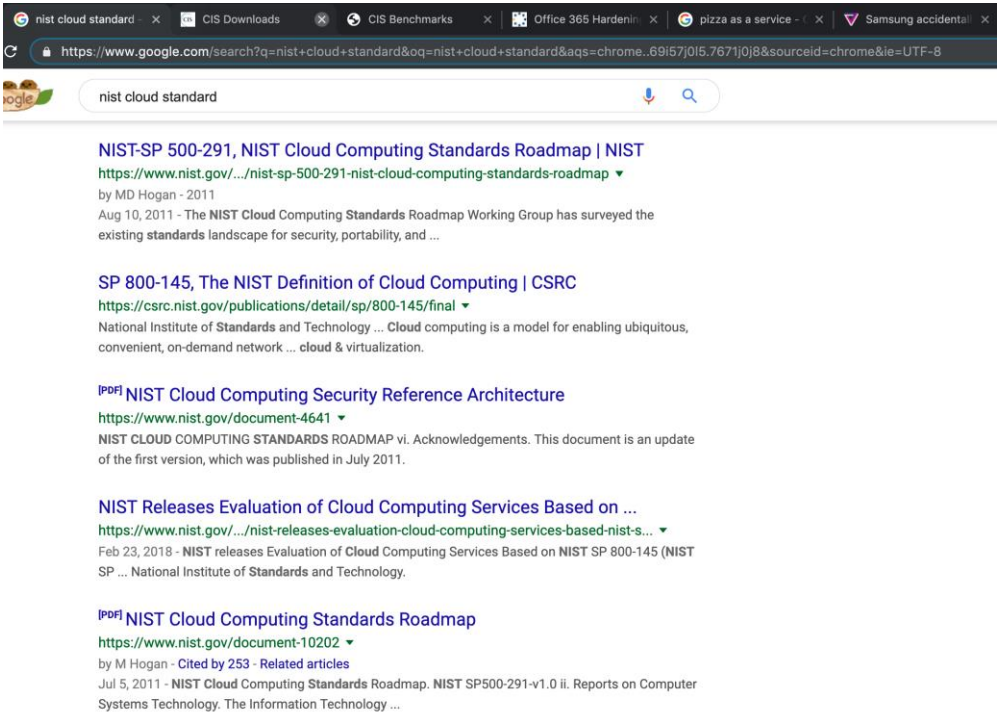
- The original “cloud computing”:

What is the Cloud – The New Cloud

- Today's cloud: Hosted service or process all the way to hosted infrastructure.



Google… NIST Cloud Standard



Standards Have Been In Place…

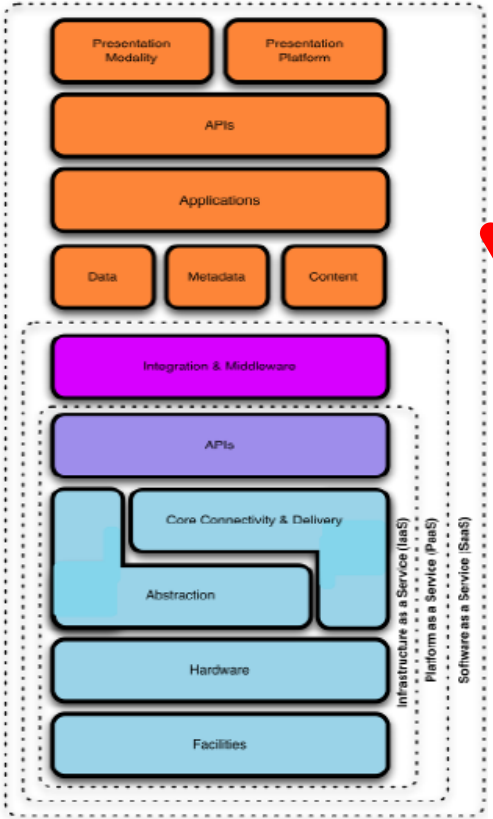
National Institute of Standards and Technology (NIST) definition of cloud computing published October 7, 2009:

