Credit Union National Association
CUNA

NASCUS
The National Voice of the State Credit Union System

Cybersecurity Emerging Trends and Threats

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

C:\whoami

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

Credit Union National Association CUNA

NASCUS The National Voice of the State Credit Union System

Cyber Security Capabilities

Information Security Thought Leadership and Service 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, FFIECI, CIS, etc…)
- PCI-DSS Readiness and Compliance Assessments
- Incident response and forensics
- Independent security consulting
- Internal audit support

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

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports ®

PCI Security Standards Council ®

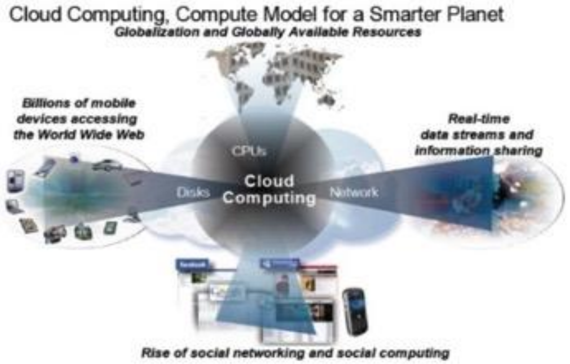
HITRUST
Authorized CSF Assessor

CUNA Credit Union National Association

NASCUS
The National Voice of the State Credit Union System

Raise Your Hand If…

Body Gateway
PAN
WAN
Care Server
Internet
Internet
ADSL
PAN
PAN
Off-body sensors


Cloud Computing, Compute Model for a Smarter Planet
Globalization and Globally Available Resources
Billions of mobile devices accessing the World Wide Web
Real-time data streams and information sharing
CPUs
Disks
Cloud Computing
Network
Rise of social networking and social computing

amazon tap

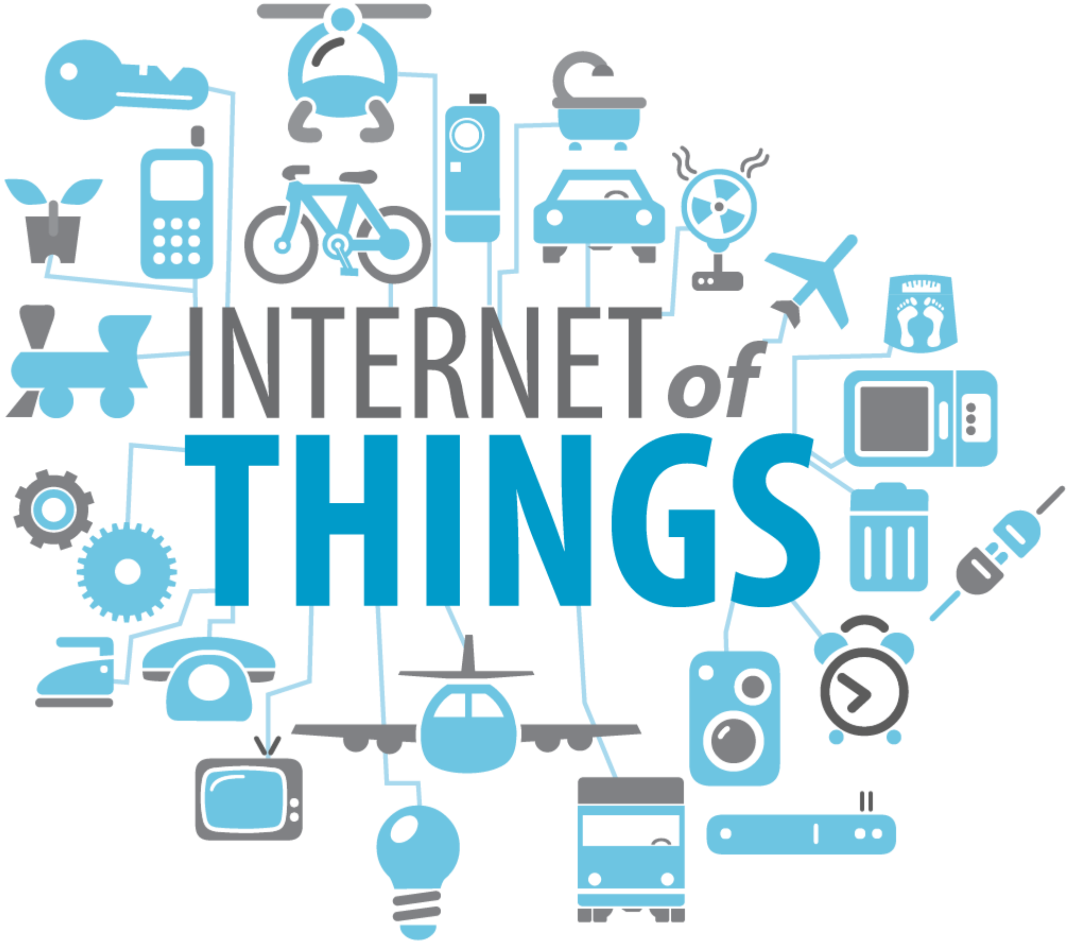
ALEXA-ENABLED
PORTABLE SPEAKER

JUST TAP & ASK

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"**



Credit Union National Association
CUNA

NASCUS
The National Voice of the State Credit Union System

Sun Tzu:
“Know your enemy and know yourself and you can fight a hundred battles without disaster”

The Current State of Cybercrime

Credit Card Breaches in the News
(Two Years Ago…)

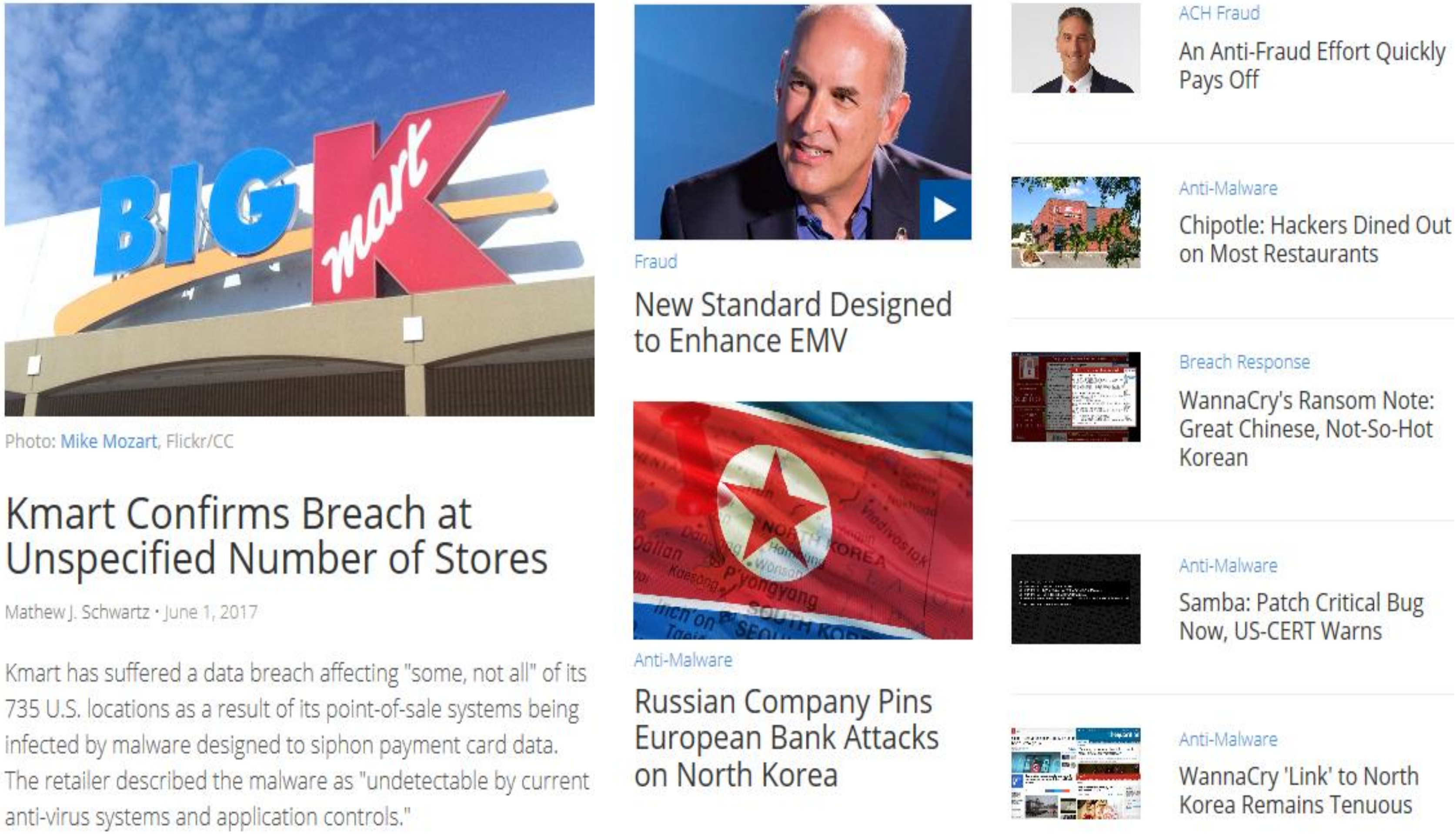


Photo: Mike Mozart, Flickr/CC

Kmart Confirms Breach at Unspecified Number of Stores

Mathew J. Schwartz • June 1, 2017

Kmart has suffered a data breach affecting "some, not all" of its 735 U.S. locations as a result of its point-of-sale systems being infected by malware designed to siphon payment card data. The retailer described the malware as "undetectable by current anti-virus systems and application controls."

Fraud

New Standard Designed to Enhance EMV

Anti-Malware

Russian Company Pins European Bank Attacks on North Korea

ACH Fraud

An Anti-Fraud Effort Quickly Pays Off

Anti-Malware

Chipotle: Hackers Dined Out on Most Restaurants

Breach Response

WannaCry's Ransom Note: Great Chinese, Not-So-Hot Korean

Anti-Malware

Samba: Patch Critical Bug Now, US-CERT Warns

Anti-Malware

WannaCry 'Link' to North Korea Remains Tenuous

Credit Union National Association CUNA

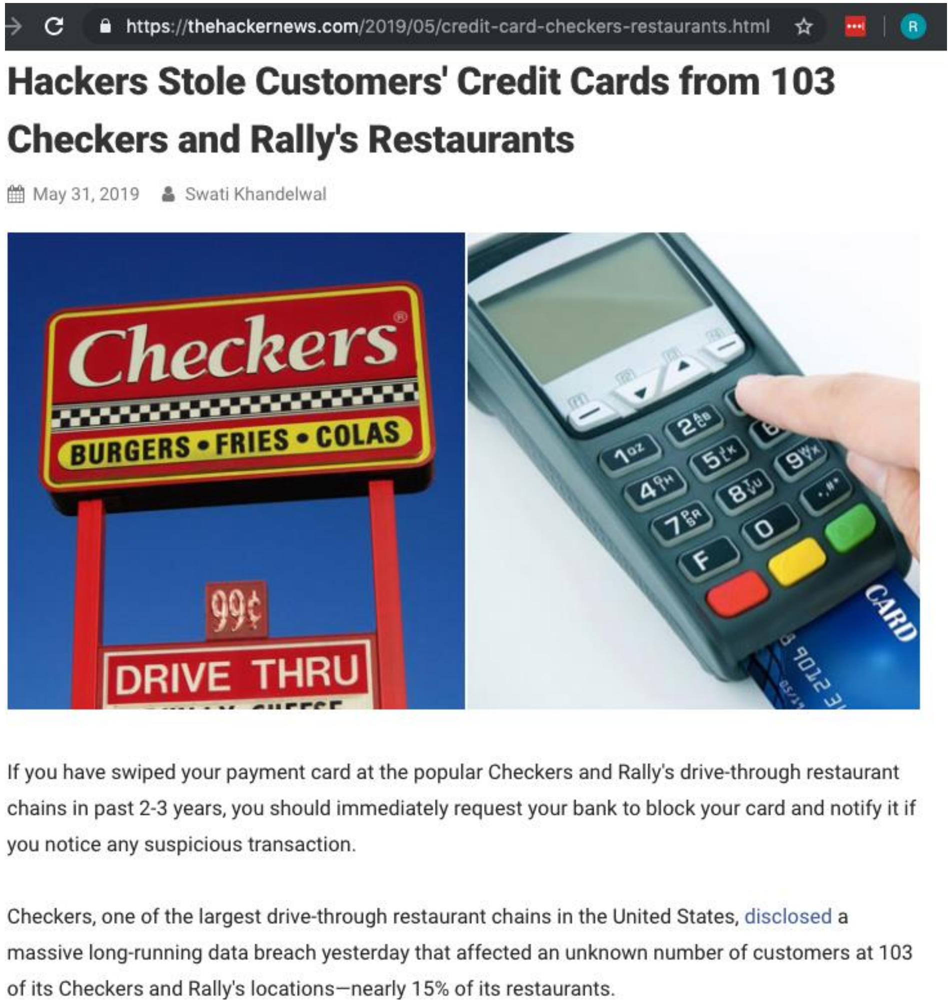
NASCUS The National Voice of the State Credit Union System

Credit Card Breaches in the News

(Two Years Ago…)

"…The PoS malware was designed to collect information stored on the magnetic stripe of payment cards, including cardholder's name, payment card number, card verification code, and expiration date.

However, the company pointed out that the investigation found no evidence suggesting that hackers made off with **additional information** belonging to the affected cardholders, and that "not all guests who visited the listed restaurants" are affected by the breach…."



https://thehackernews.com/2019/05/credit-card-checkers-restaurants.html

Hackers Stole Customers' Credit Cards from 103 Checkers and Rally's Restaurants

May 31, 2019 Swati Khandelwal

If you have swiped your payment card at the popular Checkers and Rally's drive-through restaurant chains in past 2-3 years, you should immediately request your bank to block your card and notify it if you notice any suspicious transaction.

Checkers, one of the largest drive-through restaurant chains in the United States, disclosed a massive long-running data breach yesterday that affected an unknown number of customers at 103 of its Checkers and Rally's locations—nearly 15% of its restaurants.

Largest Cyber Fraud Trends - Motivations

- Black market economy to support cyber fraud
- Business models and specialization

- Most common cyber fraud scenarios we see affecting our clients
- Theft of Credentials &
- Account take overs
- Theft of PII and PFI
- Theft of credit card information
- Ransomware and Interference
- w/ Operations

Credit Union National Association CUNA

NASCUS The National Voice of the State Credit Union System

Firewalls are Hard to Break People on the Other Hand…

Social Engineering Improves the Hackers Odds

What Makes Social Engineering Successful?

“Amateurs hack systems, professionals hack people.”
Bruce Schneier

Social Engineering relies on the following:

- The appearance of “authority”
- People want to avoid
- Inconvenience

- Timing, timing, timing…

Pre-text Phone Calls (Phishing by phone)

- "Hi, this is Randy from Comcast Business users support. I am working with Dave, and I need your help…"
  - Name dropping → Establish a rapport
  - Ask for help
  - Inject some techno-babble

- "I need you to visit the Microsoft Update site to download and install a security patch. Do you have 3 minutes to help me out?"

- Schemes result in losses from fraudulent ACH transactions,…

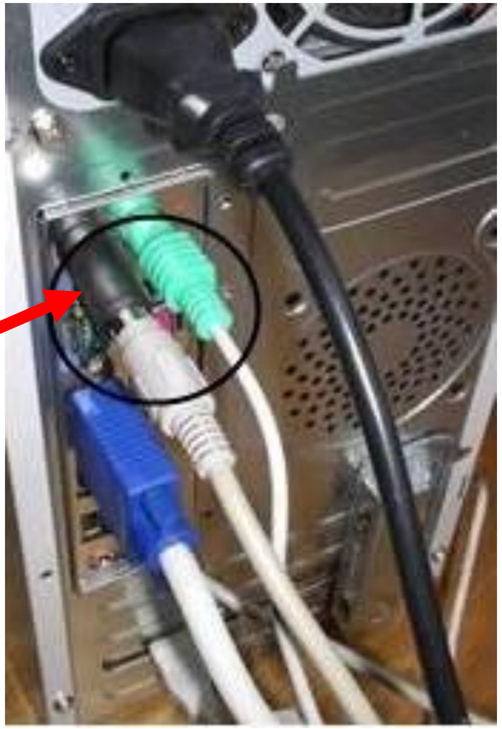
Physical (Facility) Security

Compromise the site:

- “Hi, Sally said she would let you know I was coming to fix the printers…”

Plant devices:

- Keystroke loggers
- Wireless access point
- CDs or Thumb drives



Email Phishing is a Root Cause Underlying Most Breaches

Two Minutes of Inconvenience

Email Phishing Objectives

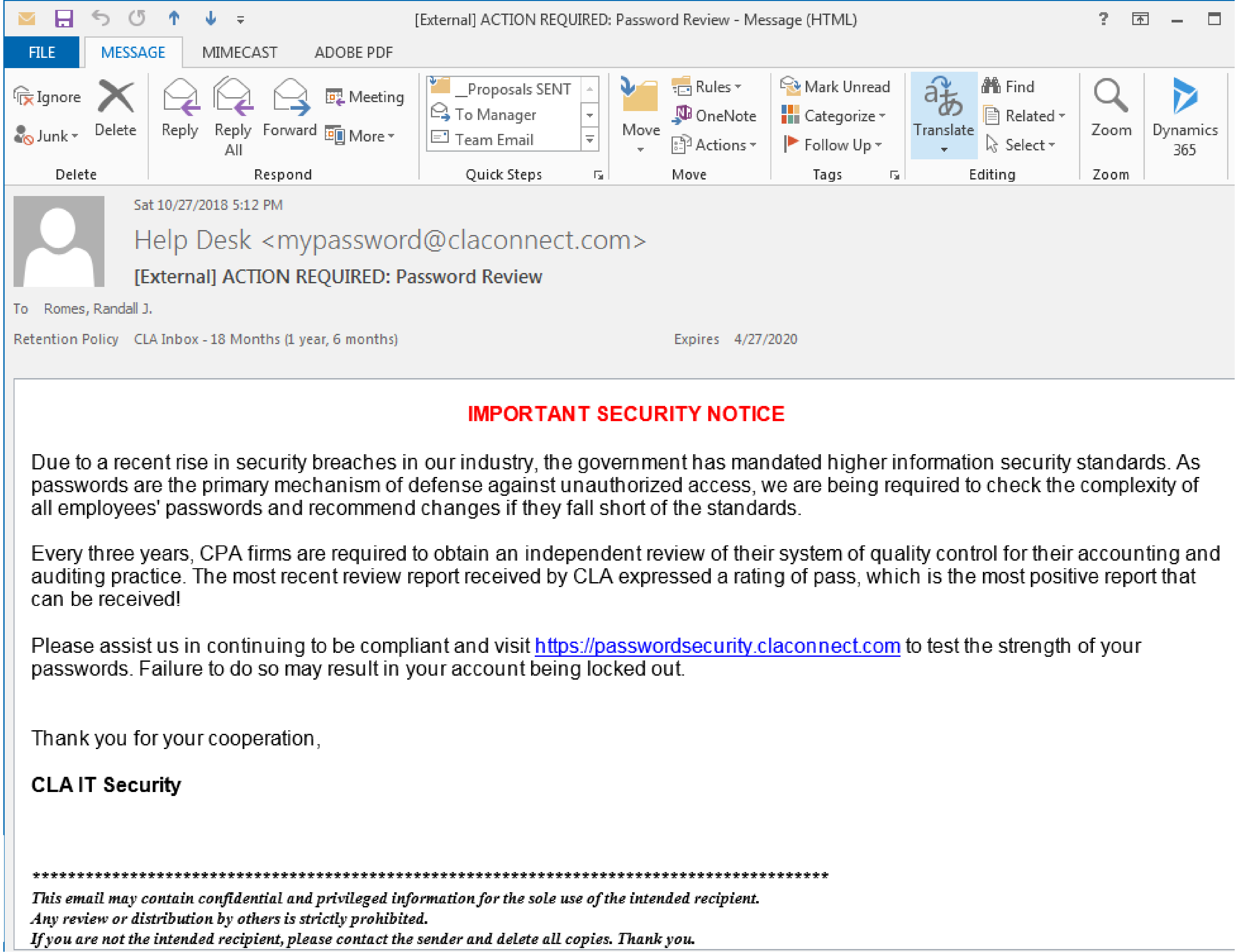
Goals:

- Convince target to do something
- Gain access to:
  - Business email accounts ("BEC" or Business Email Compromise")
  - Financial accounts (payroll, AR/AP, e-Treasury management, etc…)
  - Network resources and confidential/sensitive information
  - Personal email accounts, cloud accounts, social media accounts

Malware infection via:

- Links to malicious website containing drive-by malware
- Email Attachments
  - ZIP, RAR, HTA, JAR, etc.…
  - **Office documents with MACROS and/or PowerShell script**

Phishing?



