



We promise
to *know you* and *help you.*

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

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



Today's Cybersecurity Risks

June, 2018

About CliftonLarsonAllen



WEALTH ADVISORY

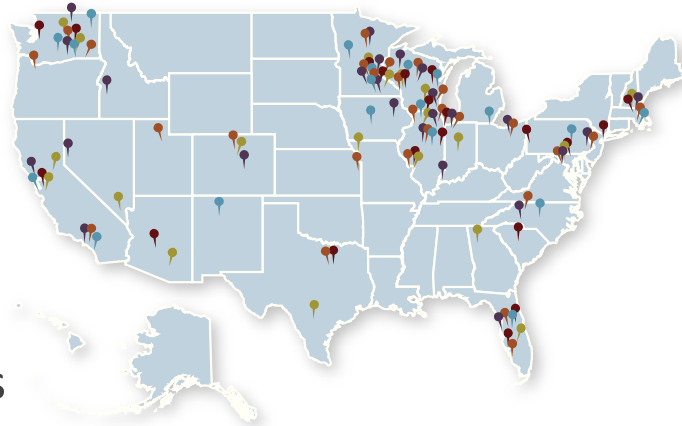


OUTSOURCING



AUDIT, TAX,
AND CONSULTING

- A professional services firm with three distinct business lines
 - Wealth Advisory
 - Outsourcing
 - Audit, Tax, and Consulting
- More than 4,500 employees
- Offices coast to coast



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



We promise to know you and help you.

Information Security Services

Information Security offered as specialized service offering for over 20 years

- Penetration Testing and Vulnerability Assessment
- IT/Cyber security risk assessments
- IT audit and compliance
 - GLBA/FFIEC, NIST, PCI-DSS, HITRUST, etc...
- Incident response and forensics
- Security awareness training
- Independent security consulting
- Internal audit support

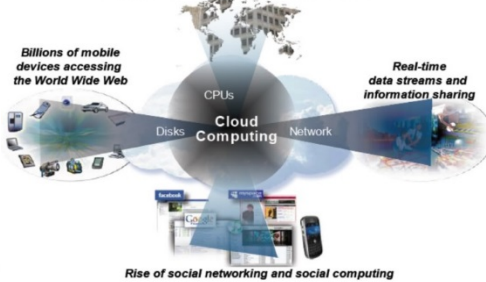
<http://www.claconnect.com/services/information-security#Resources>



Raise Your Hand If...



Cloud Computing, Compute Model for a Smarter Planet
Globalization and Globally Available Resources



INTRODUCING
echo dot

Add Alexa to any room



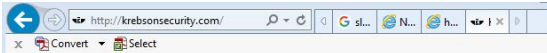
amazon tap

ALEXA-ENABLED
 PORTABLE SPEAKER

JUST TAP & ASK



Internet of Things (IoT)



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.



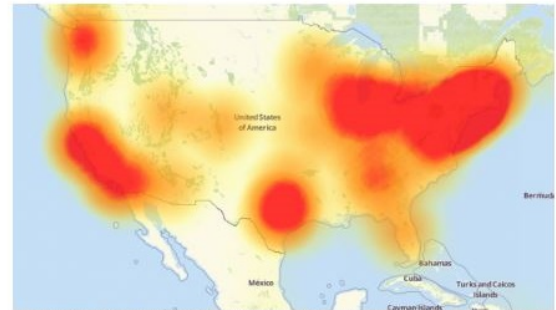
Recently, I heard from a cybersecurity researcher who'd created a virtual “honeypot” environment designed to simulate hackable IoT devices. The source, who asked to remain anonymous, said his honeypot soon began seeing traffic destined for **Asus** and **Linksys** routers running default credentials. 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: Downtime.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



Raise Your Hand If...