"Cloud computing is a model for enabling convenient, on-demand network access to **a shared pool of configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Three Cloud Computing Service Models

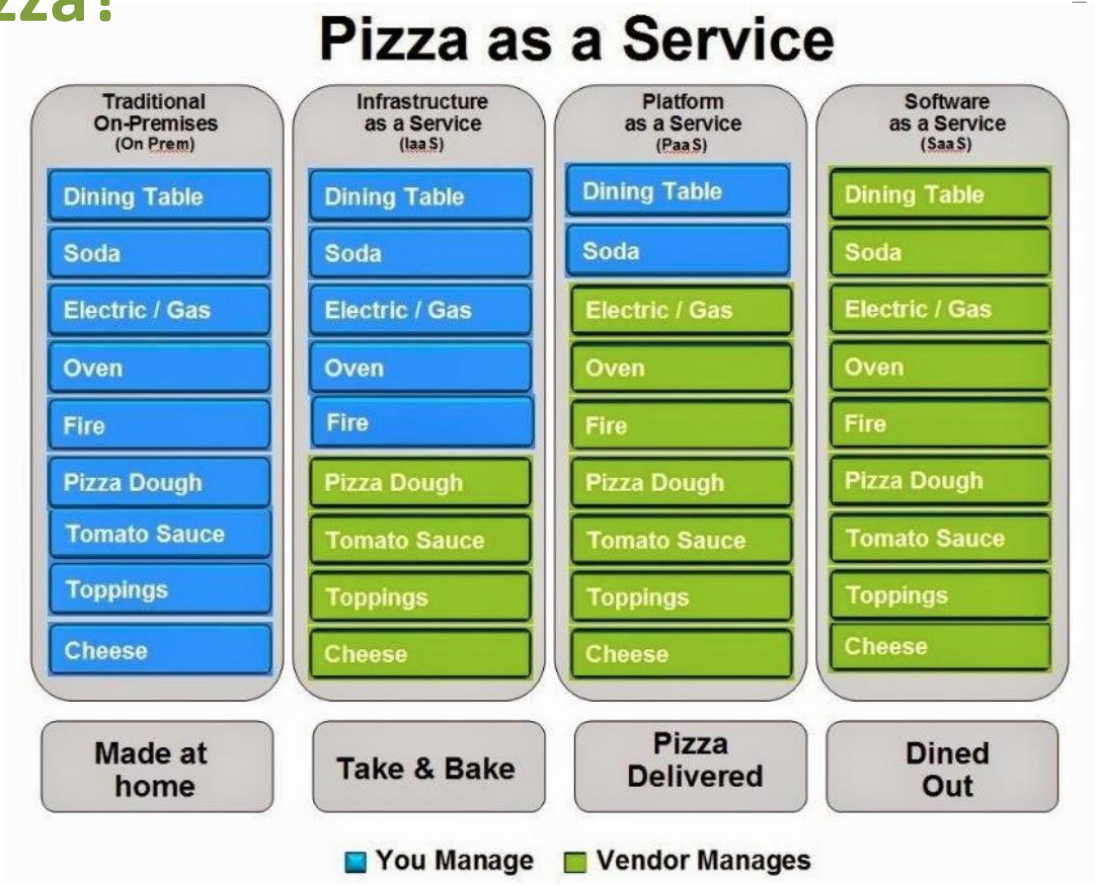
- Software as a Service (SaaS)
  - Capability to **use the provider's applications** that run on the cloud infrastructure.
- Platform as a Service (PaaS)
  - Capability to deploy onto the cloud infrastructure **customer-created or acquired applications** created using programming languages and tools supported by the provider
- Infrastructure as a Service (IaaS)
  - Capability to provision **processing, storage, networks and other fundamental computing resources** that offer the customer the ability to deploy and run arbitrary software, which can include operating systems and applications

Cloud Computing Service Models



- Multi-tenancy…
- The lower down the stack the cloud service provider stops --
- The more capabilities and management the users are responsible for implementing and managing themselves

Cloud Pizza?