Sat 10/27/2018 5:12 PM

Help Desk <mypassword@claconnect.com>

[External] ACTION REQUIRED: Password Review

To Romes, Randall J.

Retention Policy CLA Inbox - 18 Months (1 year, 6 months) Expires 4/27/2020

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, the government has mandated higher information security standards. As passwords are the primary mechanism of defense against unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standards.

Every three years, CPA firms are required to obtain an independent review of their system of quality control for their accounting and auditing practice. The most recent review report received by CLA expressed a rating of pass, which is the most positive report that can be received!

Please assist us in continuing to be compliant and visit https://passwordsecurity.claconnect.com to test the strength of your passwords. Failure to do so may result in your account being locked out.

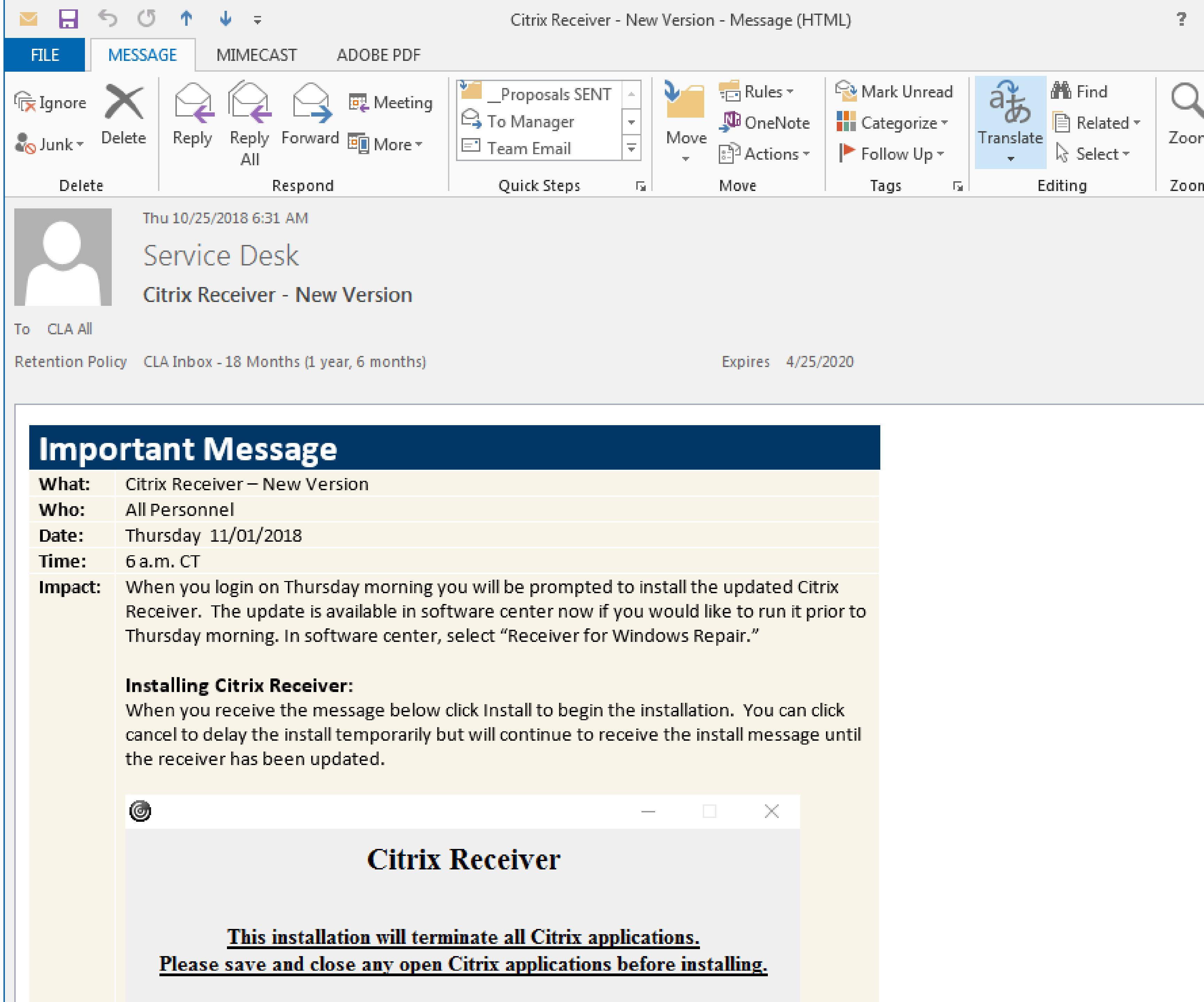
Thank you for your cooperation,

CLA IT Security

****

This email may contain confidential and privileged information for the sole use of the intended recipient.
Any review or distribution by others is strictly prohibited.
If you are not the intended recipient, please contact the sender and delete all copies. Thank you.

Phishing?



Thu 10/25/2018 6:31 AM

Service Desk

Citrix Receiver - New Version

To CLA All

Retention Policy CLA Inbox - 18 Months (1 year, 6 months) Expires 4/25/2020

Important Message

What:	Citrix Receiver – New Version
Who:	All Personnel
Date:	Thursday 11/01/2018
Time:	6 a.m. CT
Impact:	When you login on Thursday morning you will be prompted to install the updated Citrix Receiver. The update is available in software center now if you would like to run it prior to Thursday morning. In software center, select “Receiver for Windows Repair.”

Installing Citrix Receiver:
When you receive the message below click Install to begin the installation. You can click cancel to delay the install temporarily but will continue to receive the install message until the receiver has been updated.

Citrix Receiver

This installation will terminate all Citrix applications.
Please save and close any open Citrix applications before installing.

Payment Fraud

"Why do you rob the banks???"

Impersonation and Persuasion

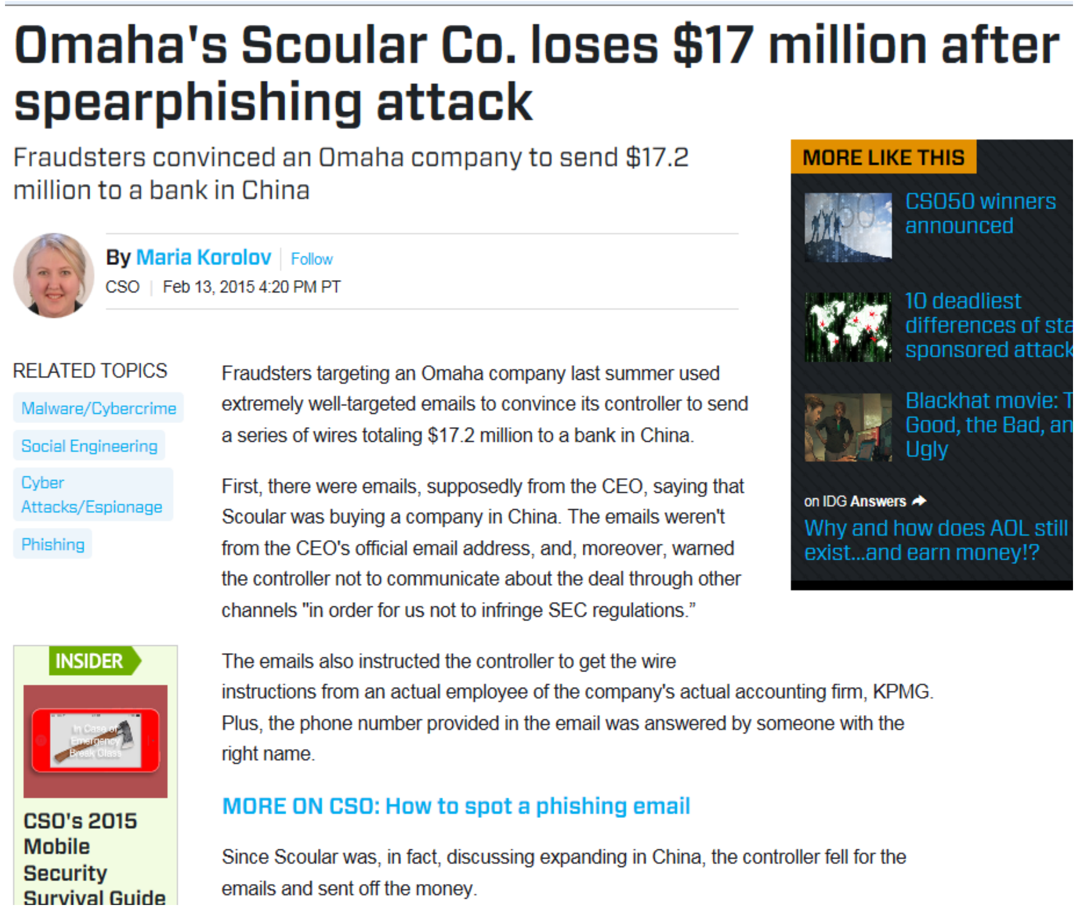
Payment Fraud – Account Take Overs

- When is the last time you wrote a check???
- Electronic payments are the norm…
  - Wire transfers & ACH payments
  - Online banking
  - ”Send money”
    - ➢(Corporate) Account Take Over (CATO)
      - Compromise accounts/credentials that can move money
    - ➢Persuasion Attacks
      - Convince others to send money

Persuasion Attacks
(Two Years Ago…)

- CEO asks the controller…

- Common mistakes
  - Use of private email
  - "Don't tell anyone"



Omaha's Scoular Co. loses $17 million after spearphishing attack

Fraudsters convinced an Omaha company to send $17.2 million to a bank in China

By Maria Korolov | Follow
CSO | Feb 13, 2015 4:20 PM PT

RELATED TOPICS
Malware/Cybercrime
Social Engineering
Cyber Attacks/Espionage
Phishing

Fraudsters targeting an Omaha company last summer used extremely well-targeted emails to convince its controller to send a series of wires totaling $17.2 million to a bank in China.

First, there were emails, supposedly from the CEO, saying that Scoular was buying a company in China. The emails weren't from the CEO's official email address, and, moreover, warned the controller not to communicate about the deal through other channels "in order for us not to infringe SEC regulations."

The emails also instructed the controller to get the wire instructions from an actual employee of the company's actual accounting firm, KPMG. Plus, the phone number provided in the email was answered by someone with the right name.

MORE ON CSO: How to spot a phishing email

Since Scoular was, in fact, discussing expanding in China, the controller fell for the emails and sent off the money.

MORE LIKE THIS
CSO50 winners announced
10 deadliest differences of sta sponsored attack
Blackhat movie: T Good, the Bad, an Ugly
on IDG Answers
Why and how does AOL still exist...and earn money!?

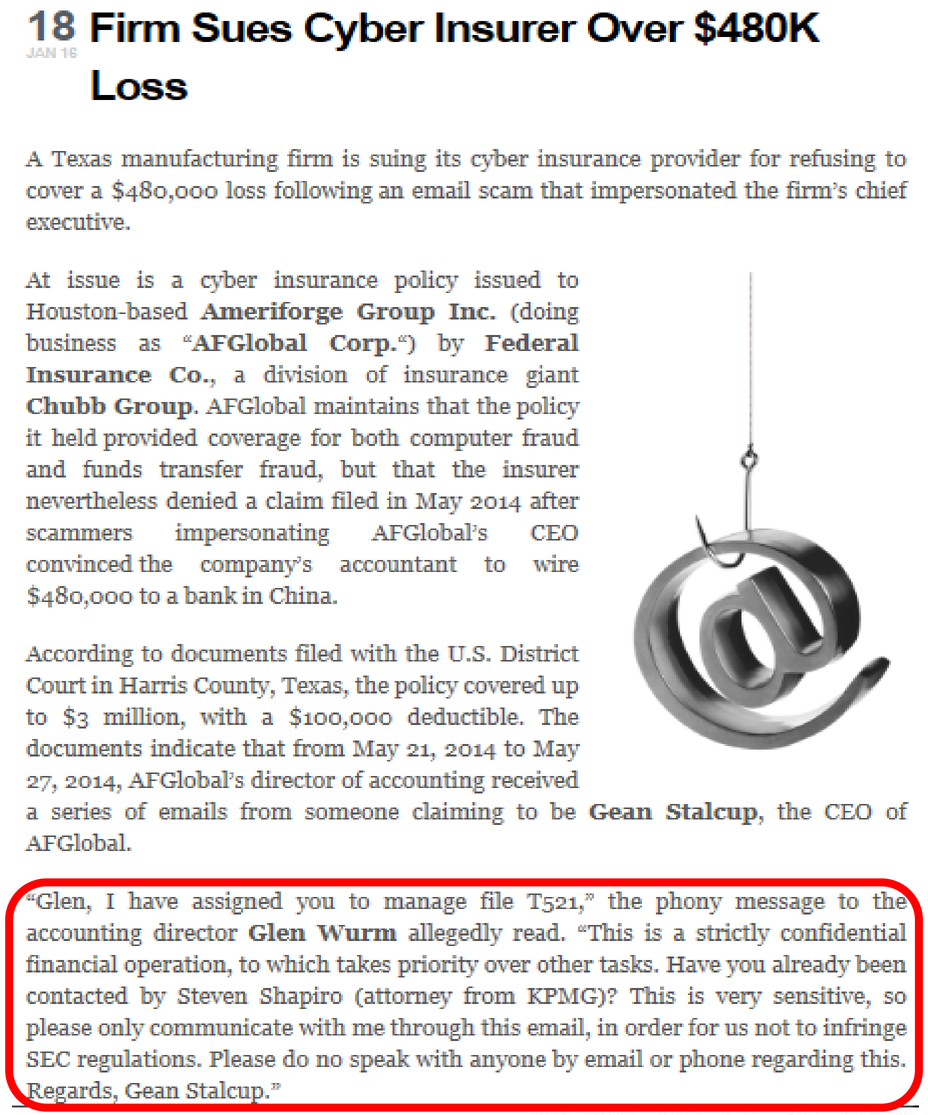
INSIDER
CSO's 2015 Mobile Security Survival Guide

Persuasion Attacks (more recently)

KrebsonSecurity
In-depth security news and investigation

https://krebsonsecurity.com/tag/bec/

- CEO asks the accountant…
- Common mistakes
  - Use of private email
  - "Don't tell anyone"



18 JAN 16 **Firm Sues Cyber Insurer Over $480K Loss**

A Texas manufacturing firm is suing its cyber insurance provider for refusing to cover a $480,000 loss following an email scam that impersonated the firm's chief executive.

At issue is a cyber insurance policy issued to Houston-based **Ameriforge Group Inc.** (doing business as "**AFGlobal Corp.**") by **Federal Insurance Co.**, a division of insurance giant **Chubb Group**. AFGlobal maintains that the policy it held provided coverage for both computer fraud and funds transfer fraud, but that the insurer nevertheless denied a claim filed in May 2014 after scammers impersonating AFGlobal's CEO convinced the company's accountant to wire $480,000 to a bank in China.

According to documents filed with the U.S. District Court in Harris County, Texas, the policy covered up to $3 million, with a $100,000 deductible. The documents indicate that from May 21, 2014 to May 27, 2014, AFGlobal's director of accounting received a series of emails from someone claiming to be **Gean Stalcup**, the CEO of AFGlobal.

"Glen, I have assigned you to manage file T521," the phony message to the accounting director **Glen Wurm** allegedly read. "This is a strictly confidential financial operation, to which takes priority over other tasks. Have you already been contacted by Steven Shapiro (attorney from KPMG)? This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations. Please do no speak with anyone by email or phone regarding this. Regards, Gean Stalcup."

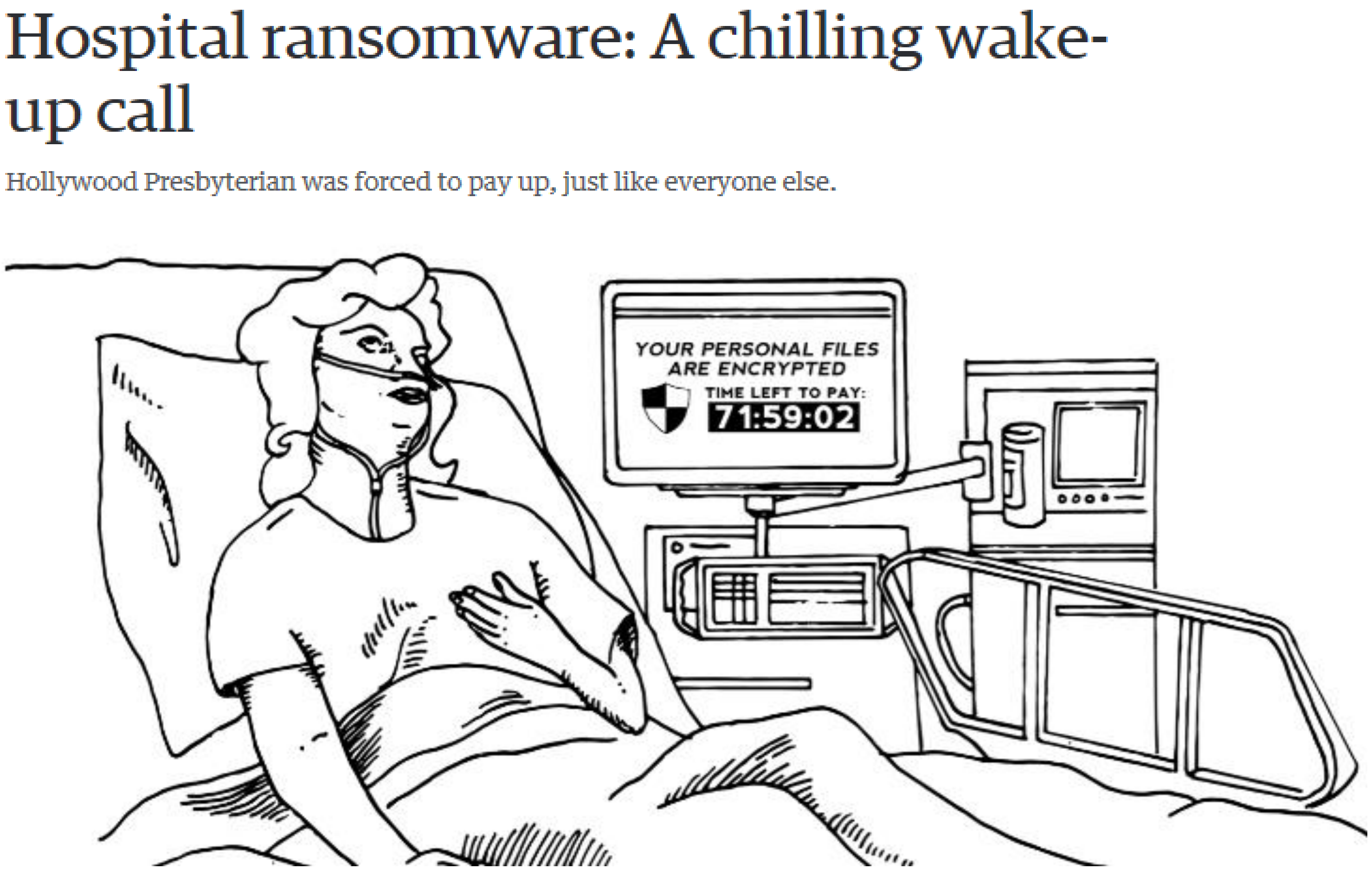
CUNA Credit Union National Association

NASCUS
The National Voice of the State Credit Union System

Ransomware

Would you like your pictures back?