We promise
to *know you* and *help you.*

**Ten Ways to Lose
EVERYTHING...**

10 Ways to Lose EVERYTHING

1. Users clicking links

Fax Message [Caller-ID: MedSource]

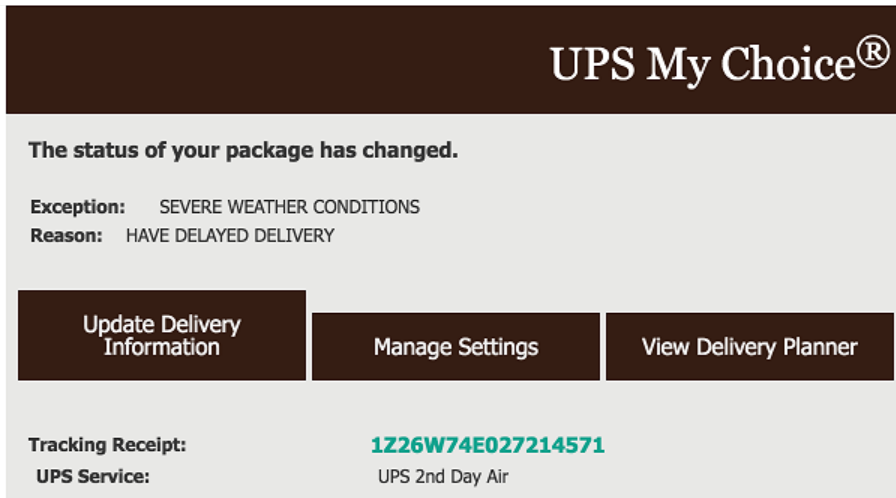
You have received a 2 page fax on **Tuesday, December 19**, 2016 at 8:34 -500
The reference number for this fax is 84502384542

[Click here to view this message](#)



10 Ways to Lose EVERYTHING

2. Users clicking links



The screenshot shows a notification from UPS My Choice. At the top, the text reads "UPS My Choice®". Below this, a message states "The status of your package has changed." followed by "Exception: SEVERE WEATHER CONDITIONS" and "Reason: HAVE DELAYED DELIVERY". There are three buttons: "Update Delivery Information", "Manage Settings", and "View Delivery Planner". At the bottom, it shows "Tracking Receipt: 1Z26W74E027214571" and "UPS Service: UPS 2nd Day Air".

UPS My Choice®

The status of your package has changed.

Exception: SEVERE WEATHER CONDITIONS
Reason: HAVE DELAYED DELIVERY

[Update Delivery Information](#) [Manage Settings](#) [View Delivery Planner](#)

Tracking Receipt: **1Z26W74E027214571**
UPS Service: UPS 2nd Day Air



10 Ways to Lose EVERYTHING

3. Users clicking links


ADP Immediate Notification

Over the past few days we have had reports of issues with the distributed W-2's. As a result we are issuing W-2c (Corrected W-2) for a large subset ADP customers, including _____ employees. Please use ADP's W2 Secure Download portal below to obtain the corrected W-2 and contact your Human Resources department with any further questions.

[W2 Secure Download](#)

Ref: 22771

As usual, thank you for choosing ADP as your business affiliate!



HR. Payroll. Benefits.

The ADP logo and ADP are registered trademarks of ADP, Inc.
In the business of your success is a service mark of ADP, Inc.
© 2012 ADP, Inc. All rights reserved.



We promise to know you and help you.

10 Ways to Lose EVERYTHING

4. Users clicking links

New ZixCorp secure email message from

Open Message

To view the secure message, click Open Message.

The secure message expires on July 22, 2016 @ 07:39 PM (GMT).

Do not reply to this notification message; this message was auto-generated by the sender's security system. To reply to the sender, click Open Message.

If clicking Open Message does not work, copy and paste the link below into your Internet browser address bar.

<https://web1.zixmail.net/s/e>

Want to send and receive your secure messages transparently?

[Click here](#) to learn more.



10 Ways to Lose EVERYTHING

5. Users clicking links

Your wireless bill is ready.



The current billing statement for your wireless account is now available in My Verizon.

Please note, payments and/or adjustment made to your account since your invoice was generated will not be reflected in the amount shown.

In order to view your bill, please sign in to [My Verizon](#).

Thank you for choosing Verizon Wireless.

Online Bill Summary

Account Number:
XXXXX5722-00009

Scheduled Automatic
Payment:
01/15/2016

Total Amount Due:
\$ 958.54

[Pay Bill](#) | [View Online Bill](#)



We promise to know you and help you.

10 Ways to Lose EVERYTHING

6. Users clicking links

Hi,

I am applying for an IT internship and I received your email through our IT program here at ISU. I am really interested in learning about networking and system administration. Can you take a look at my resume and let me know if I would be a good fit for your program and if there are any current openings?

[Resume](#)



10 Ways to Lose EVERYTHING

7. Users clicking links

Microsoft has released a tool that will ensure our computers and software are compatible with Windows 10. Please download and run the tool. The tool will run in the background so you can continue working and will not require you to reboot your computer.