Pizza as a Service
Traditional On-Premises (On Prem)
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Dining Table
Soda
Electric / Gas
Oven
Fire
Pizza Dough
Tomato Sauce
Toppings
Cheese
Made at home
Take & Bake
Pizza Delivered
Dined Out
You Manage
Vendor Manages

Cloud Computing Controls

- Cloud computing means:
  - An increased need for good polices
  - Clear communication between the provider and the consumer of the services
  - **Understanding of providers responsibilities and your responsibilities**
  - Ownership and governance of the relationship with the provider.

Cloud Computing Deployment Models

- **Private cloud:** *(You probably already have this…)*
  - Operated solely for an organization
- **Community cloud:**
  - Shared by several organizations
  - Supports a specific community that has a shared mission or interest
- **Public cloud:** *(You are probably using this…)*
  - Made available to the general public or a large industry group
  - Owned by an organization that sells cloud services
- **Hybrid cloud:**
  - Composed of two or more clouds (private, community or public) that remain unique entities

Cloud Computing Controls

- The overall control domains are the same as an in house IT environment

➢ **The challenge is to figure out who is doing what**

➢ **YOU are still responsible…**

Domain	Focus
Organization and Management Controls	• IT Organization & Governance • Policies, Standards & Guidelines • Personnel Administration • Vendor Administration, including External Dependency Management • Technology Administration • Cyber Risk Management & Oversight • Threat Intelligence & Collaboration
Technical Infrastructure	• Technical Documentation & Illustration(s) • Network Administration • Server Administration • Workstation Administration • Peripheral Administration • Cybersecurity Controls
Software Administration	• Software Asset Administration • Software Development Administration • Software Change Management
Data Administration	• Data Management • Database Administration (*If Applicable*) • Data Transfer(s) Administration • Data Storage & Backup Administration
Application Administration *(For Each "In Scope" Application)*	• Access Controls & Permissions • Business Rules/Parameters • Data Input/Processing/Output • Data Maintenance • Activity Logging/Monitoring
IT Operations & Support	• User Account Administration • IT Systems Operations • Problem Management (*Help Desk*)
Physical Environment	• Physical Security • Environment Controls
Business Continuity	• Incident Response Management and Resilience • Disaster Recovery

Cloud Computing Controls

- Controls in the cloud computing environment may be provided by the consumer/company, the cloud service provider, or a separate 3rd party.

- SSAE 16/18 SOC2 report from service providers

Cloud Computing

Activity :

- Describe an outsourced (cloud) IT service relationship in place at your credit union
  - What do they do/manage for you (data, processes, etc…)
  - How do they interact with you
  - What are the service provider's responsibilities and what your credit union staff's responsibilities
  - What is the Service Model
  - What is the Deployment Model

Cloud Computing

Activity :

- Describe an outsourced (cloud) IT service relationship in place at your credit union
  - What security measures do you think/assume they now take care of for you?
  - Who at the credit union is an expert for your credit unions cloud based system?

    (Are they an engineer, mechanic, or uber driver?)

Internet of Things (IoT)

http://krebsonsecurity.com/

Convert Select

Other — 45 comments

13 IoT Devices as Proxies for Cybercrime

OCT 16

Multiple stories published here over the past few weeks have examined the disruptive power of hacked "Internet of Things" (IoT) devices such as routers, IP cameras and digital video recorders. This post looks at how crooks are using hacked IoT devices as proxies to hide their true location online as they engage in a variety of other types of cybercriminal activity — from frequenting underground forums to credit card and tax refund fraud.