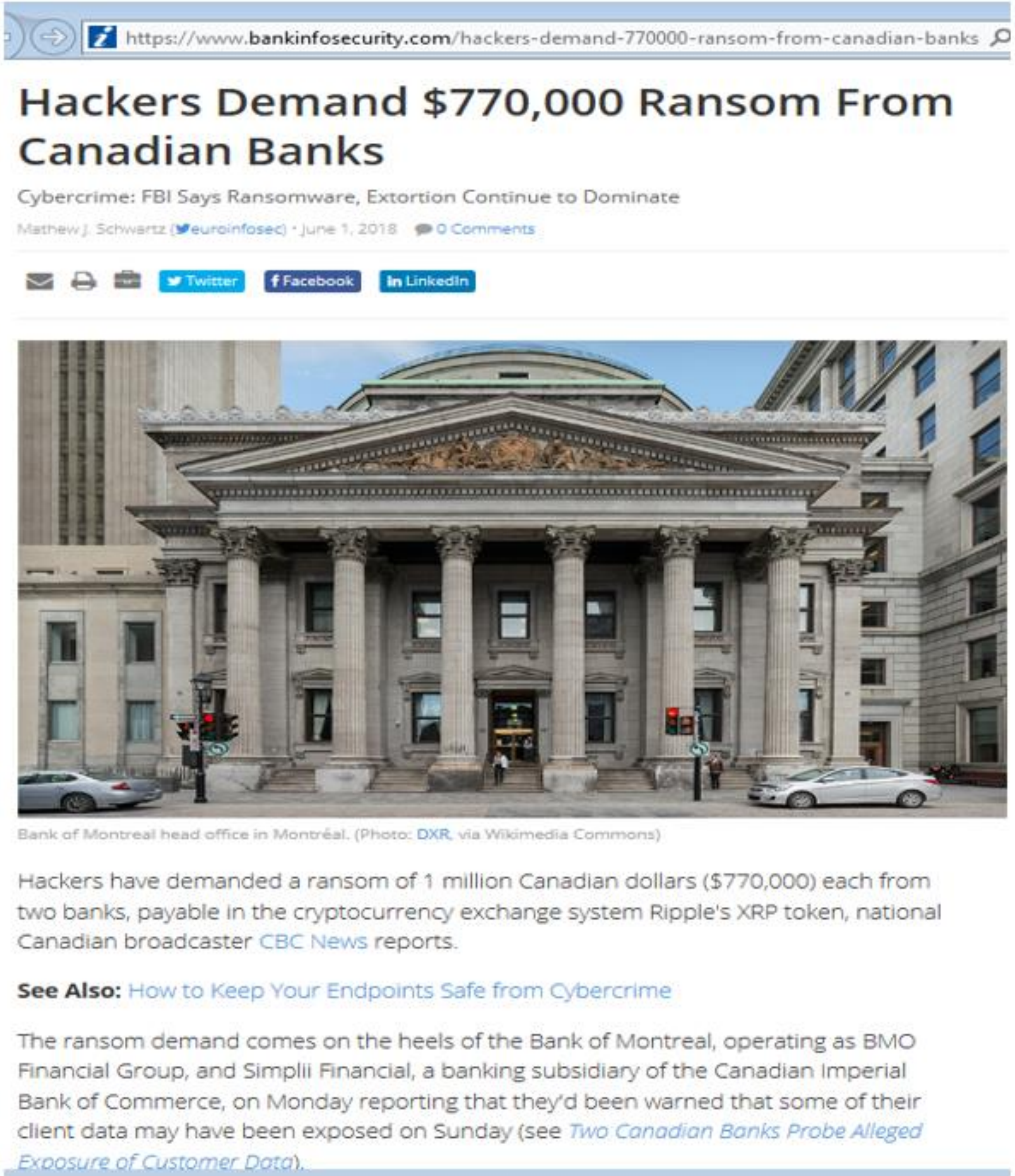
Ransomware (two years ago…)



Hospital ransomware: A chilling wake-up call

Hollywood Presbyterian was forced to pay up, just like everyone else.

Ransomware
(more recently)



https://www.bankinfosecurity.com/hackers-demand-770000-ransom-from-canadian-banks

Hackers Demand $770,000 Ransom From Canadian Banks

Cybercrime: FBI Says Ransomware, Extortion Continue to Dominate

Mathew J. Schwartz (euroinfosec) • June 1, 2018 0 Comments

Bank of Montreal head office in Montréal. (Photo: DXR, via Wikimedia Commons)

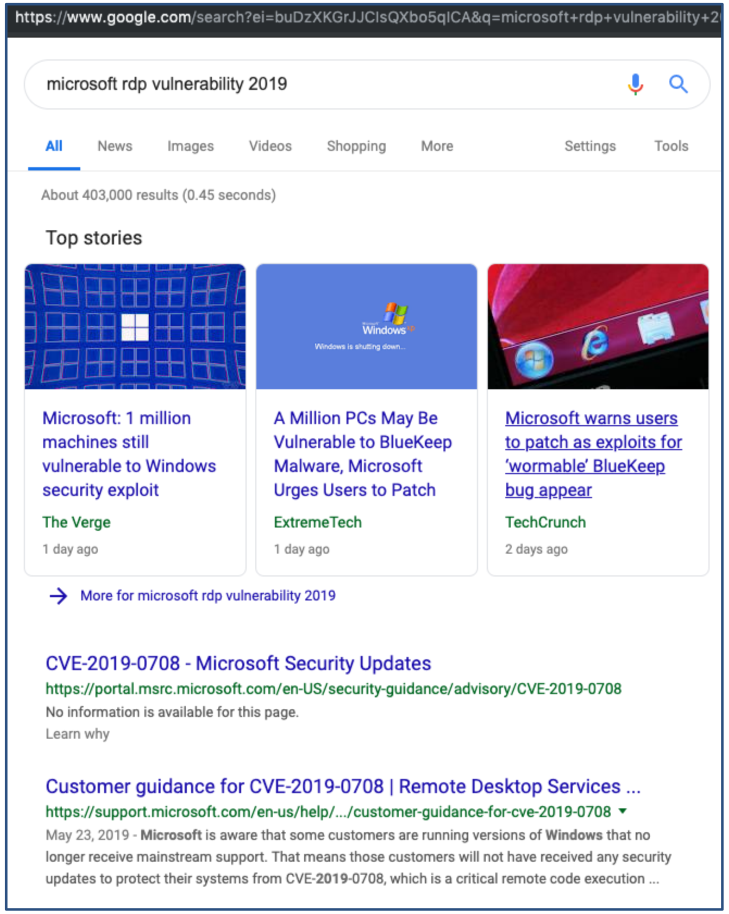
Hackers have demanded a ransom of 1 million Canadian dollars ($770,000) each from two banks, payable in the cryptocurrency exchange system Ripple's XRP token, national Canadian broadcaster CBC News reports.

See Also: How to Keep Your Endpoints Safe from Cybercrime

The ransom demand comes on the heels of the Bank of Montreal, operating as BMO Financial Group, and Simplii Financial, a banking subsidiary of the Canadian Imperial Bank of Commerce, on Monday reporting that they'd been warned that some of their client data may have been exposed on Sunday (see *Two Canadian Banks Probe Alleged Exposure of Customer Data*).

Ransomware

(Last week…)
(Next week?)



https://www.google.com/search?ei=buDzXKGrJJCIsQXbo5qICA&q=microsoft+rdp+vulnerability+2

microsoft rdp vulnerability 2019

About 403,000 results (0.45 seconds)

Top stories

Microsoft: 1 million machines still vulnerable to Windows security exploit
The Verge
1 day ago

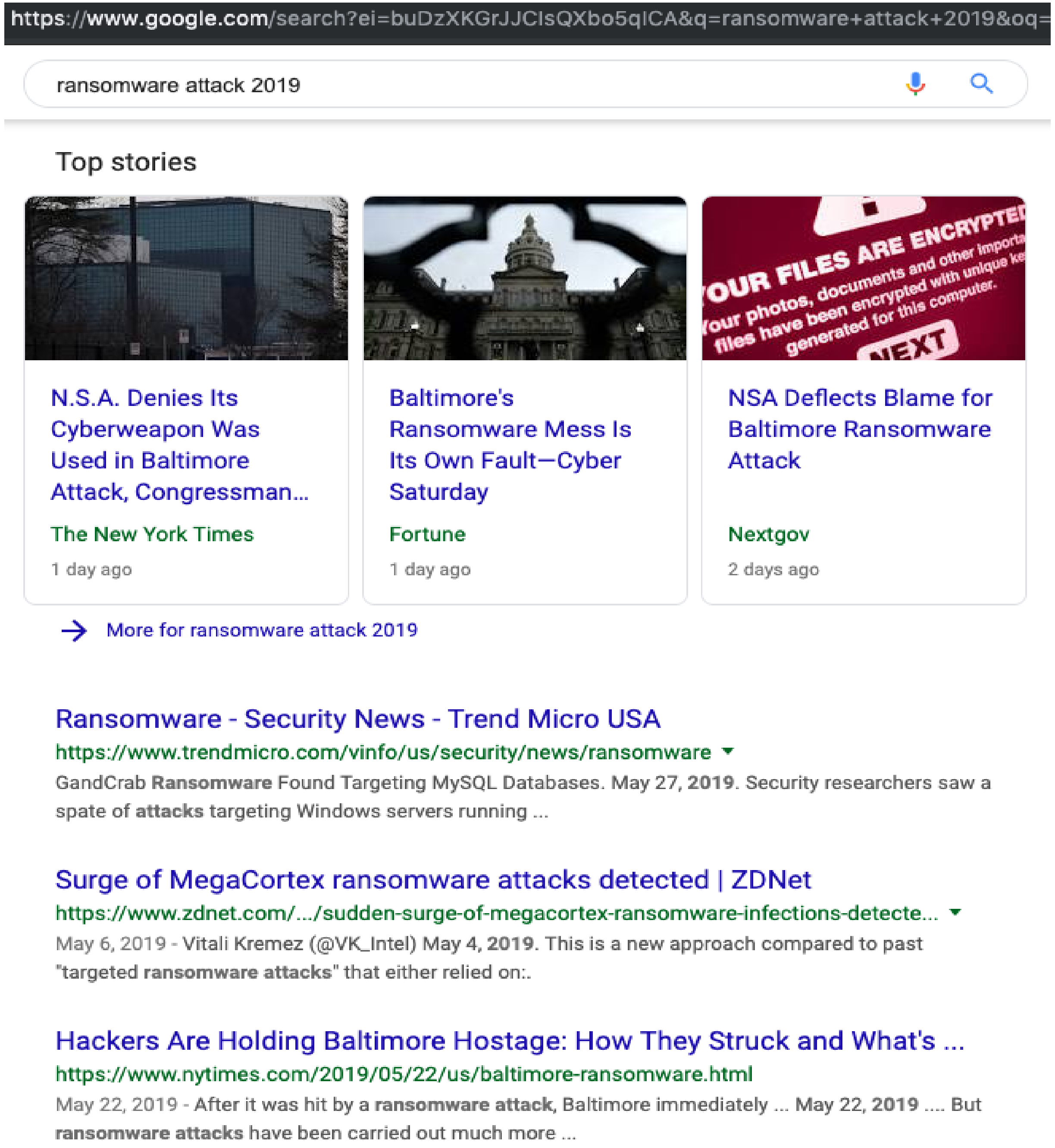
A Million PCs May Be Vulnerable to BlueKeep Malware, Microsoft Urges Users to Patch
ExtremeTech
1 day ago

Microsoft warns users to patch as exploits for ‘wormable’ BlueKeep bug appear
TechCrunch
2 days ago

→ More for microsoft rdp vulnerability 2019

CVE-2019-0708 - Microsoft Security Updates
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
No information is available for this page.
Learn why

Customer guidance for CVE-2019-0708 | Remote Desktop Services ...
https://support.microsoft.com/en-us/help/.../customer-guidance-for-cve-2019-0708 ▾
May 23, 2019 - **Microsoft** is aware that some customers are running versions of **Windows** that no longer receive mainstream support. That means those customers will not have received any security updates to protect their systems from CVE-**2019**-0708, which is a critical remote code execution ...



https://www.google.com/search?ei=buDzXKGrJJCIsQXbo5qICA&q=ransomware+attack+2019&oq=

ransomware attack 2019

Top stories

N.S.A. Denies Its Cyberweapon Was Used in Baltimore Attack, Congressman...
The New York Times
1 day ago

Baltimore's Ransomware Mess Is Its Own Fault—Cyber Saturday
Fortune
1 day ago

NSA Deflects Blame for Baltimore Ransomware Attack
Nextgov
2 days ago

→ More for ransomware attack 2019

Ransomware - Security News - Trend Micro USA
https://www.trendmicro.com/vinfo/us/security/news/ransomware ▾
GandCrab **Ransomware** Found Targeting MySQL Databases. May 27, **2019**. Security researchers saw a spate of **attacks** targeting Windows servers running ...

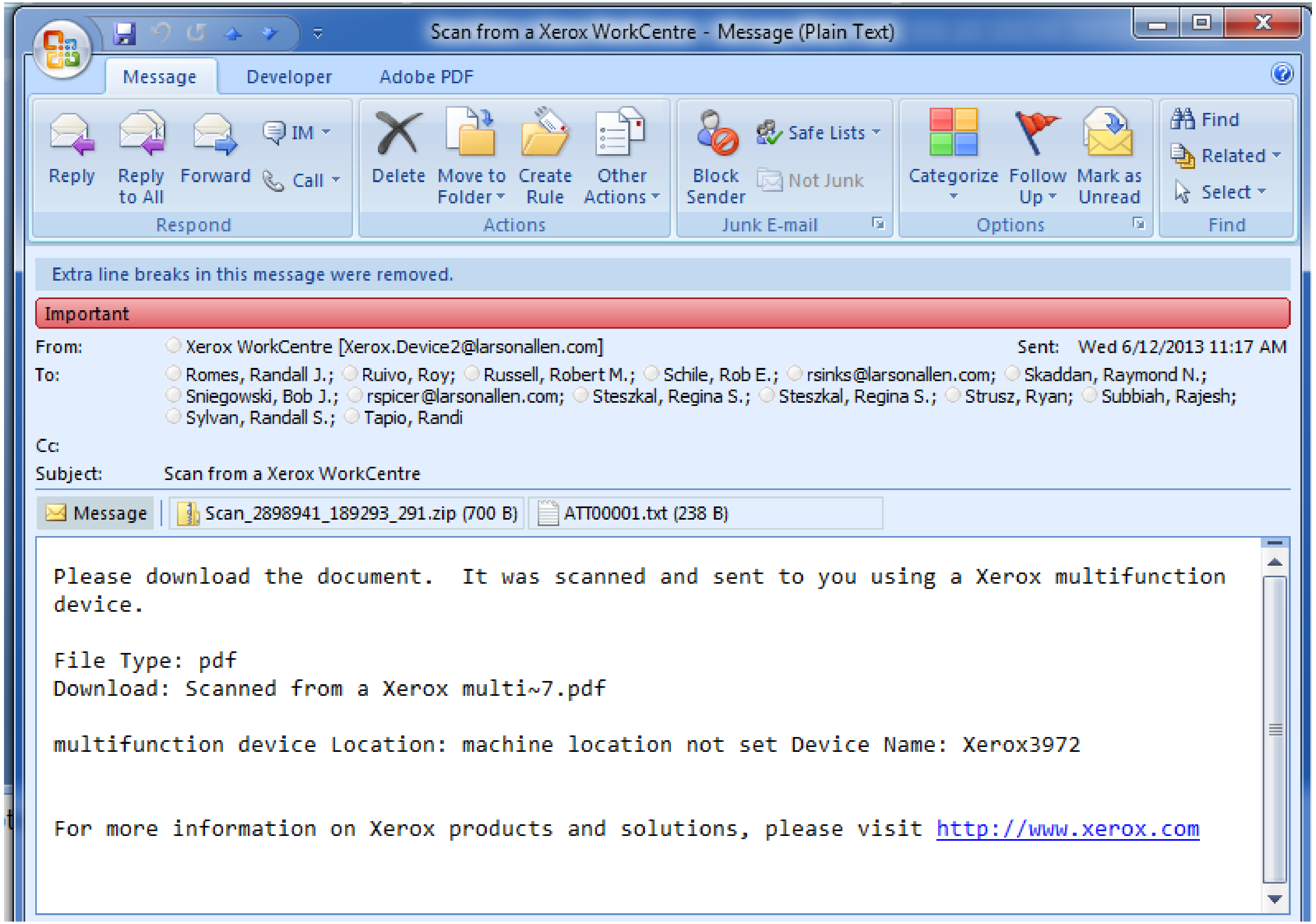
Surge of MegaCortex ransomware attacks detected | ZDNet
https://www.zdnet.com/.../sudden-surge-of-megacortex-ransomware-infections-detecte... ▾
May 6, 2019 - Vitali Kremez (@VK_Intel) May 4, **2019**. This is a new approach compared to past "targeted **ransomware attacks**" that either relied on:.

Hackers Are Holding Baltimore Hostage: How They Struck and What's ...
https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html
May 22, 2019 - After it was hit by a **ransomware attack**, Baltimore immediately ... May 22, **2019** .... But **ransomware attacks** have been carried out much more ...

Credit Union National Association CUNA

NASCUS
The National Voice of the State Credit Union System

Ransomware



Scan from a Xerox WorkCentre - Message (Plain Text)

Extra line breaks in this message were removed.

Important

From: Xerox WorkCentre [Xerox.Device2@larsonallen.com]

Sent: Wed 6/12/2013 11:17 AM

To: Romes, Randall J.; Ruivo, Roy; Russell, Robert M.; Schile, Rob E.; rsinks@larsonallen.com; Skaddan, Raymond N.; Sniegowski, Bob J.; rspicer@larsonallen.com; Steszkal, Regina S.; Steszkal, Regina S.; Strusz, Ryan; Subbiah, Rajesh; Sylvan, Randall S.; Tapio, Randi

Cc:

Subject: Scan from a Xerox WorkCentre

Message | Scan_2898941_189293_291.zip (700 B) | ATT00001.txt (238 B)

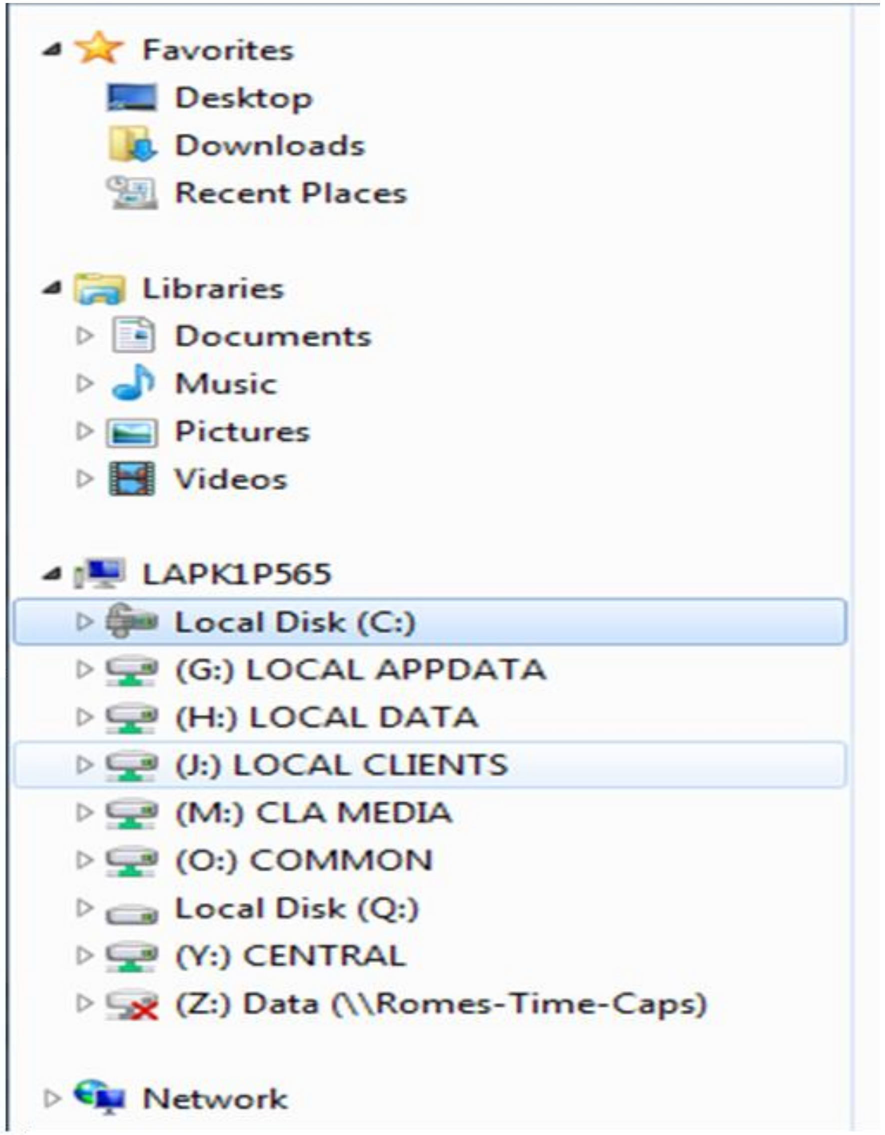
```
Please download the document.  It was scanned and sent to you using a Xerox multifunction
device.

File Type: pdf
Download: Scanned from a Xerox multi~7.pdf

multifunction device Location: machine location not set Device Name: Xerox3972


For more information on Xerox products and solutions, please visit http://www.xerox.com
```