If after running the tool, it says that your computer is not compatible, please let me know along with the reason it gives.

Download the Windows 10 Preparation Tool from the link on the top of the page at <http://windows10.microsoft.com>.



10 Ways to Lose EVERYTHING

8. Users clicking links

Buongiorno!

In celebration of the grand opening of our new Alexandria franchise, and as a local favorite for authentic Italian food, we're offering coupons redeemable for one **FREE** lunch or dinner. This offer is being made in appreciation of the patronage of local businesses and is redeemable at any of our locations.

Your coupon is valid through the end of August. Follow the link for the direct download of your coupon, along with our valid menu items that may be purchased with your coupon. Please print out just the coupon and deliver it to your server to enjoy a **FREE** authentic Italian meal at Bello Cucina!

[Coupon Link](#)

Arrivederci,

Jason Mueller, Owner, Bello Cucino
106 West Lincoln Ave



10 Ways to Lose EVERYTHING

9. Users clicking links



Greetings,

A recent group of viruses have been released which put systems at risk. These viruses destroy data on the local systems and leak personal information.

Anyone running Mac OS X or Windows should download the following patch to be exploited.

Instructions:

1. Click on this link <http://www.java.com/download/>



10 Ways to Lose EVERYTHING

10. Users opening attachments

Dennis Johnson <dennis[redacted]@gmail.com>

to [redacted]

Hi,

I found the [redacted] form on your website and filled it out. Can you take a look and see if it has all the information you need? [redacted]

Thanks,

Dennis Johnson



[Redacted area]

[Redacted area]





Questions



Thank you!

Randy Romes, CISSP, CRISC, MCP, PCI-QSA
Principal, Information Security,
Direct: 612-397-3114
Randy.Romes@claconnect.com



We promise
to *know you* and *help you*.

**Current State of
Cybercrime**

**What are the Bad
Guys Doing?**

Cyber Fraud Themes

- Hackers have “monetized” their activity
 - More sophisticated hacking
 - More “hands-on” effort
 - Smaller organizations targeted
 - Cybercrime as an industry
- Everyone is a target...
- Phishing is a root cause behind the majority of cyber fraud and hacking attacks



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 PII and PFI
 - ◊ W2/Payroll/Benefit info
 - Theft of credit card information
 - Account take overs
 - Ransomware and Interference w/ Operations



The Cost



Global cybercrime cost businesses up to:
\$400 BILLION annually

Some estimate it will reach:
\$2.1 TRILLION by 2019



Marketplace for Stolen (information)

- Attackers buy and sell data on cyber black market
 - “The Dark Web” - Similar to amazon.com

<input type="checkbox"/>	Bin	Card	Debit/Credit	Mark	Expires	Track 1	Code	Country	Bank	Base	Price	Cart
<input type="checkbox"/>	371736	AMEX	CREDIT		07/15	Yes	110	United States, 23456, Virginia Beach, VA	BANK OF AMERICA	American Sanctions 14	305	+
<input type="checkbox"/>	371555	AMEX	CREDIT		09/16	Yes	101	United States, 80123, Littleton, CO	BANK OF AMERICA	American Sanctions 14	305	+
<input type="checkbox"/>	371736	AMEX	CREDIT		03/17	Yes	101	United States, 60540, Naperville, IL	BANK OF AMERICA	American Sanctions 14	305	+
<input type="checkbox"/>	371564	AMEX	CREDIT		05/15	Yes	110	United States, 77081, Houston, TX	BANK OF AMERICA	American Sanctions 14	305	+
<input type="checkbox"/>	371554	AMEX	CREDIT		04/17	Yes	101	United States, 37027, Brentwood, TN	BANK OF AMERICA	American Sanctions 14	305	+
<input type="checkbox"/>	371242	AMEX	CREDIT	GREEN	06/17	Yes	101	United States, 98512, Olympia, WA	AMERICAN EXPRESS COMPANYY	American Sanctions 14	305	+
<input type="checkbox"/>	371570	AMEX	CREDIT		10/16	Yes	101	United States, 97123, Hillsboro, OR	BANK OF AMERICA	American Sanctions 14	305	+
<input type="checkbox"/>	371381	AMEX	CREDIT		10/16	Yes	201	United States, 30328, Atlanta, GA	CITIBANK	American Sanctions 14	248	+



We promise to know you and help you.