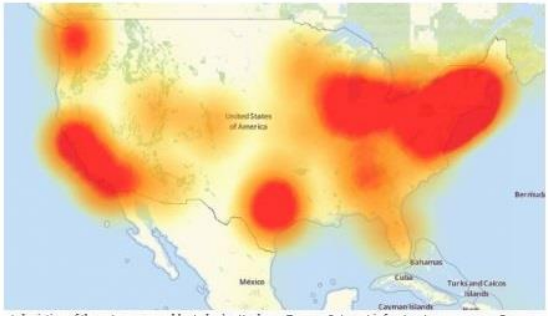
Recently, I heard from a cybersecurity researcher who'd created a virtual "honeypot" environment designed to simulate hackable IoT devices. The source, who asked to remain anonymous, said his honeypot soon began seeing traffic destined for **Asus** and **Linksys** routers running default credentials. When he examined what that traffic was designed to do, he found his honeypot systems were being told to download a piece of malware from a destination on the Web.

21 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

OCT 16

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

At first, it was unclear who or what was behind the attack on Dyn. But over the past few hours, at least one computer security firm has come out saying the attack involved **Mirai**, the same malware strain that was used in the record 620 Gpbs attack on my site last month. At the end September 2016, the hacker responsible for creating the Mirai malware released the source code for it, effectively letting anyone build their own attack army using Mirai.

Mirai scours the Web for IoT devices protected by little more than factory-default usernames and passwords, and then enlists the devices in attacks that hurl junk traffic at an online target until it can no longer accommodate legitimate visitors or users.

According to researchers at security firm Flashpoint, today's attack was launched at least in part by a Mirai-based botnet. **Allison Nixon**, director of research at Flashpoint, said the botnet used in today's ongoing attack is built on the backs of hacked IoT devices — mainly compromised digital video recorders (DVRs) and IP cameras made by a Chinese hi-tech company called **XiongMai Technologies**. The components that XiongMai makes are sold

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/

Examples closer to home…

- Business Email Compromise
- Persuasion Attack
- RDP compromise… leads to Ransomware

The Boy Scouts Motto:

"Be Prepared"

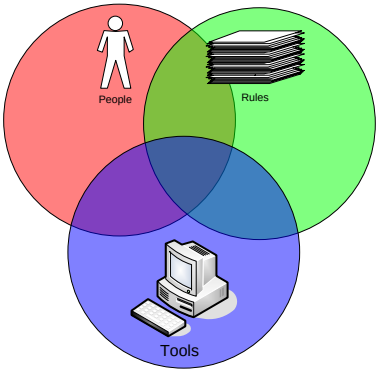
Strategies and Action Items

Strategies

Our information security strategy should have the following objectives:

- Users who are aware and savvy
- Systems that are hardened and resistant to malware and attacks
- Resilience Capabilities: Monitoring, Incident Response, Testing, and Validation

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, NCUA 748 A&B, etc…
  - PCI – DSS
  - CIS Critical Controls, NIST, ISO

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

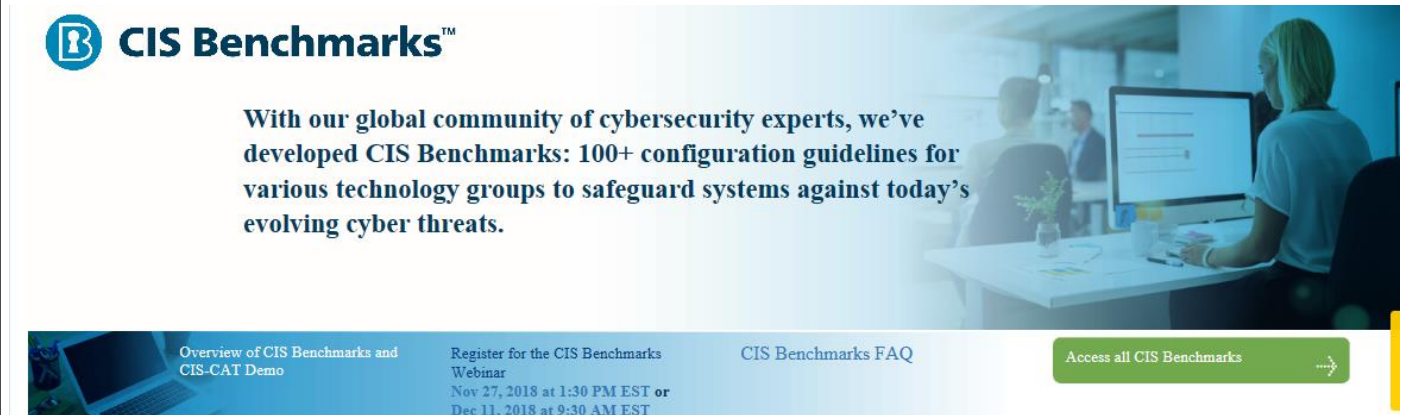
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