Credit Union National Association

NASCUS The National Voice of the State Credit Union System

Ransomware

- Malware encrypts everything it can interact with


Favorites
Desktop
Downloads
Recent Places

Libraries
Documents
Music
Pictures
Videos

LAPK1P565
Local Disk (C:)
(G:) LOCAL APPDATA
(H:) LOCAL DATA
(J:) LOCAL CLIENTS
(M:) CLA MEDIA
(O:) COMMON
Local Disk (Q:)
(Y:) CENTRAL
(Z:) Data (\\Romes-Time-Caps)

Network

Ransomware Defensive Strategies

1. Filtering capabilities

2. Users that are aware and savvy

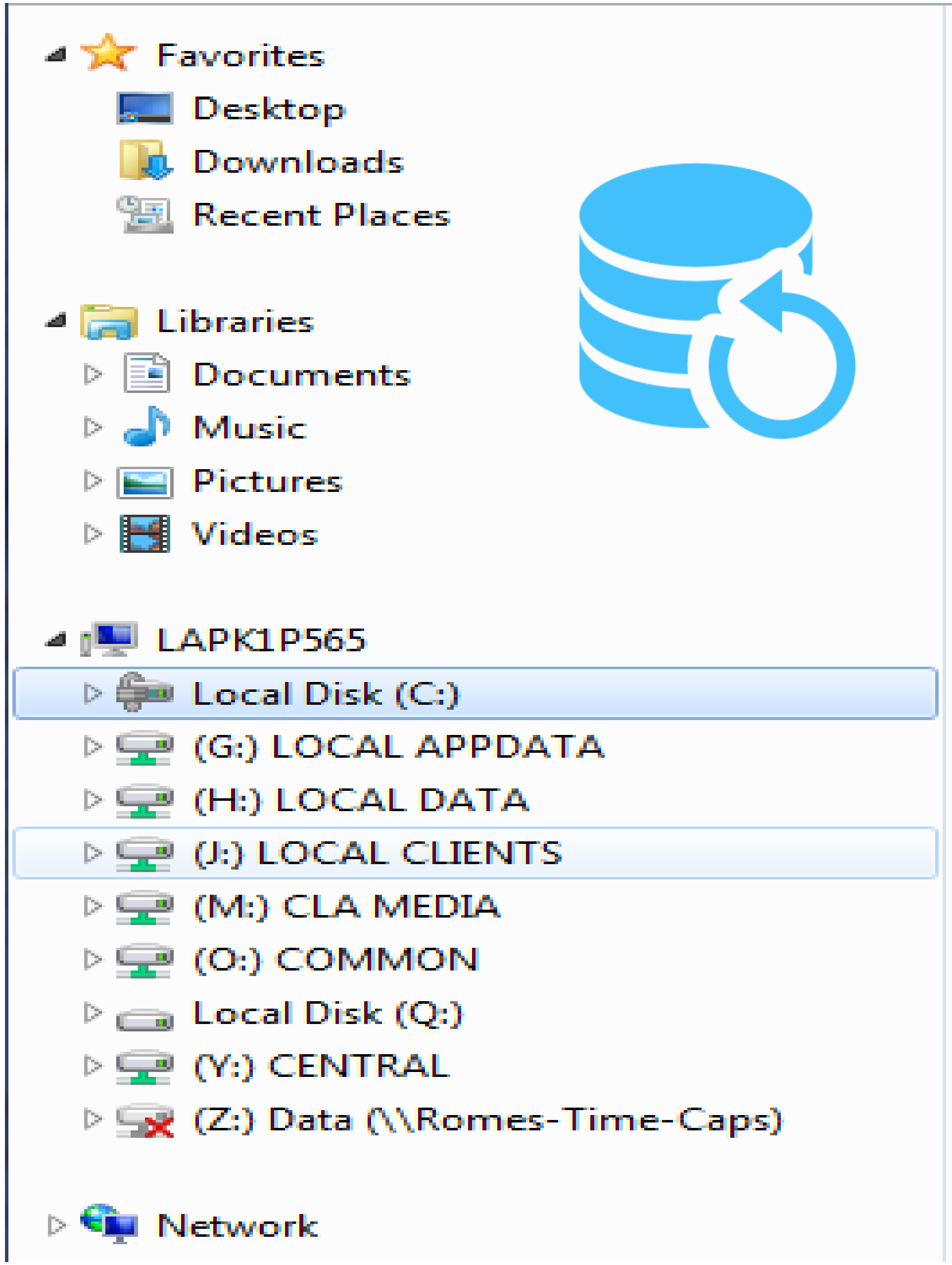
3. Minimized User Access Rights

4. Current operation systems and up to date/patched software

Ransomware Defensive Strategies

5. Working backup and restore capabilities

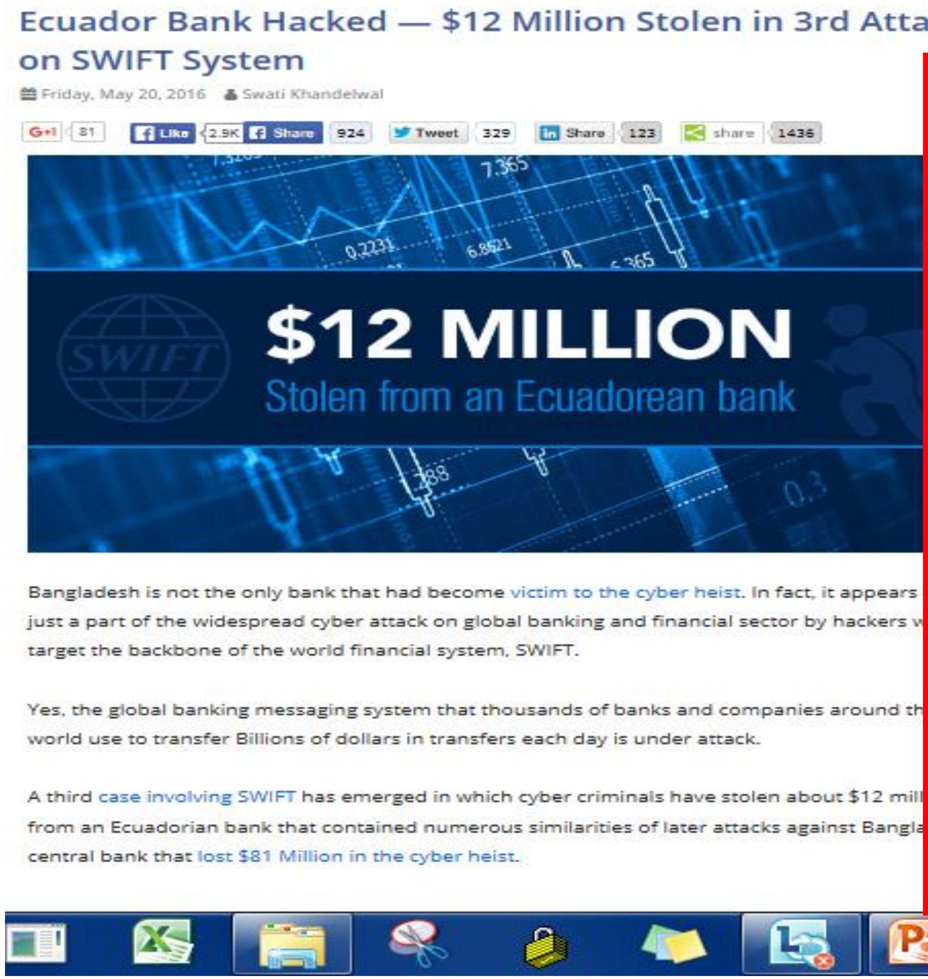
6. Secure the backup process
   - Backups should be done with a service account.
   - Storage location of back ups should be very restrictive – read only access even for most administrators.
   - Identify which users could encrypt backups if they were to become infected.
   - You could also restrict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



Back End Payment Systems

- Hack them one at a time?
- Or all at once???

Backend Payment Systems - SWIFT



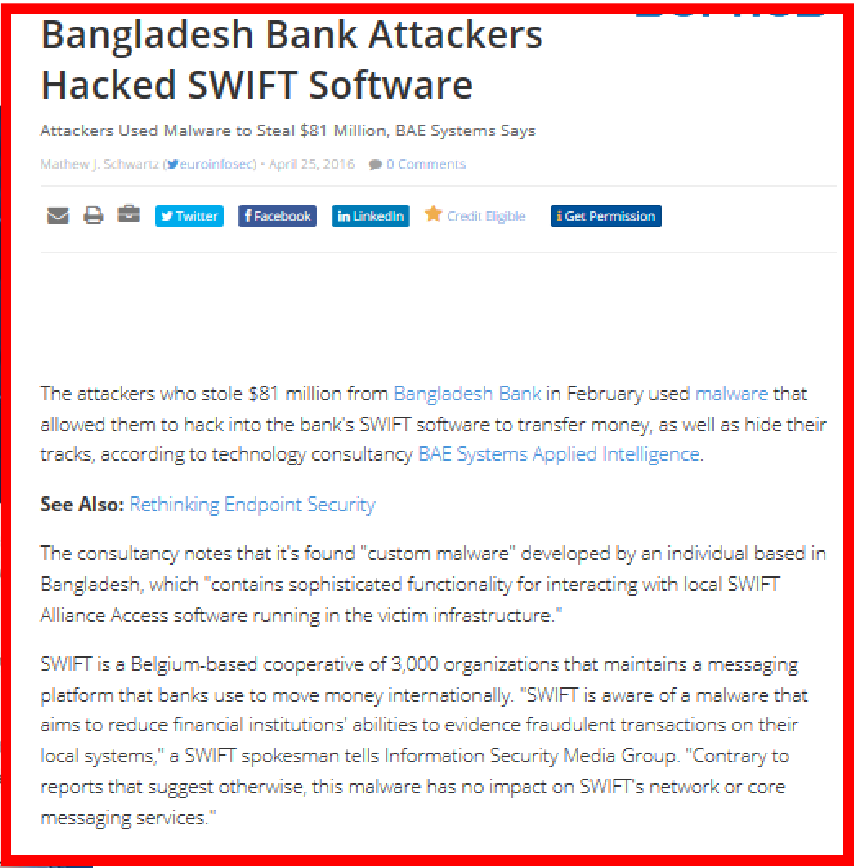
Ecuador Bank Hacked — $12 Million Stolen in 3rd Attack on SWIFT System

Friday, May 20, 2016 Swati Khandelwal

Bangladesh is not the only bank that had become victim to the cyber heist. In fact, it appears just a part of the widespread cyber attack on global banking and financial sector by hackers w target the backbone of the world financial system, SWIFT.

Yes, the global banking messaging system that thousands of banks and companies around th world use to transfer Billions of dollars in transfers each day is under attack.

A third case involving SWIFT has emerged in which cyber criminals have stolen about $12 mill from an Ecuadorian bank that contained numerous similarities of later attacks against Bangla central bank that lost $81 Million in the cyber heist.



Bangladesh Bank Attackers Hacked SWIFT Software

Attackers Used Malware to Steal $81 Million, BAE Systems Says

Mathew J. Schwartz (euroinfosec) • April 25, 2016 0 Comments

The attackers who stole $81 million from Bangladesh Bank in February used malware that allowed them to hack into the bank's SWIFT software to transfer money, as well as hide their tracks, according to technology consultancy BAE Systems Applied Intelligence.

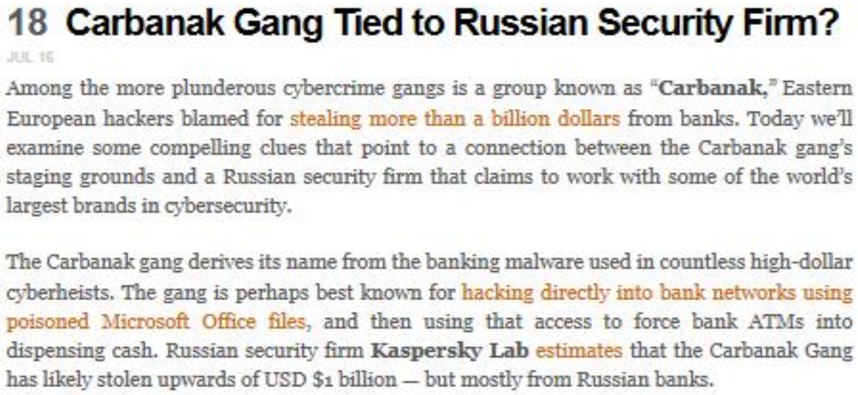
See Also: Rethinking Endpoint Security

The consultancy notes that it's found "custom malware" developed by an individual based in Bangladesh, which "contains sophisticated functionality for interacting with local SWIFT Alliance Access software running in the victim infrastructure."

SWIFT is a Belgium-based cooperative of 3,000 organizations that maintains a messaging platform that banks use to move money internationally. "SWIFT is aware of a malware that aims to reduce financial institutions' abilities to evidence fraudulent transactions on their local systems," a SWIFT spokesman tells Information Security Media Group. "Contrary to reports that suggest otherwise, this malware has no impact on SWIFT's network or core messaging services."

Backend Payment Systems
Carbanak - Biggest Bank Heist EVER

- $1B over 2 years
- Average $10M per bank.
- 2 to 4 months per bank
- Methods: Online Banking, Swift, ATMs
- Attackers primarily in Russia, Ukraine, China
- Banks primarily Russia, Europe, United States



18 Carbanak Gang Tied to Russian Security Firm?

JUL 16

Among the more plunderous cybercrime gangs is a group known as "**Carbanak,**" Eastern European hackers blamed for stealing more than a billion dollars from banks. Today we'll examine some compelling clues that point to a connection between the Carbanak gang's staging grounds and a Russian security firm that claims to work with some of the world's largest brands in cybersecurity.

The Carbanak gang derives its name from the banking malware used in countless high-dollar cyberheists. The gang is perhaps best known for hacking directly into bank networks using poisoned Microsoft Office files, and then using that access to force bank ATMs into dispensing cash. Russian security firm **Kaspersky Lab** estimates that the Carbanak Gang has likely stolen upwards of USD $1 billion — but mostly from Russian banks.

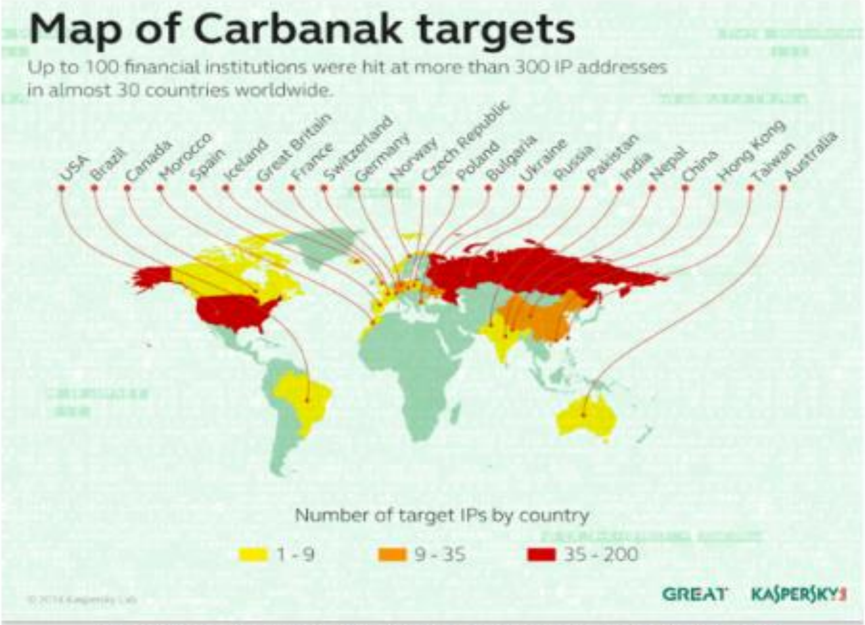
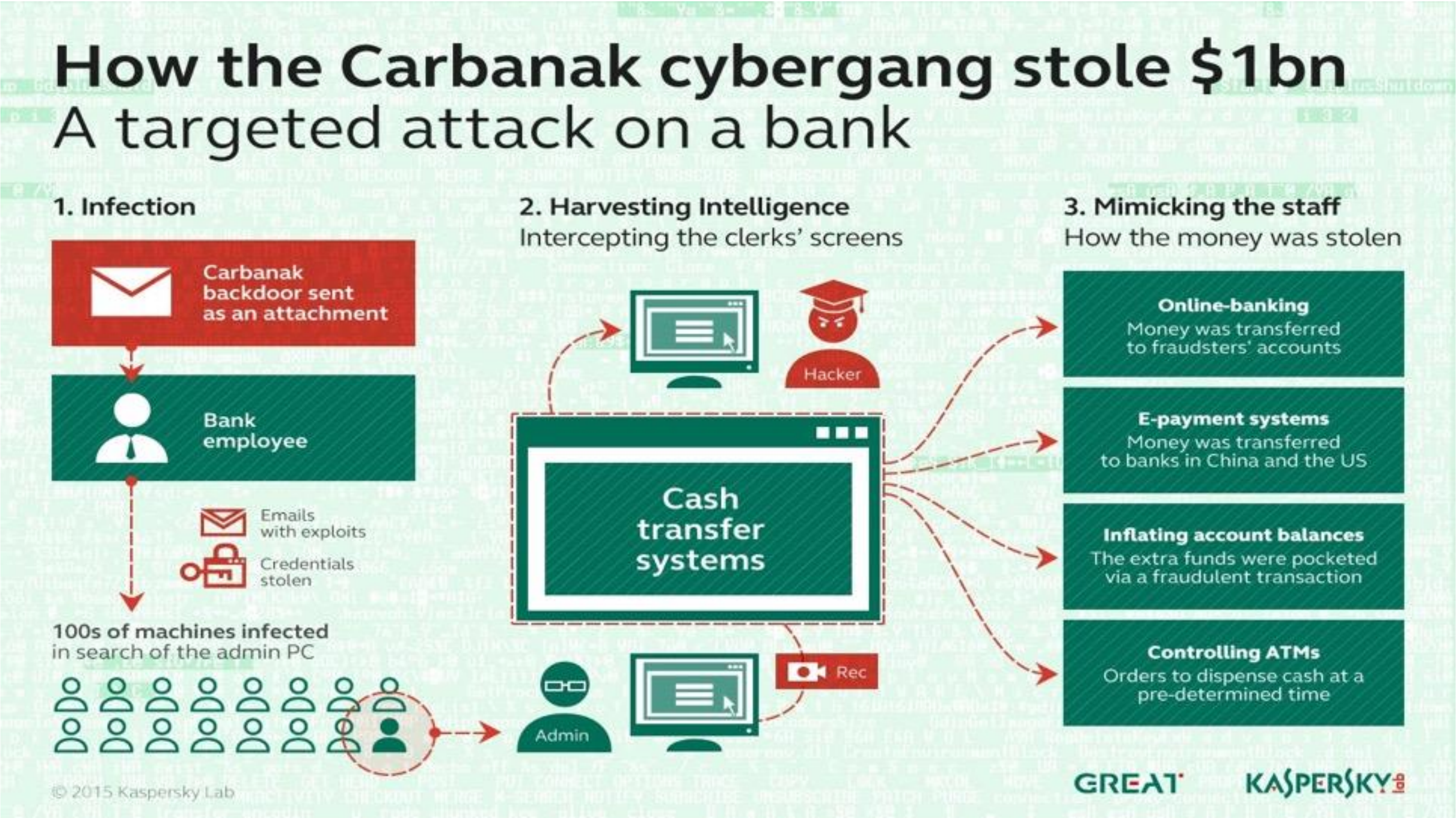


Figure 9. Geographical distribution of targets according to C2 data

Backend Payment Systems
Carbanak - Biggest Bank Heist EVER



How the Carbanak cybergang stole $1bn
A targeted attack on a bank

1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected in search of the admin PC