Payment Fraud

- Most people interact with their CU electronically
 - Wire transfers & ACH payments
 - Online banking
- Account Take Over (CATO)
 - Compromise accounts/credentials that can move money



Payment Fraud

- Can occur via technical means
 - Attackers “hack” into finance computers
 - Banking Trojans monitor online banking
 - Create fake employees in payroll/ACH file
- Can occur via non-technical means
 - Social engineering
 - Coerce employee to send money
 - ◇ E.g. Fake CEO emails cost businesses BILLIONS over last 3years



CATO Lawsuits – UCC

- Electrical Contractor vs. Bank
 - > \$300,000 stolen via ACH through CATO
 - Internet banking site was “down” – DOS?
 - Contractor asserting bank processed bogus ACH file without any call back
- Escrow Company vs. Bank
 - > \$400,000 stolen via single wire through CATO
 - ◇ *Escrow company passed on dual control offered by the bank*
 - Court ruled in favor of bank
 - Company’s attorneys failed to demonstrate bank’s procedures were not commercially reasonable



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

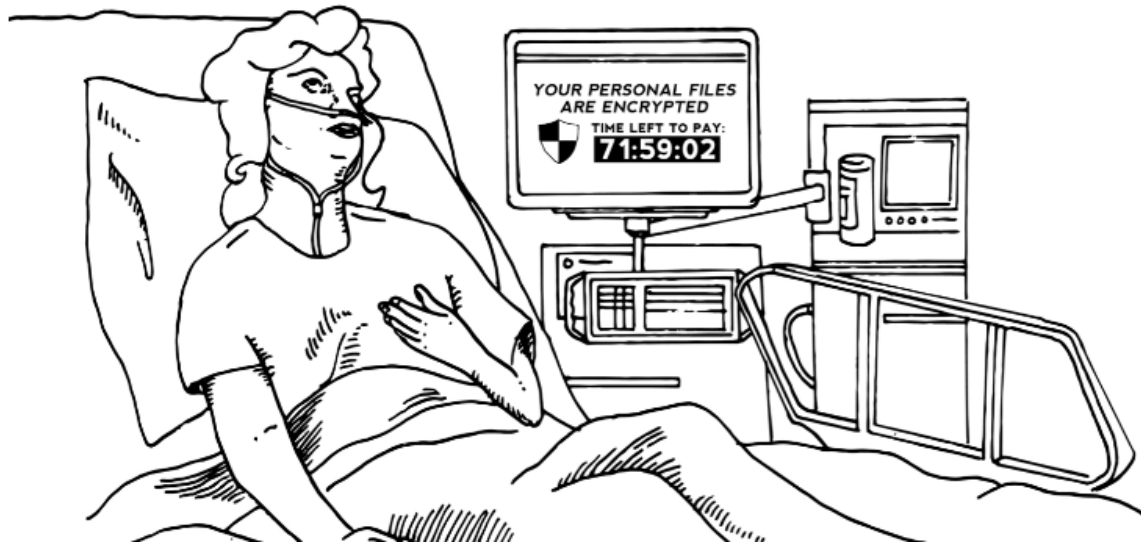
- Unique twist related to Core Conversion...



Ransomware

Hospital ransomware: A chilling wake-up call

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



<http://www.engadget.com/2016/02/19/hospital-ransomware-a-chilling-wake-up-call/>



We promise to know you and help you.

Ransomware

<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

📄 🖨️ 📧 🐦 Twitter 📘 Facebook 🌐 LinkedIn ⭐ Credit Eligible [Get Permission](#)



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](#)).