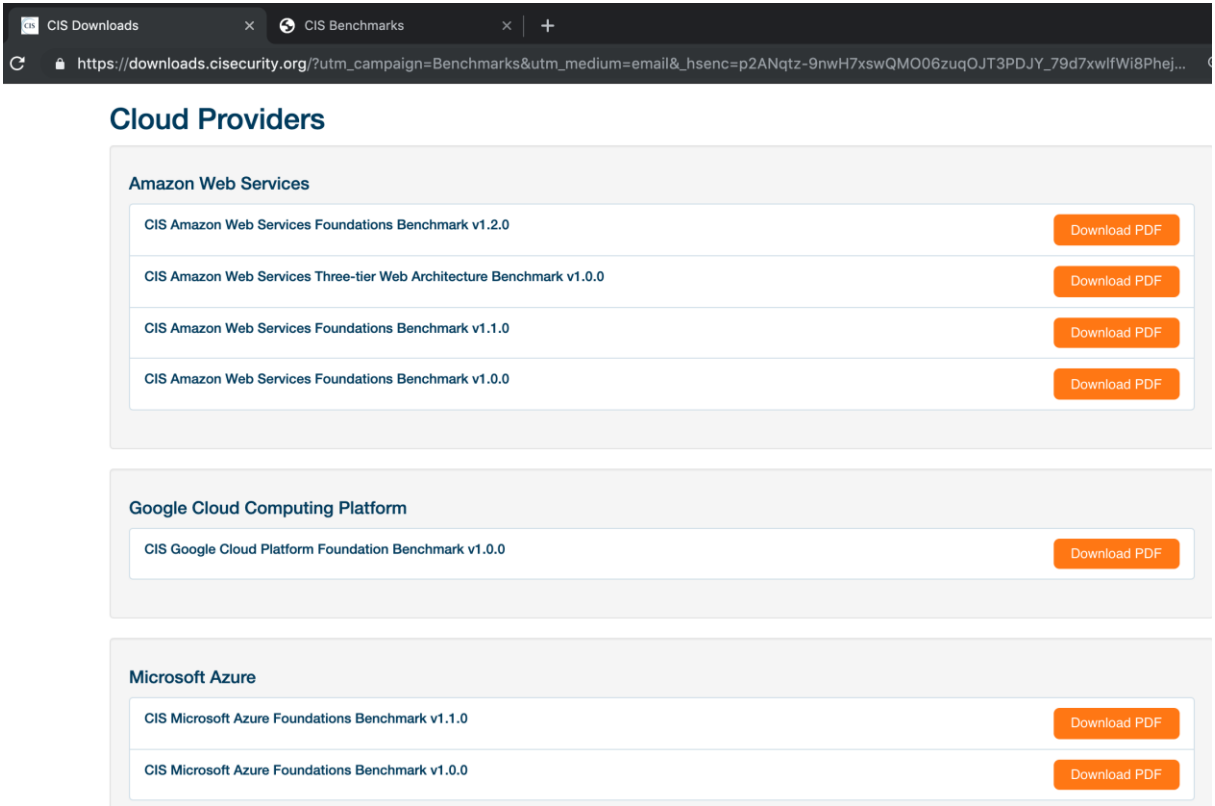
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