2. Harvesting Intelligence
Intercepting the clerks' screens

Hacker

Cash transfer systems

Admin

Rec

3. Mimicking the staff
How the money was stolen

Online-banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the US

Inflating account balances
The extra funds were pocketed via a fraudulent transaction

Controlling ATMs
Orders to dispense cash at a pre-determined time

© 2015 Kaspersky Lab

GREAT KASPERSKY lab

A Unique CATO Example

EXAMPLE 1

- 3 Member accounts
  - Adam and Beth
    - ❖ Accounts compromised "previously"
    - ❖ No changes
  - Joe
    - ❖ Account compromised – PII Changed
    - ❖ New/replacement debit card ordered
  - Account to account transfers initiated (to Joe account)
    - ❖ Funds removed from Joe account

EXAMPLE 2

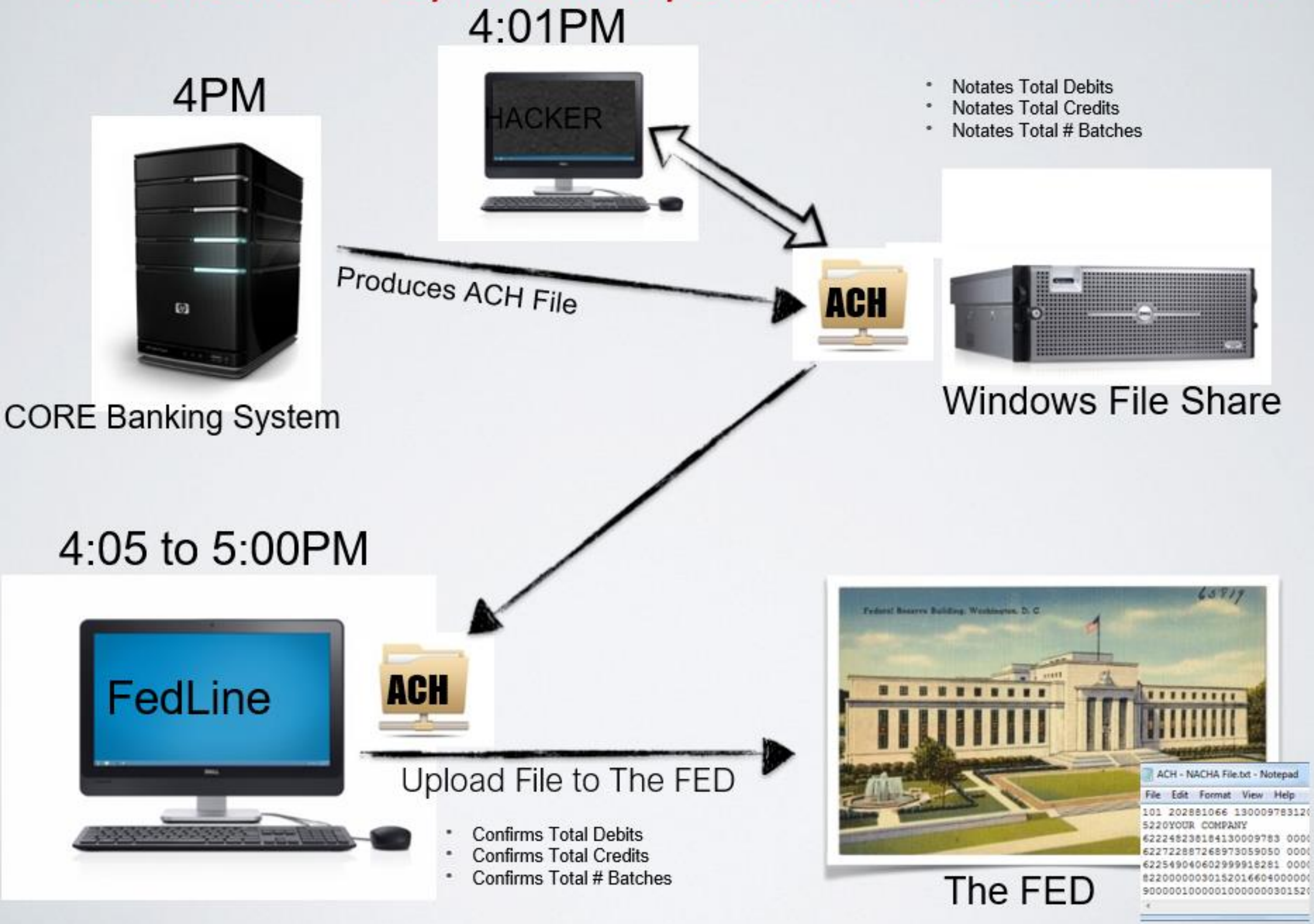
- 3 Member accounts
  - Mike and Sue
    - Accounts compromised "previously"
    - No changes
  - Ann
    - New account set up with minimal funds
    - Member to Member transfers initiated (to Ann account)
      - Funds removed from Ann account

- Unique twist related to Core and Internet Banking Conversion…

Credit Union National Association CUNA

NASCUS The National Voice of the State Credit Union System

Backend Payment Systems - Is ACH Next?



- Notates Total Debits
- Notates Total Credits
- Notates Total # Batches

- Confirms Total Debits
- Confirms Total Credits
- Confirms Total # Batches

```
101 202881066 13000978312
5220YOUR COMPANY
6222482381841300009783 000
6227222887268973059050 000
6225490406029999182 81 000
822000000301520166040000
900000100000100000000301520
```

The Boy Scouts Motto: *"Be Prepared"*

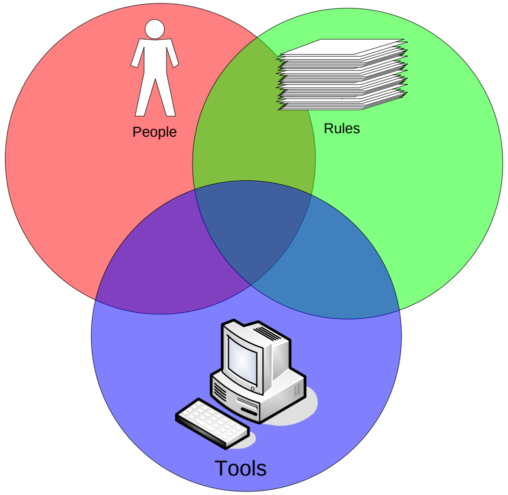
Strategies and Action Items

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

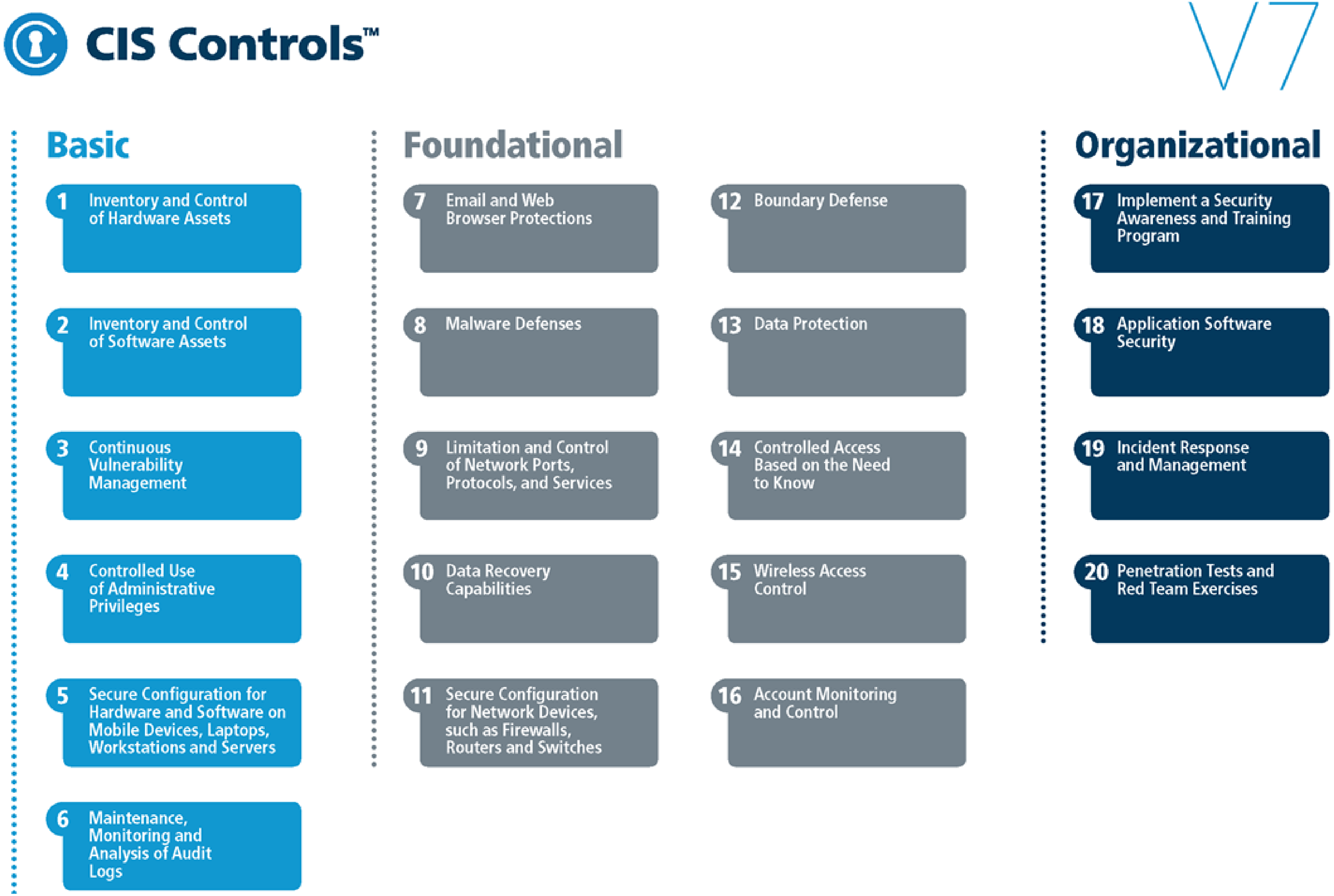
Policies and Standards



- ➢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/

Credit Union National Association
CUNA

NASCUS
The National Voice of the State Credit Union System

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 (independent)
  - Patch Tuesday and vulnerability scanning
  - Rogue devices

© Cre

Passwords

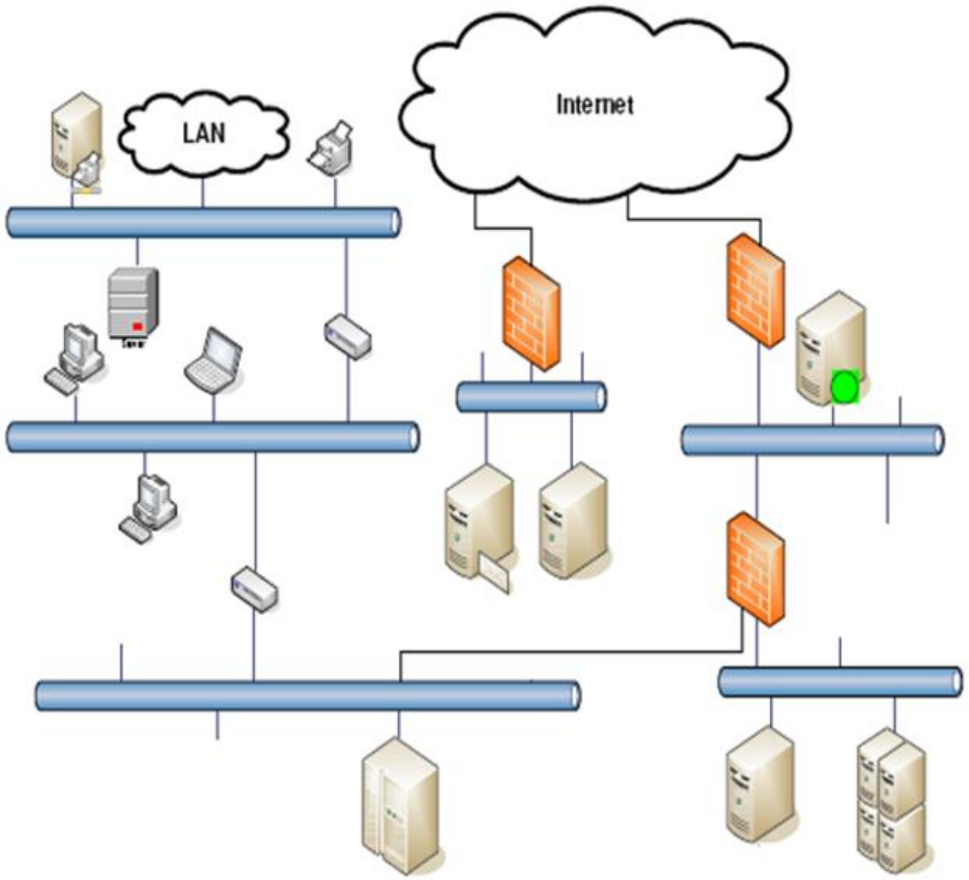
- Good Passwords
- Two Factor / Multi-Factor Authentication
- Password Managers

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



Credit Union National CUNA Association

NASCUS The National Voice of the State Credit Union System

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

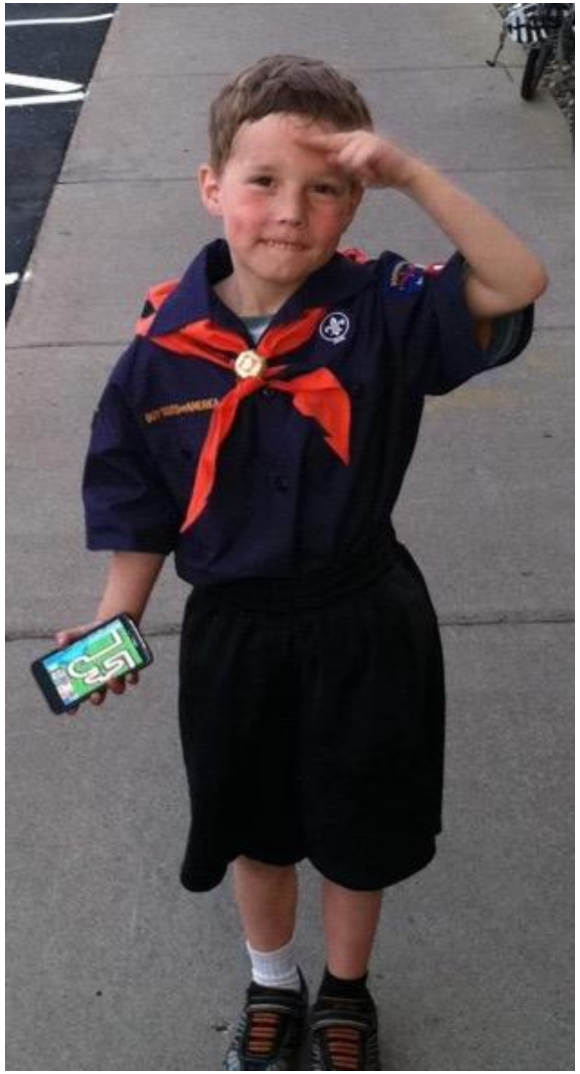
- Test backup and restore processes
  - Periodically test backup systems to ensure you can recover from ransomware
  - Have IT perform a full, bare-metal system restore (operating system, applications, and data)
  - Have IT document how long it takes to recover various files or systems

➢**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?

Credit Union National Association CUNA

NASCUS The National Voice of the State Credit Union System

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

June 2019

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

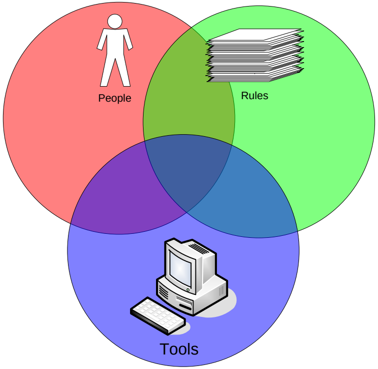
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Understanding the CIS Critical Controls

Create Opportunities

We promise to know you and help you.

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

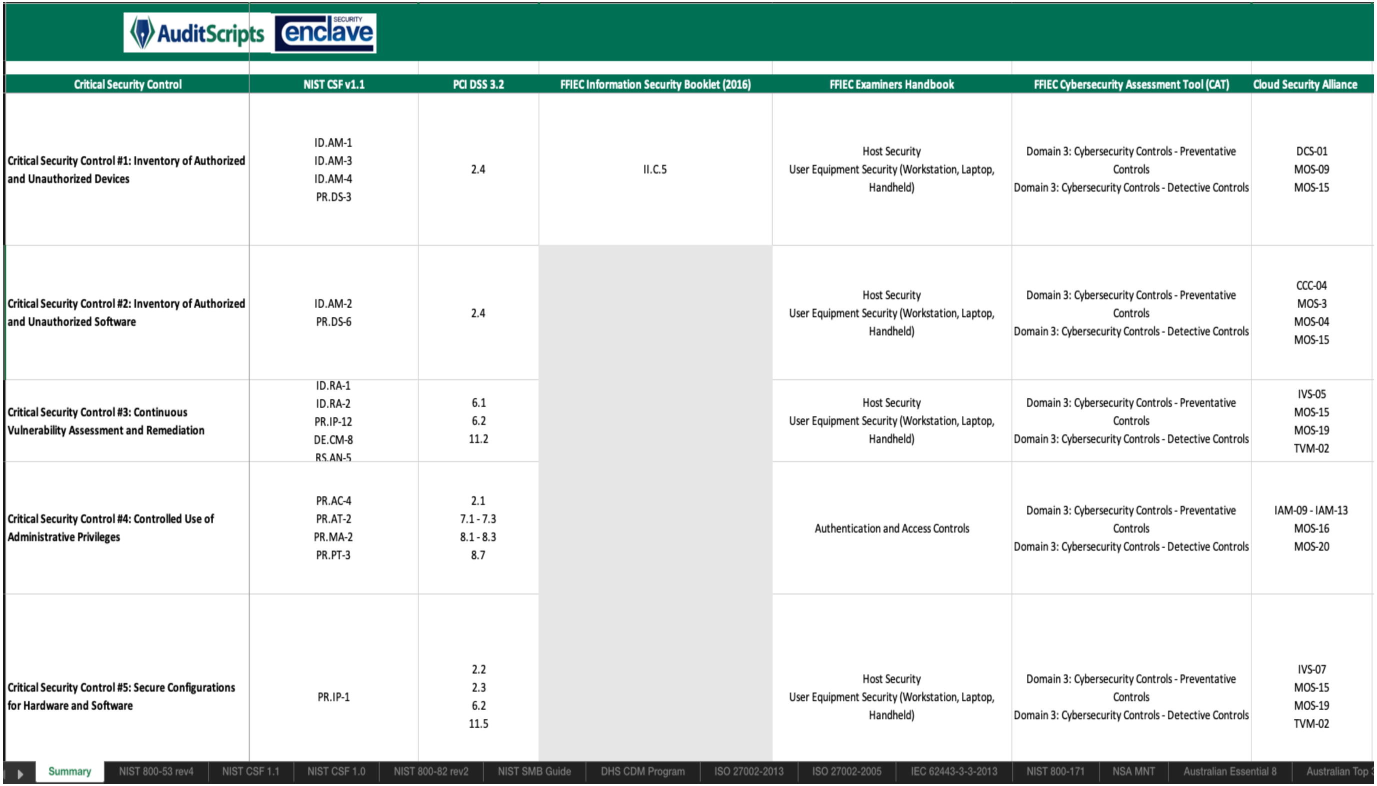
- FFIEC
  Federal Financial Institutions Examination Council IT Examination Handbook InfoBase

- CIS
  Center for Internet Security CIS controls

- PCI
  Payment Card Industry Security Standards council

- CSA
  Cloud Security Allowance

Standards Based Operations

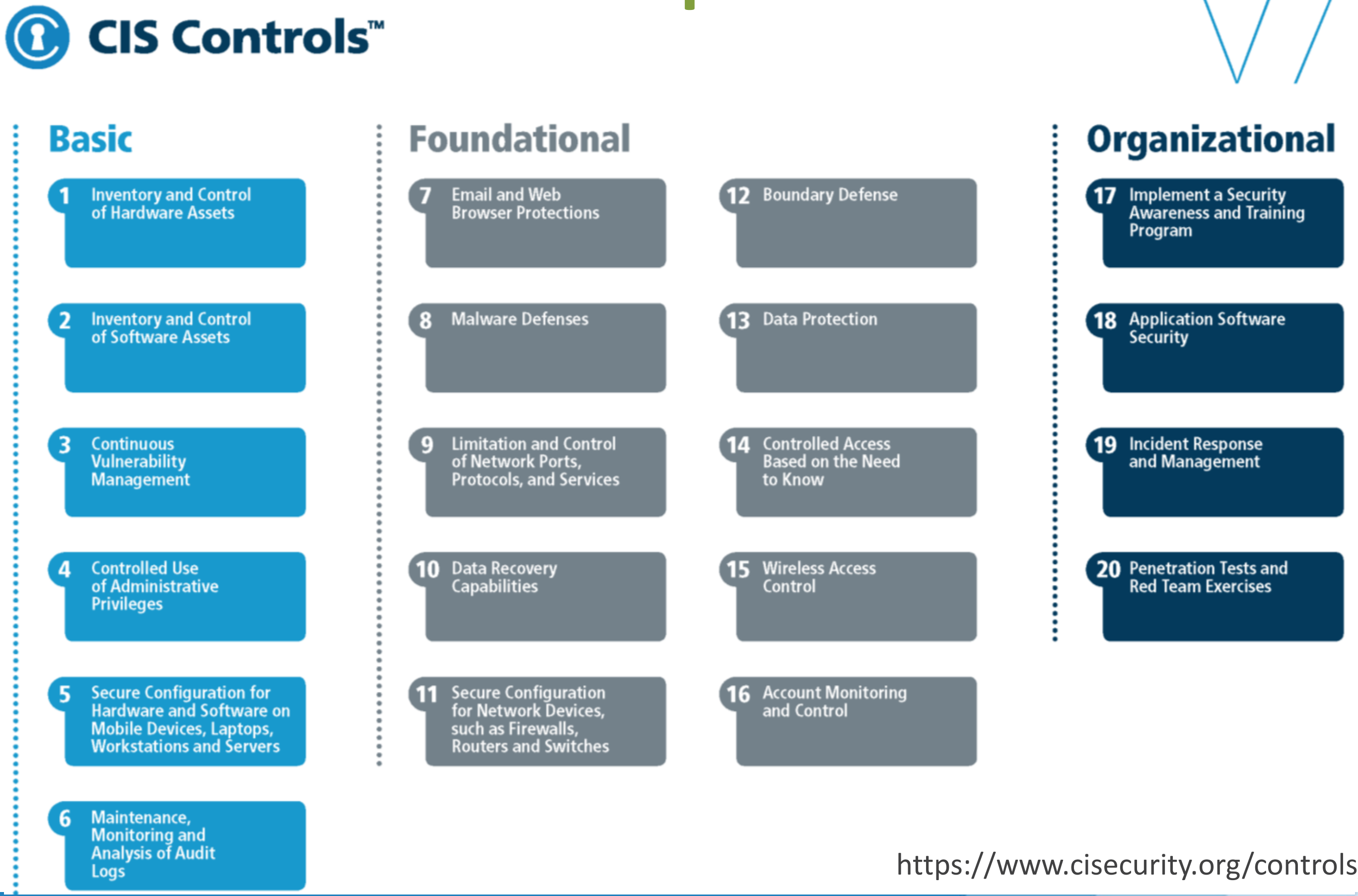


AuditScripts enclave SECURITY

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

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

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

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

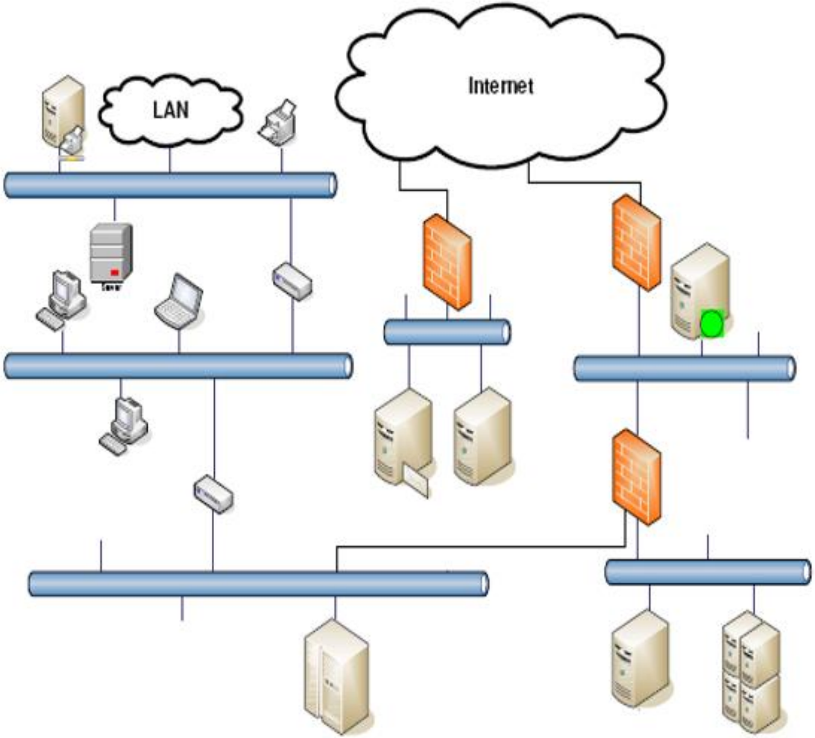
Apply The CIS Critical Controls

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

“Inventory”…

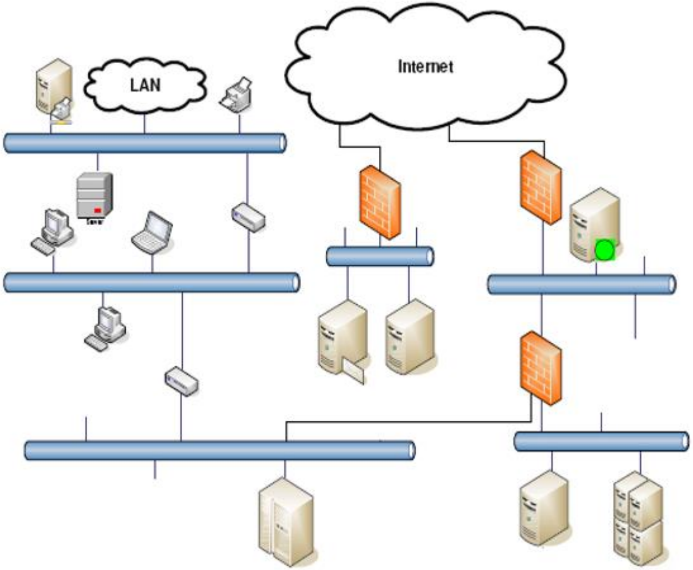
- Set the standard for “Normal”
- Sets the stage for the rest of the controls



Vulnerability Management

3 Continuous Vulnerability Management

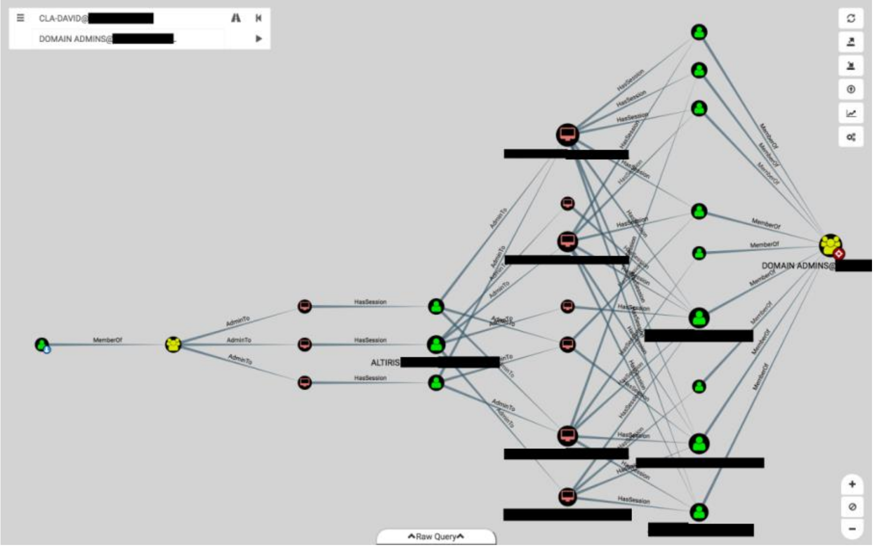
- Monitoring (built in) and scanning (independent) for vulnerabilities
  - “Patch Tuesday” and vulnerability scanning
  - Rogue devices



Passwords

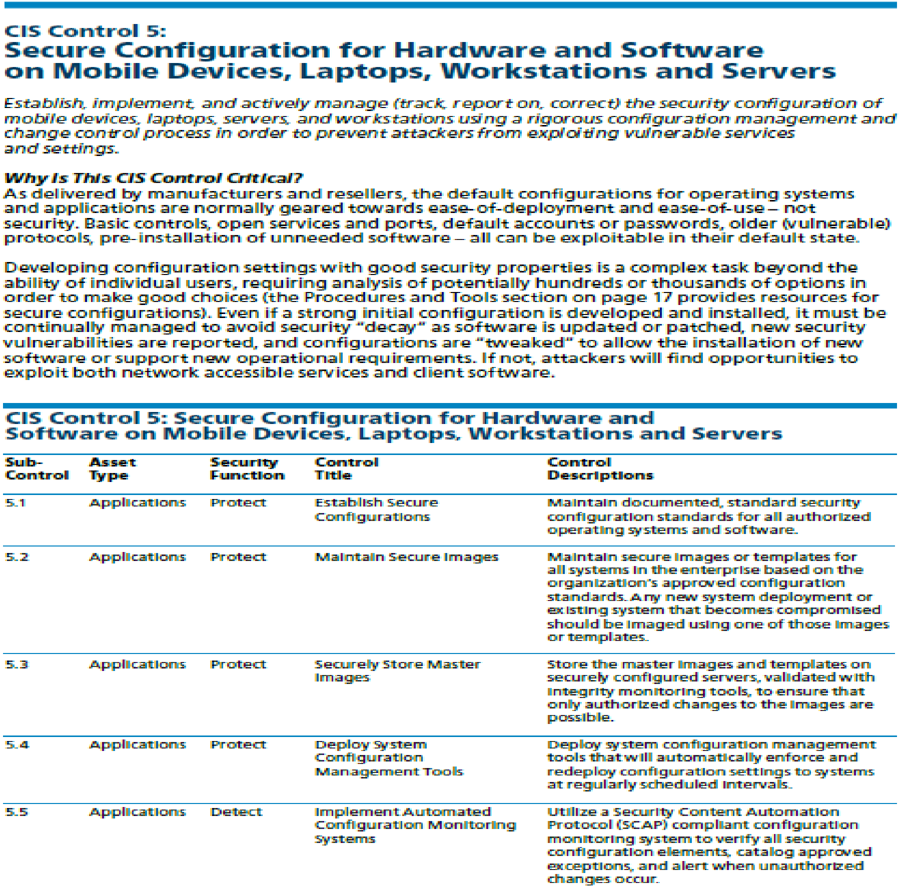
- Controlled use of administrative privileges
  - Standard users should not have admin rights
  - Administrators should have two sets of credentials
- Do NOT log into workstations with administrator privileges

4 Controlled Use of Administrative Privileges


CLA-DAVID@[redacted]
DOMAIN ADMINS@[redacted]

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.

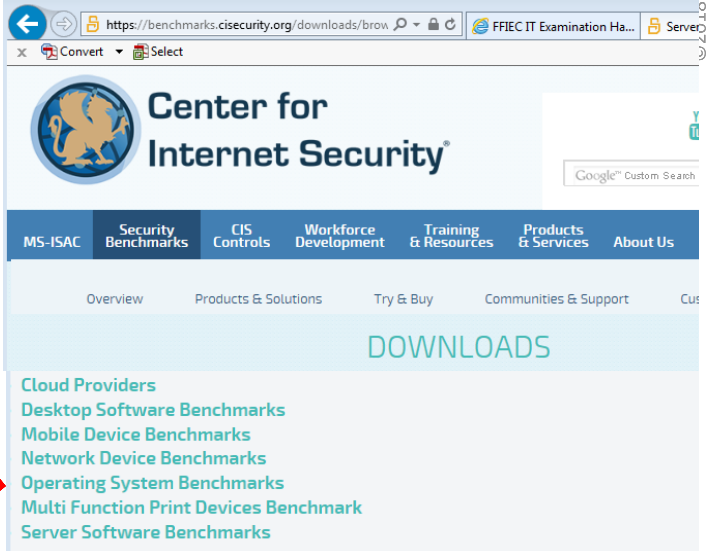
CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

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

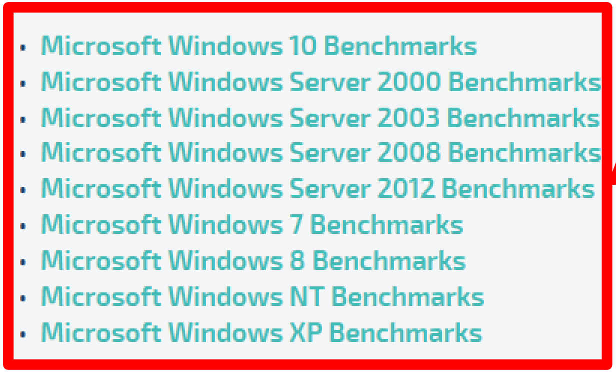
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

- Secure Standard Builds
- Hardening Checklists



DOWNLOADS

- Cloud Providers
- Desktop Software Benchmarks
- Mobile Device Benchmarks
- Network Device Benchmarks
- Operating System Benchmarks
- Multi Function Print Devices Benchmark
- Server Software Benchmarks

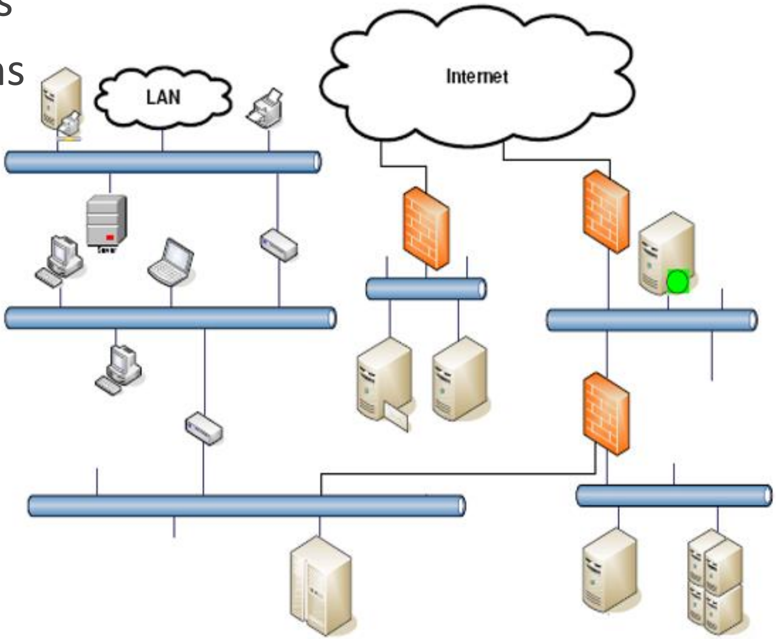


- Microsoft Windows 10 Benchmarks
- Microsoft Windows Server 2000 Benchmarks
- Microsoft Windows Server 2003 Benchmarks
- Microsoft Windows Server 2008 Benchmarks
- Microsoft Windows Server 2012 Benchmarks
- Microsoft Windows 7 Benchmarks
- Microsoft Windows 8 Benchmarks
- Microsoft Windows NT Benchmarks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

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

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

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

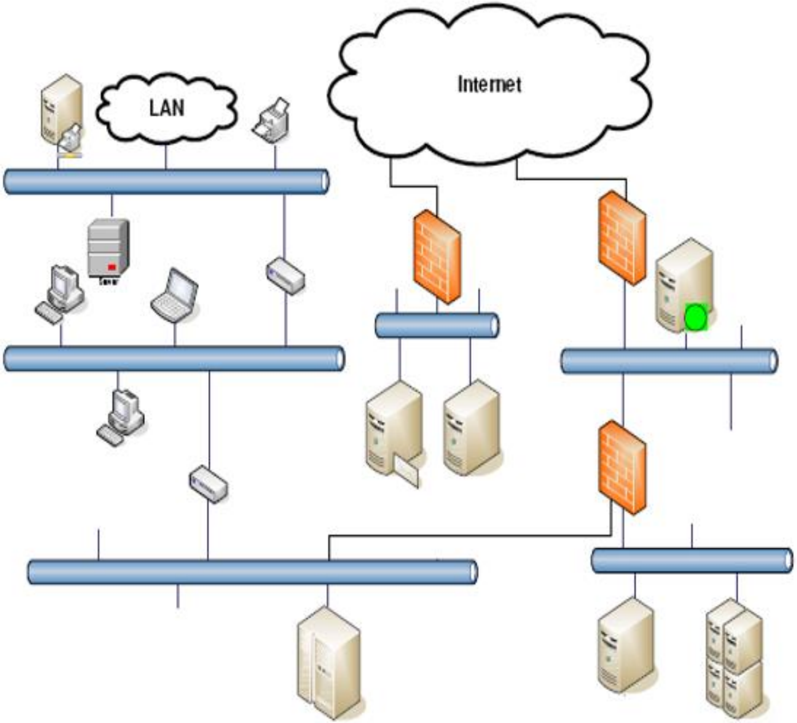
12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

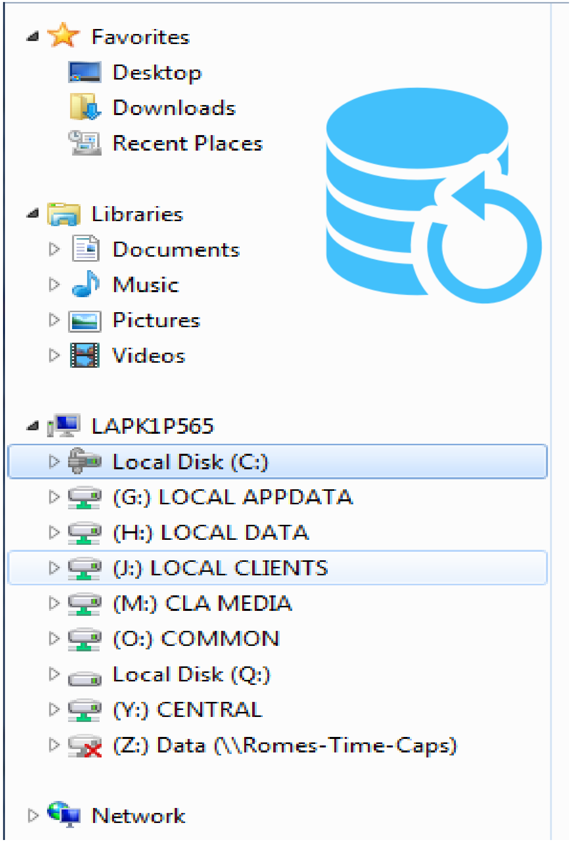
15 Wireless Access Control

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*


Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
LAPK1P565
Local Disk (C:)
(G:) LOCAL APPDATA
(H:) LOCAL DATA
(J:) LOCAL CLIENTS
(M:) CLA MEDIA
(O:) COMMON
Local Disk (Q:)
(Y:) CENTRAL
(Z:) Data (\\Romes-Time-Caps)
Network

Organizational Controls

Improvement Processes and Resilience

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

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

Standards Based Operations

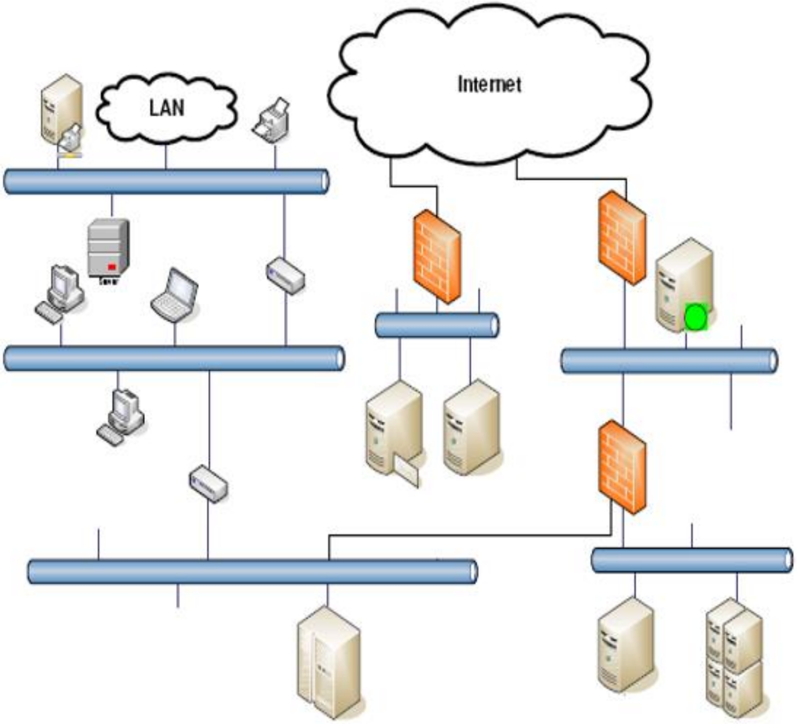
Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