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

CIS Benchmarks



CIS Cloud Standards and Benchmarks



Microsoft Office 365

Limit or Disable Remote Access

- The majority of email compromises occur through Outlook web access (OWA). Disabling OWA for the organization or enabling it only on an as-needed, per-user basis offers additional protection to your organization.
- By default, Office 365 allows access via POP3, IMAP, MAPI, EWS, OWA, and ActiveSync for every system user.
  - Users rarely need access using all of these methods.
  - Does your organization use POP3 or IMAP for email connections regularly?
  - If not – disable them.

Require Multi-factor Authentication (MFA)

- The most important thing you can do to protect your organization is to require MFA for users to log in to O365. Microsoft provides guidance for O365 administrators:
  - Set up multi-factor authentication for Office 365 users
  - Plan for multi-factor authentication for Office 365 deployments

- Users should select the MFA mobile app for authentication.
  - SMS (text message)-based MFA is **no longer regarded as secure** because of SIM swaps and other social engineering risks.

Manage Message Forwarding

- Cybercriminals often set up inbox rules to forward messages to an external account or to delete messages in order to hide them from the inbox owner. Sometimes the only sign of an account takeover is the presence of unauthorized mailbox rules.
- From an administrative level, you can configure O365 to alert you every time a user sets up a new inbox rule, which can then be followed up on to check the legitimacy of the rule.
- If there isn't a business need for them, it's even more secure to disable forwarding and deletion rules for all users and enable them as needed only for specific users
- Office 365: Determine accounts that have forwarding enabled

Turn On Audit Logging & Mailbox Auditing

- Without the proper logs, you have to assume the bad actor accessed everything, which can lead to having to provide notification to individuals whose information may not even have been affected.
- To provide useful logs, you need to:
  1. Turn ON audit logging and
  2. Enable mailbox auditing for each user mailbox.
     - By default, audit logging and mailbox auditing are not turned on. Microsoft has plans to change that soon. You need to turn on both *before you experience an incident* for the logs to be helpful.
- Search the audit log in the Office 365 Security & Compliance Center
- Enable mailbox auditing in Office 365
- Consider extending the retention time for logs beyond the default 90 days if resources permit.

Tools To Manage Configuration Changes

- Microsoft provides information about how to use Powershell to manage your O365 configuration.
- Manage Office 365 with Office 365 PowerShell
- Connect to Office 365 PowerShell

- Other resources to (open-source script) to help automate the process.
- Secure Your Office 365 Accounts
- https://github.com/LMGsec/O365-Lockdown

Disciplined Exception Control, Vulnerability Management and Monitoring

- Monitoring (“built in”)
  - Key system configurations
  - System and application logs
  - Accounts
  - Critical data systems/files
  - Data activity and flow

- Scanning/testing (independent)
  - Patch Tuesday and vulnerability scanning
  - Rogue devices