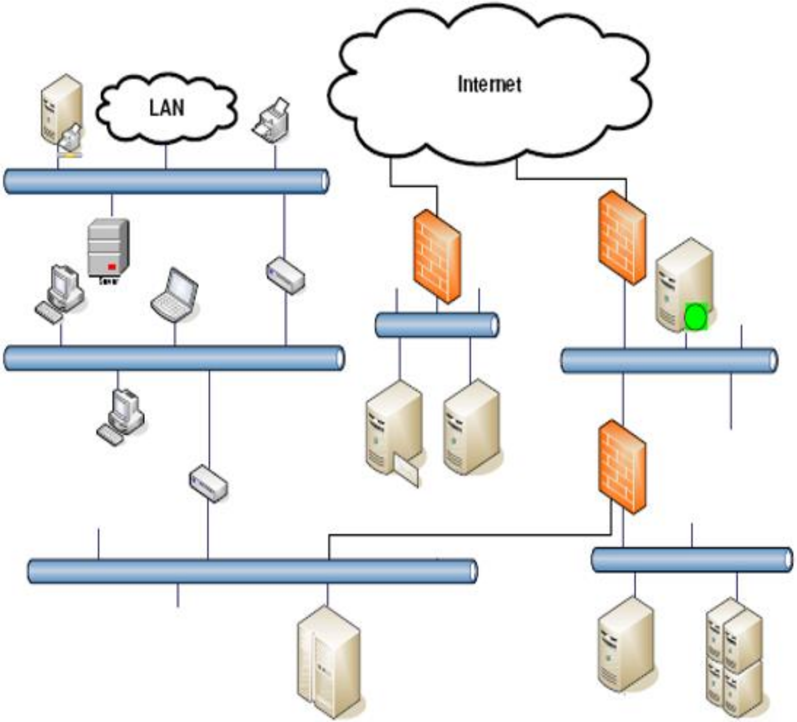
19 Incident Response and Management

20 Penetration Tests and Red Team Exercises



Know Your Network
Know What "Normal" Looks Like

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

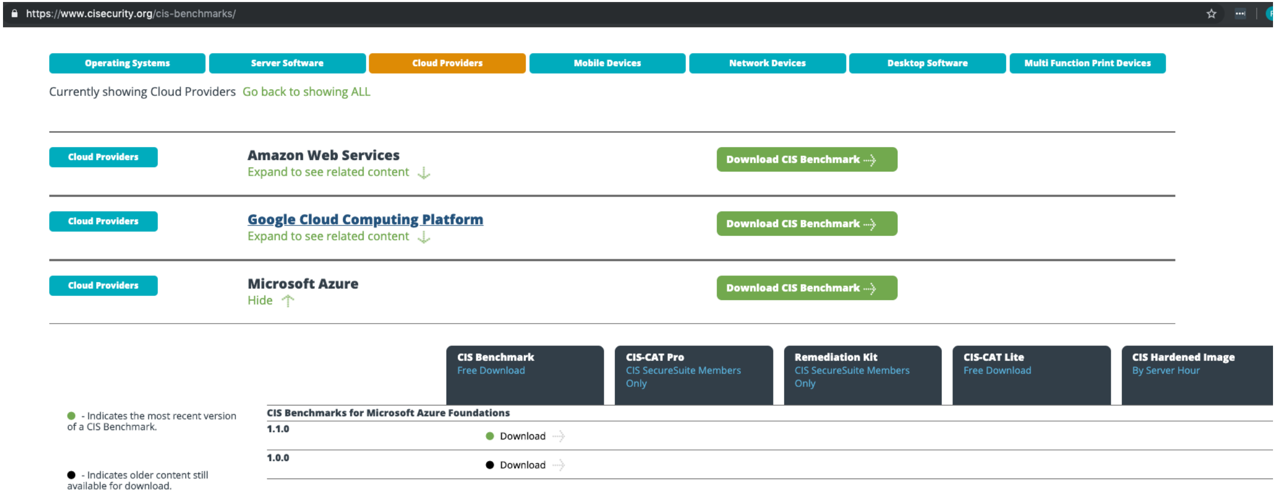


- System inventory
- Application inventory
- Data inventory

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



https://www.cisecurity.org/cis-benchmarks/

Currently showing Cloud Providers Go back to showing ALL

Cloud Providers	**Amazon Web Services** Expand to see related content	Download CIS Benchmark
Cloud Providers	**Google Cloud Computing Platform** Expand to see related content	Download CIS Benchmark
Cloud Providers	**Microsoft Azure** Hide	Download CIS Benchmark

CIS Benchmark	CIS-CAT Pro	Remediation Kit	CIS-CAT Lite	CIS Hardened Image
Free Download	CIS SecureSuite Members Only	CIS SecureSuite Members Only	Free Download	By Server Hour

CIS Benchmarks for Microsoft Azure Foundations

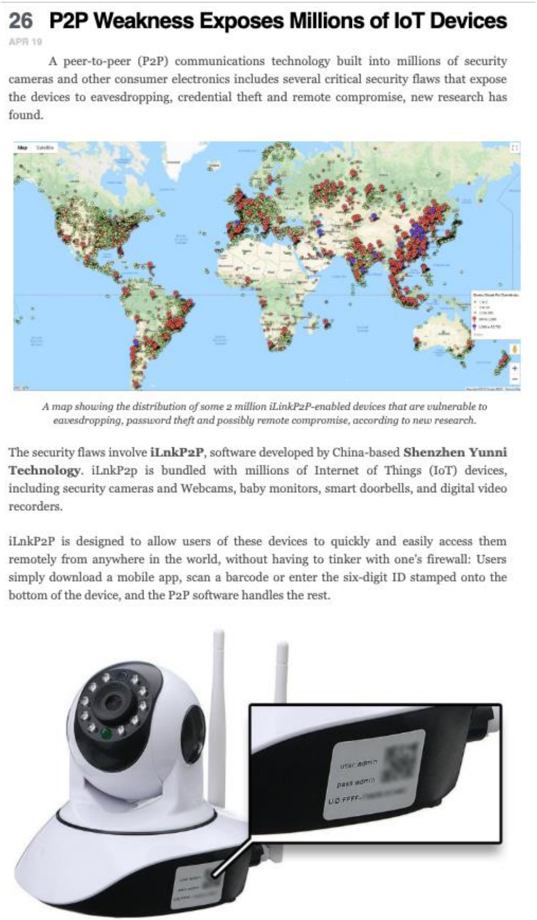
1.1.0	● Download
1.0.0	● Download

● - Indicates the most recent version of a CIS Benchmark.

● - Indicates older content still available for download.

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

Summary

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

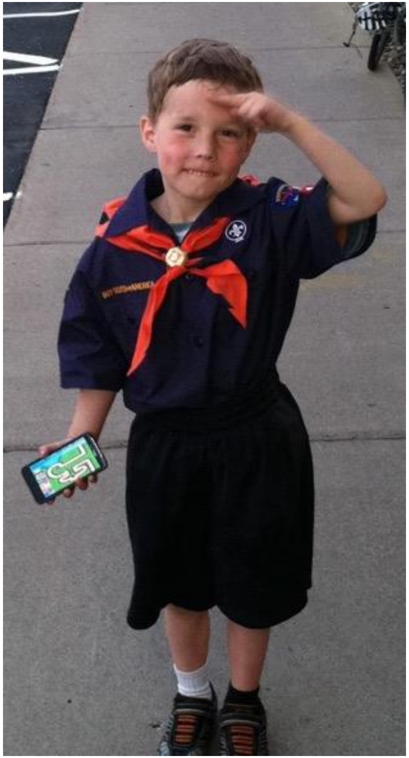
➤PRACTICE

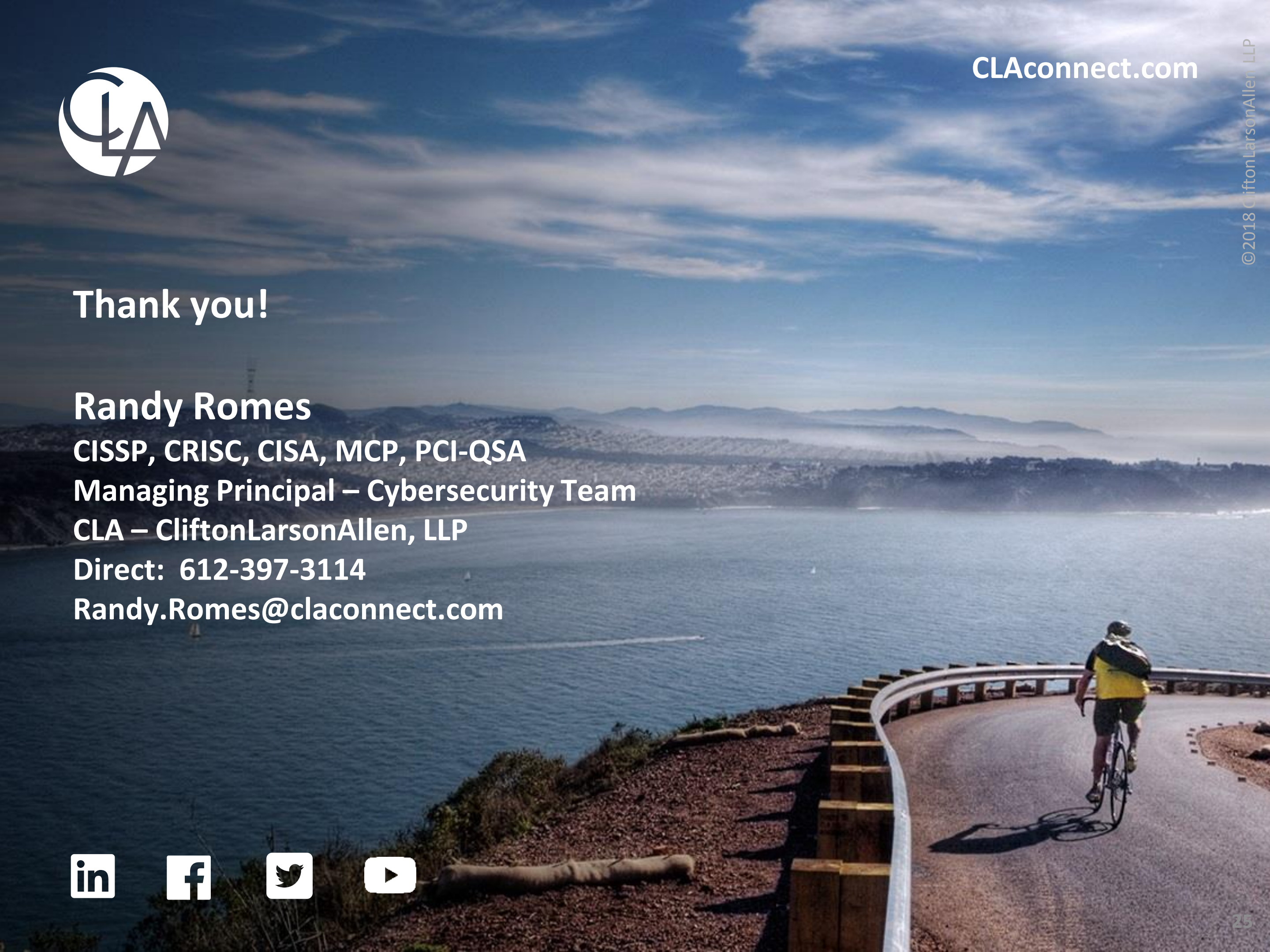
Summary

- 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

ABC’s of Hardening the Network

June 2019

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

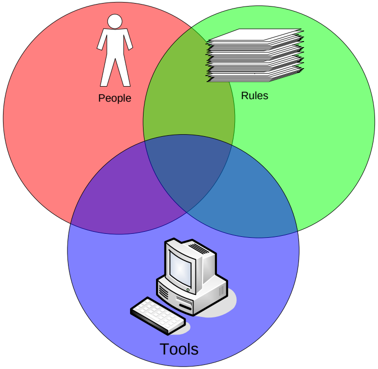
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Create Opportunities

We promise to know you and help you.

Bottom Line Up Front

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



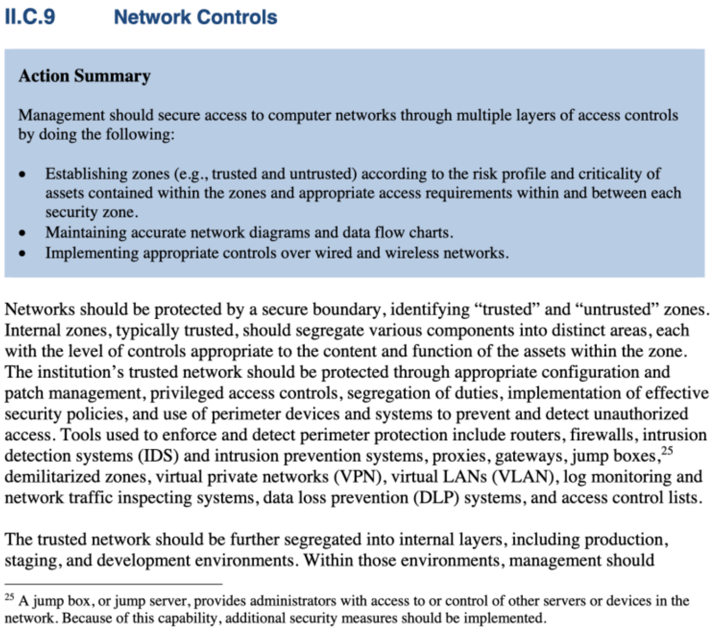
- Turn off the components you don't need
- Change the defaults
- Train your people
- Manage, Tune, and Monitor the systems

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

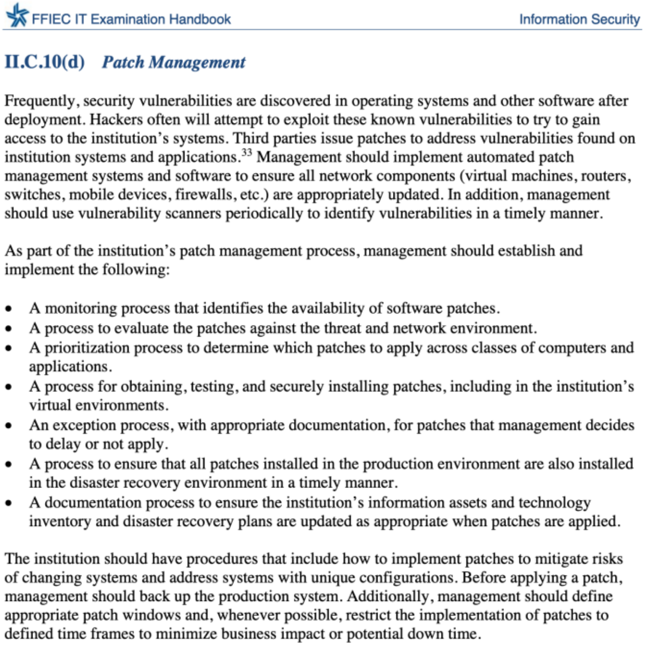
Management should secure access to computer networks through multiple layers of access controls by doing the following:

- 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.



FFIEC IT Examination Handbook Information Security

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.