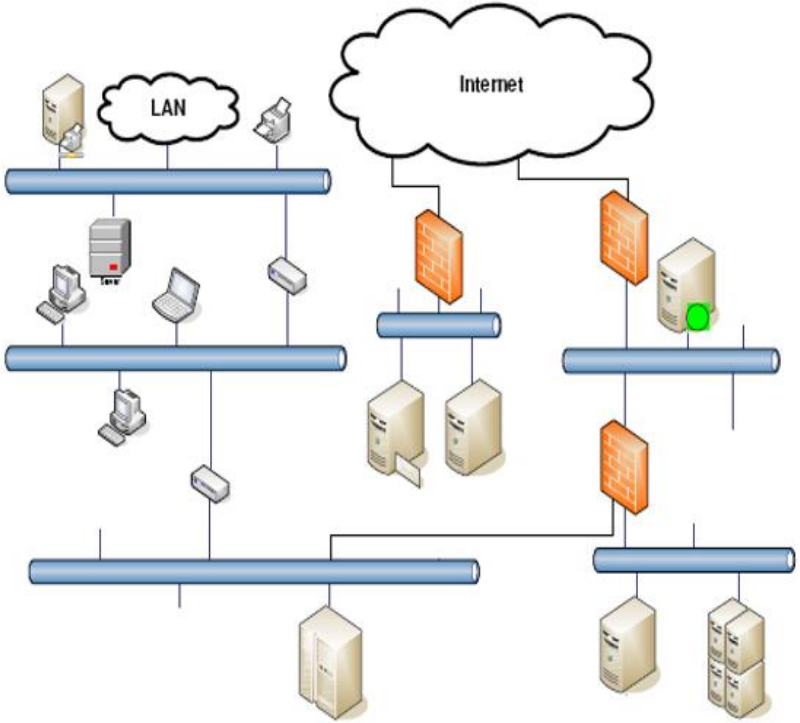
Passwords

- Good Passwords
- Password Managers
- Two Factor / Multi-Factor Authentication

Password Audit	Total
Number of passwords audited	855
Passwords cracked	794
Passwords that were all letters	63
Passwords that were all numbers	5
Passwords that were an English word	20
Passwords that were a word with numbers appended to it	200
Passwords that were the same as the username	6
Passwords that do not meet Windows complexity	584

Know Your Network
Know What "Normal" Looks Like

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



- System inventory
- Application inventory
- Data inventory

Audit Logs and Password Auditing

- Configure system auditing/logging
  - Understand and document logging capabilities
  - Ensure all systems are configured to log important information
  - Retain logs for at least 1 year, longer is better

- Audit systems for default/weak passwords
  - Most systems have default passwords
    - ◊ Google: “Default password list”
  - Don’t overlook “simple” systems
    - ◊ E.g. Printer/multi-function devices, IP security cameras, etc.
    - ◊ IoT devices…

Action Items

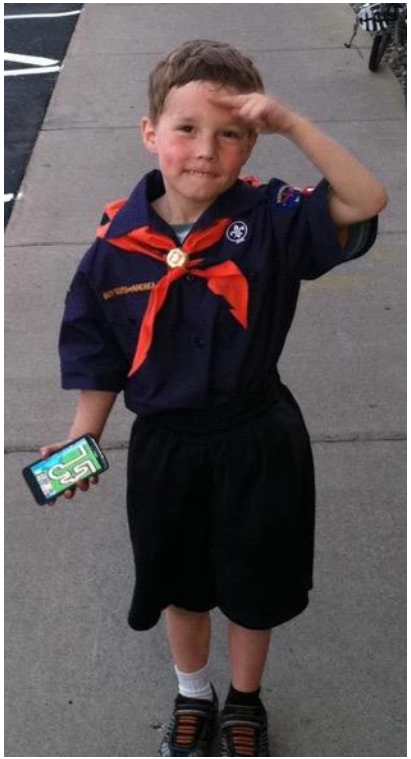
- Review and Validate Your Design
  - Do NOT wait till after you are “in the cloud”
  - Independently validate design
  - Test design BEFORE full production use
  - Periodically test the implemented design
    (it changes more often then on-prem systems)

➢PRACTICE

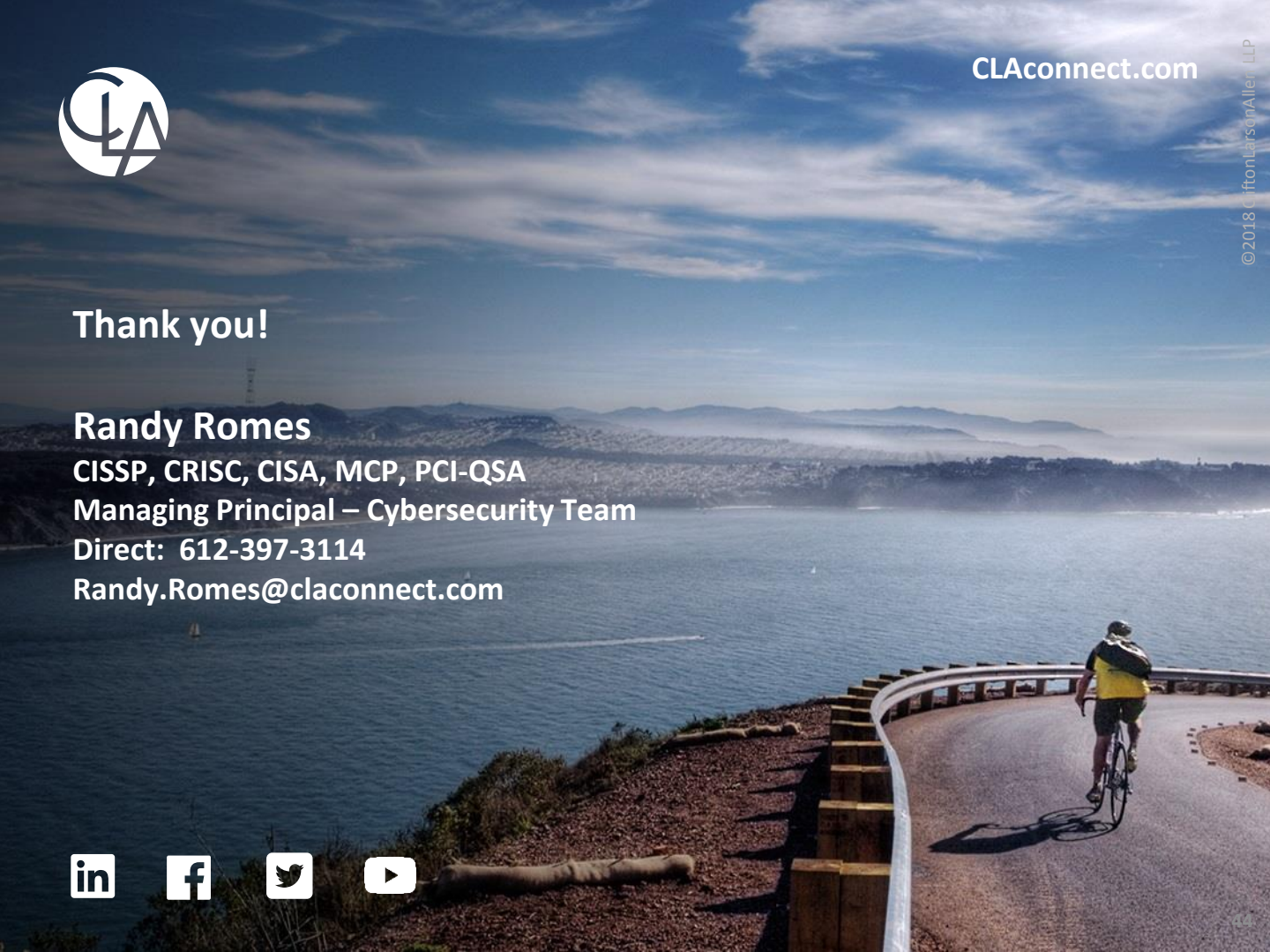
Action Items

- TEST systems and people - Validate that your expectations are being met for cybersecurity
  - Penetration Testing
    - ◊ Collaborative/Informed/White Box
    - ◊ Uninformed/Black Box
  - Social Engineering Testing
  - True Breach Simulation
    - ◊ Red Team/Blue Team

➢PRACTICE



Questions?



CLAconnect.com

Thank you!

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