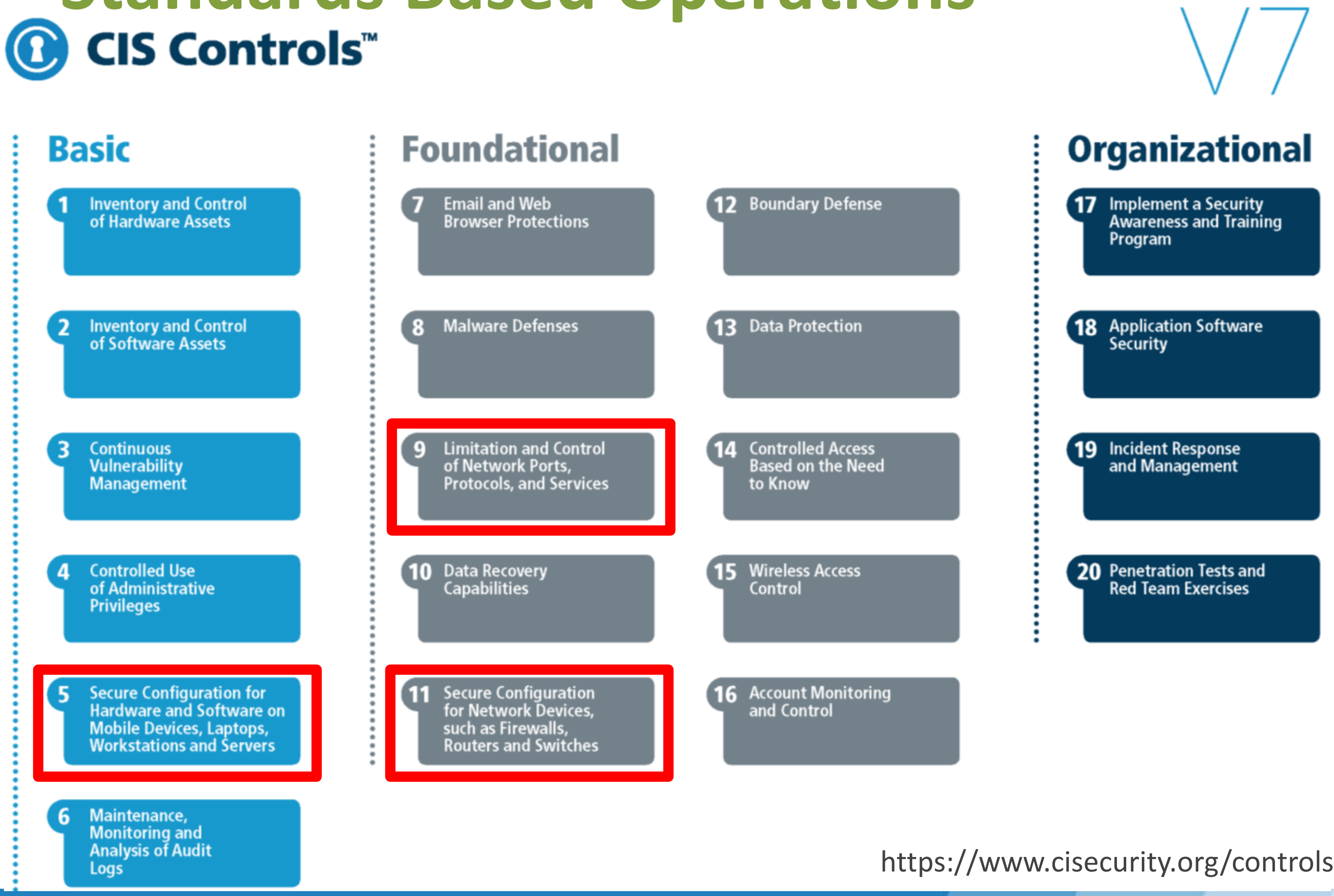
FFIEC Network Controls Handbook Example

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/

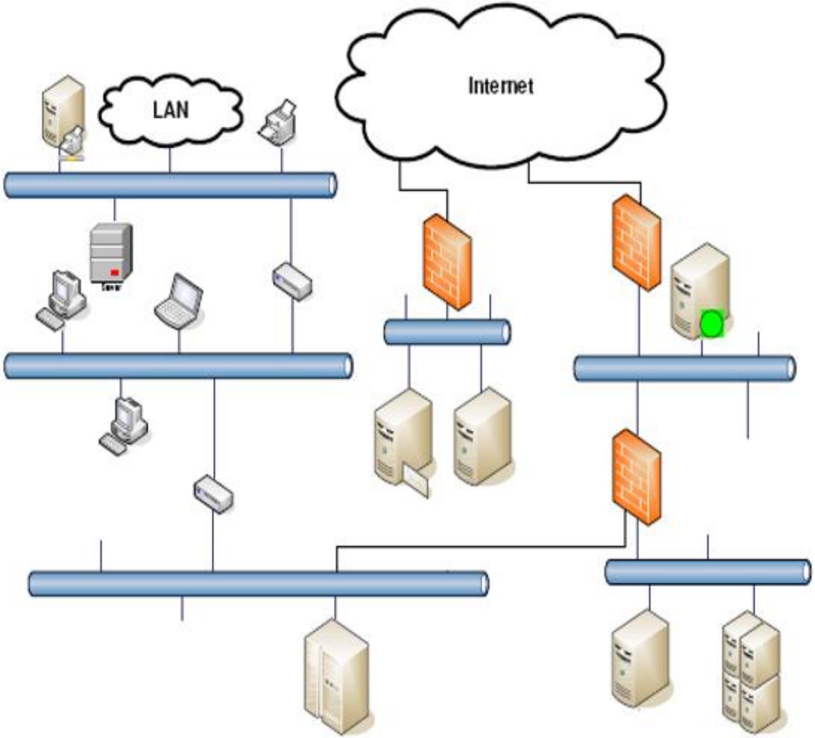
Apply The CIS Critical Controls

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

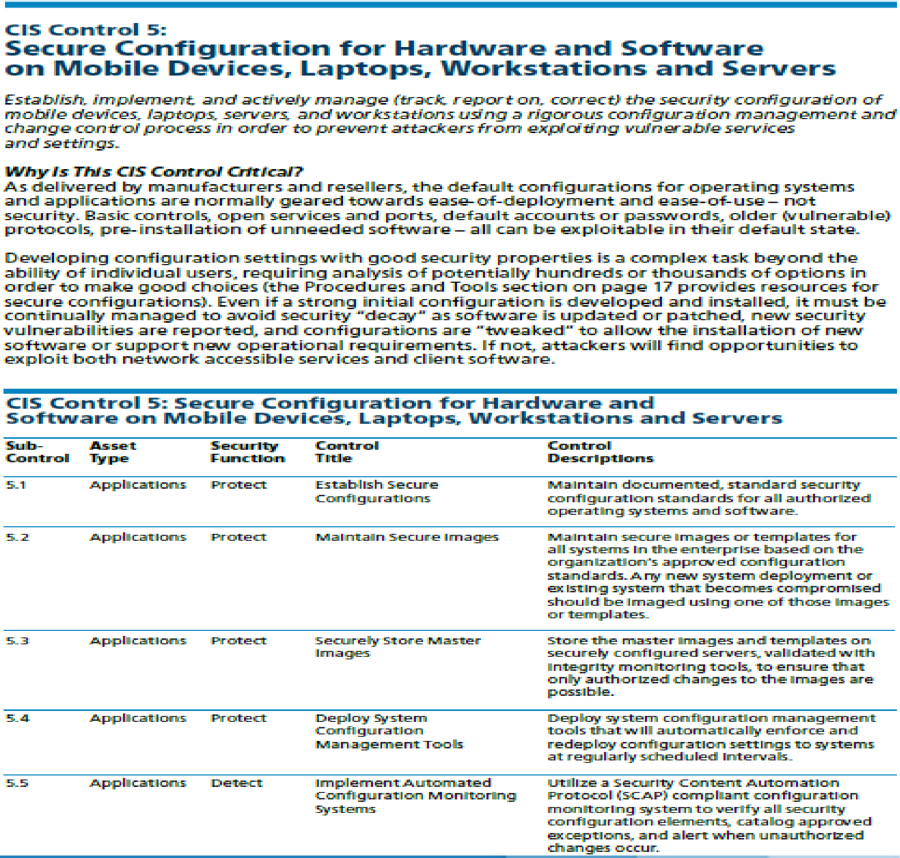
“Inventory”…

- 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.

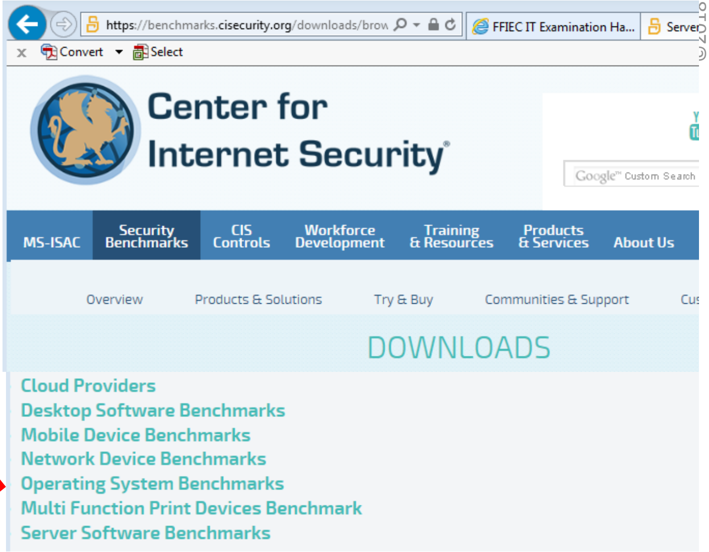
CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

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

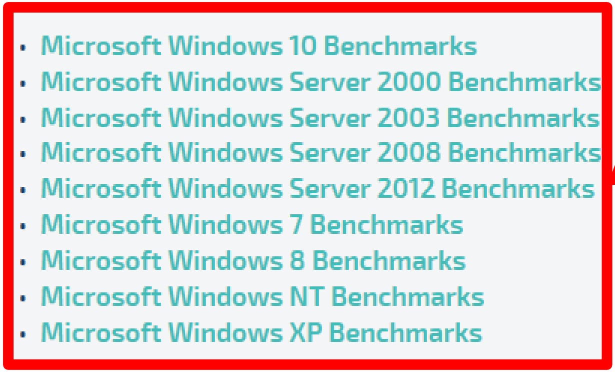
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

- Secure Standard Builds
- Hardening Checklists



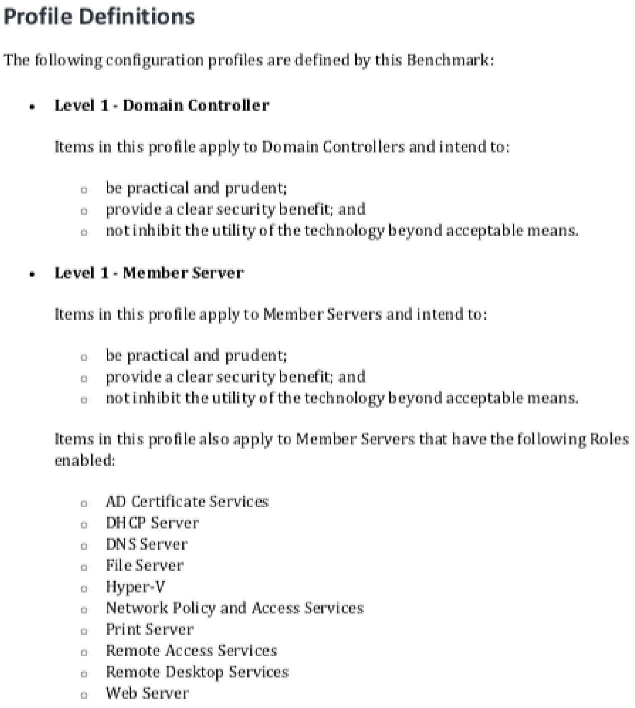
DOWNLOADS

Cloud Providers
Desktop Software Benchmarks
Mobile Device Benchmarks
Network Device Benchmarks
Operating System Benchmarks
Multi Function Print Devices Benchmark
Server Software Benchmarks



- 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.

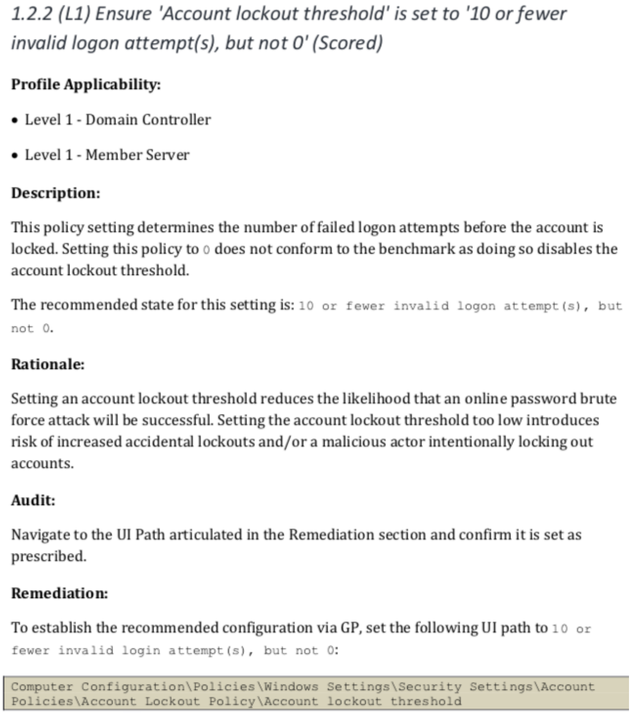
- **Level 1 - Member Server**

  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

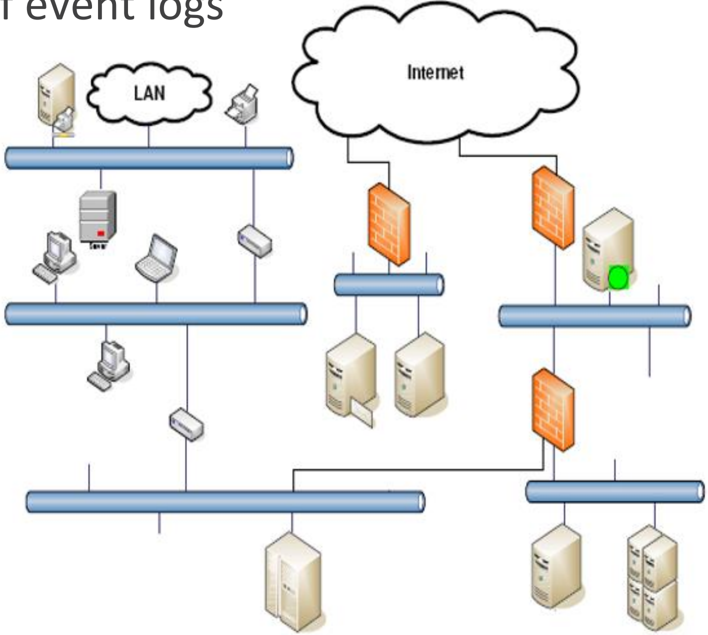
Hardening the Network – Internet of Things (IoT)

- 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

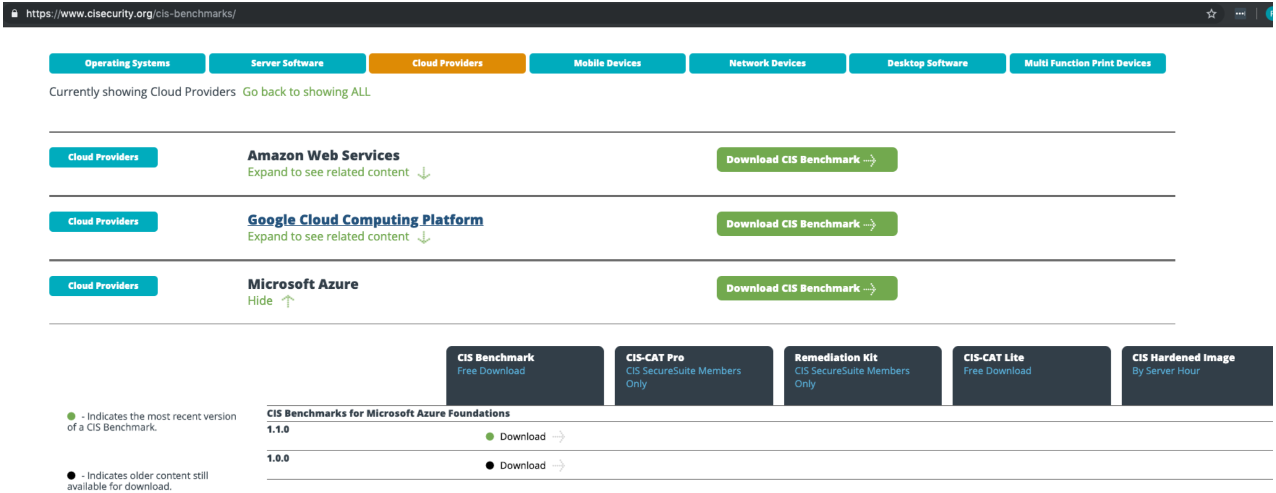
Common Security Issues

- 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



https://www.cisecurity.org/cis-benchmarks/

Currently showing Cloud Providers Go back to showing ALL

Cloud Providers	**Amazon Web Services** Expand to see related content	Download CIS Benchmark
Cloud Providers	**Google Cloud Computing Platform** Expand to see related content	Download CIS Benchmark
Cloud Providers	**Microsoft Azure** Hide	Download CIS Benchmark

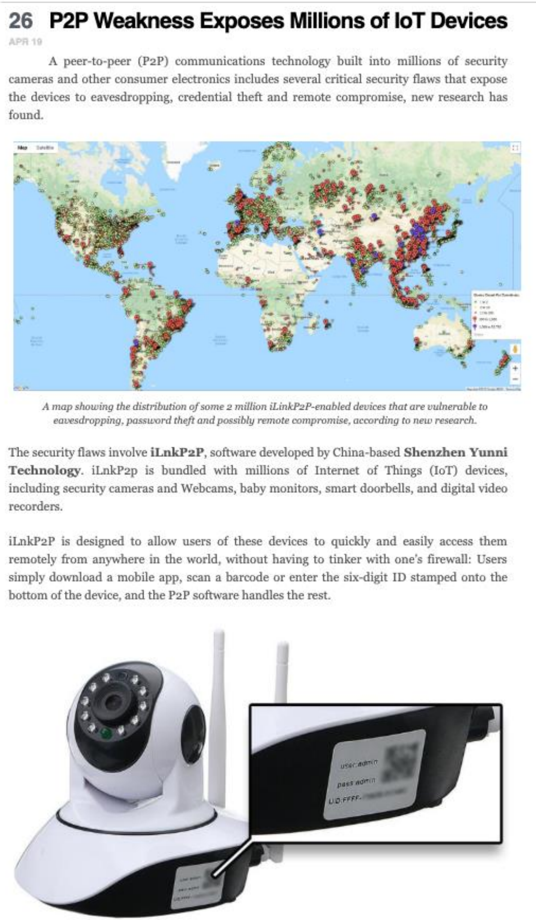
	CIS Benchmark Free Download	CIS-CAT Pro CIS SecureSuite Members Only	Remediation Kit CIS SecureSuite Members Only	CIS-CAT Lite Free Download	CIS Hardened Image By Server Hour
CIS Benchmarks for Microsoft Azure Foundations					
1.1.0	🟢 Download				
1.0.0	● Download				

🟢 - Indicates the most recent version of a CIS Benchmark.

● - Indicates older content still available for download.

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.

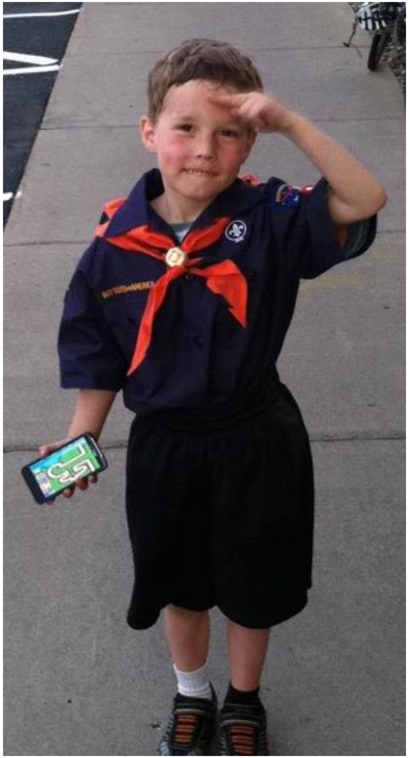
iLnkP2P is designed to allow users of these devices to quickly and easily access them remotely from anywhere in the world, without having to tinker with one's firewall: Users simply download a mobile app, scan a barcode or enter the six-digit ID stamped onto the bottom of the device, and the P2P software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

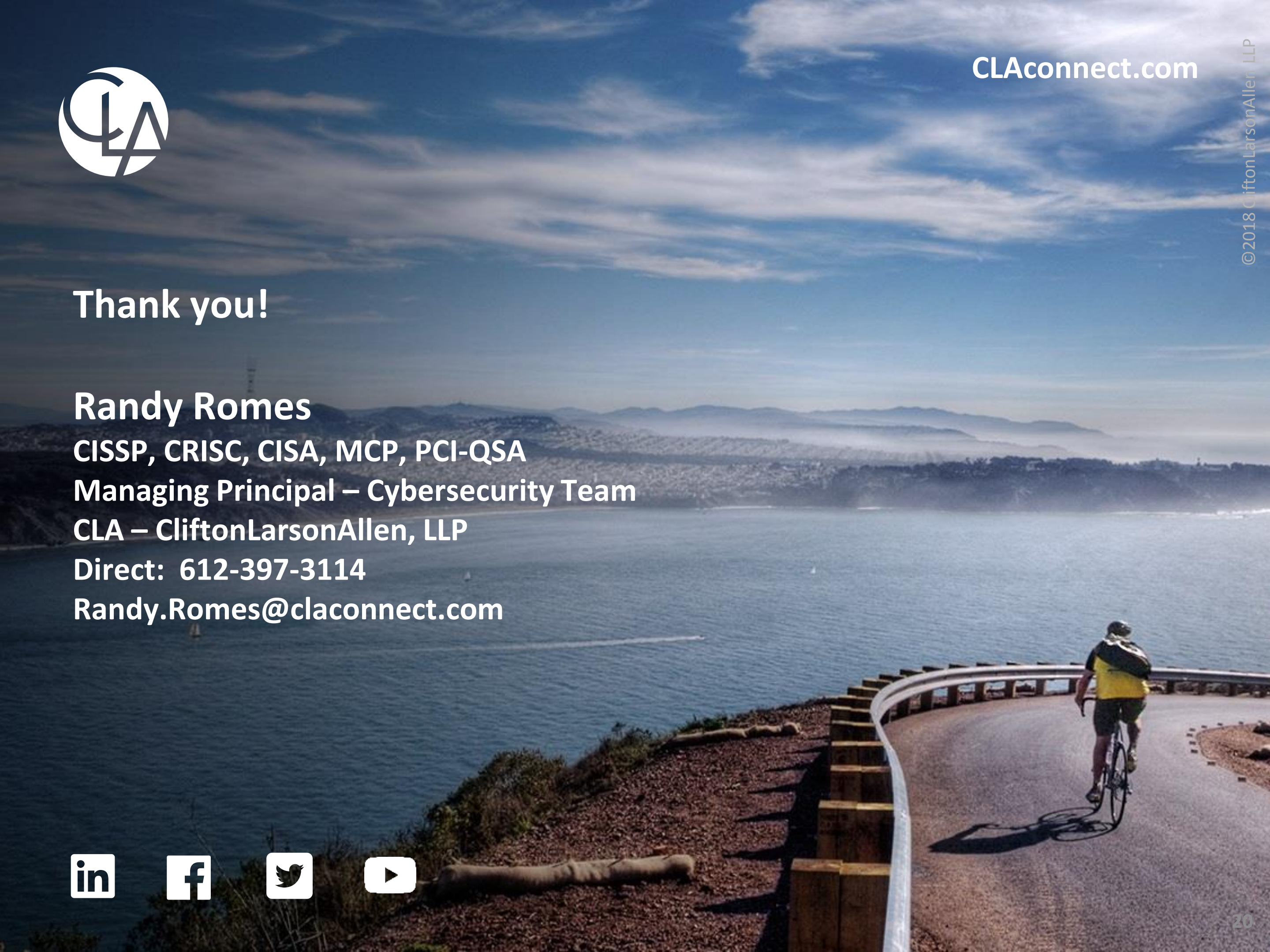
https://krebsonsecurity.com/2019/04/p2p-weakness-exposes-millions-of-iot-devices/

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