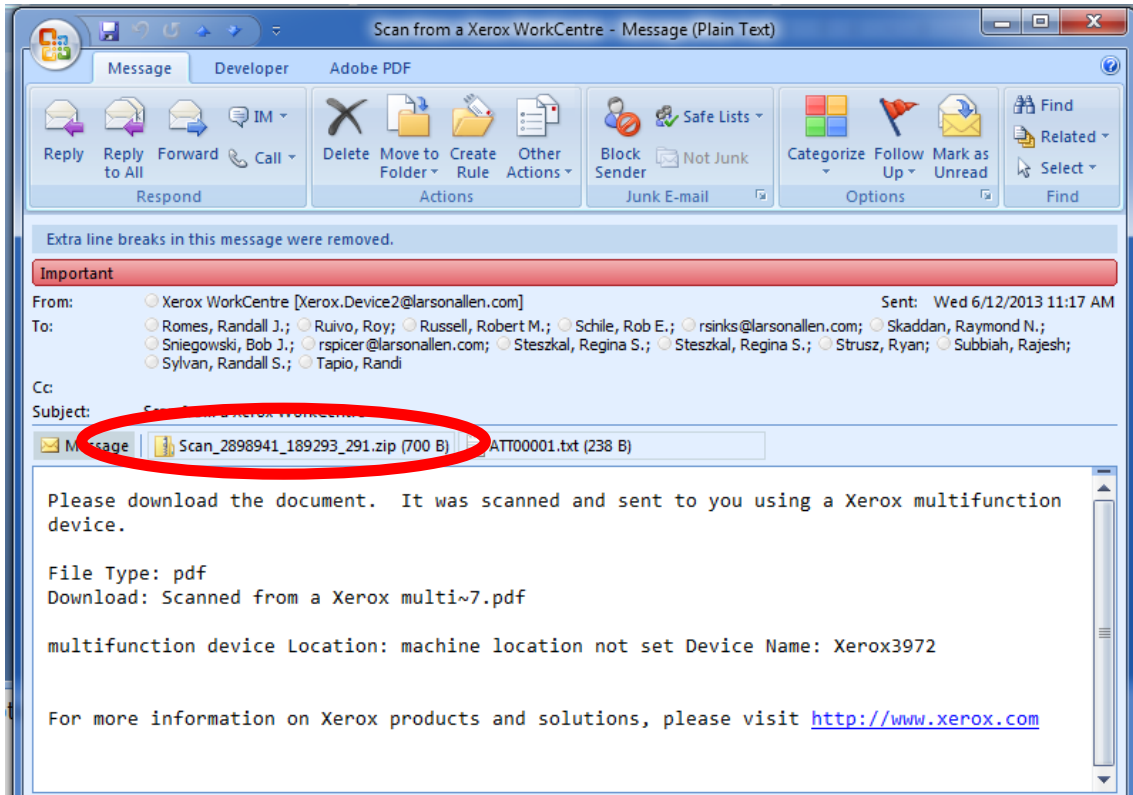
We promise to know you and help you.

Ransomware



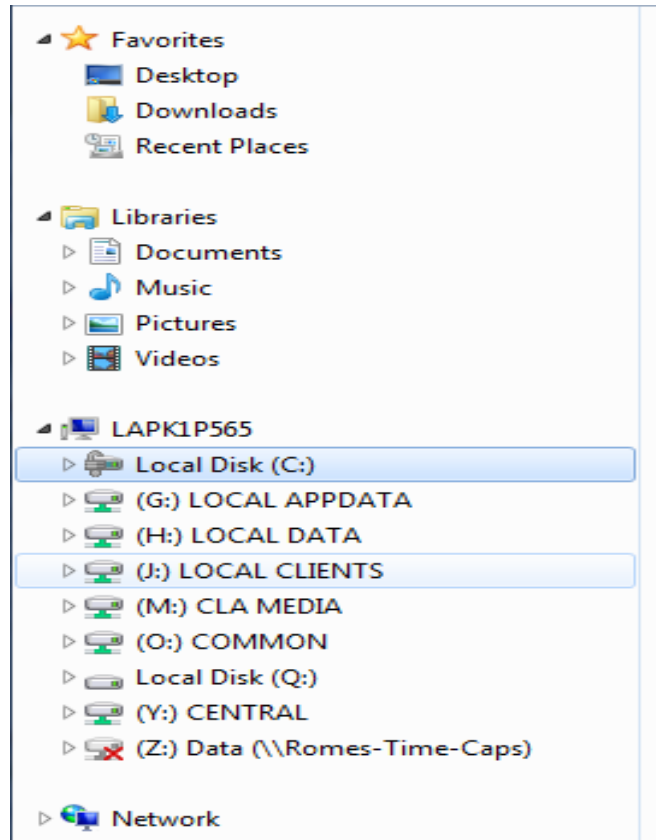
- Cryptolocker, Locky, WannaCry, etc.
- Encrypts all data, holds in “ransom” for \$\$
 - Data on local machine and on network
- Can affect non-Windows OS (e.g. Mac)

Ransomware



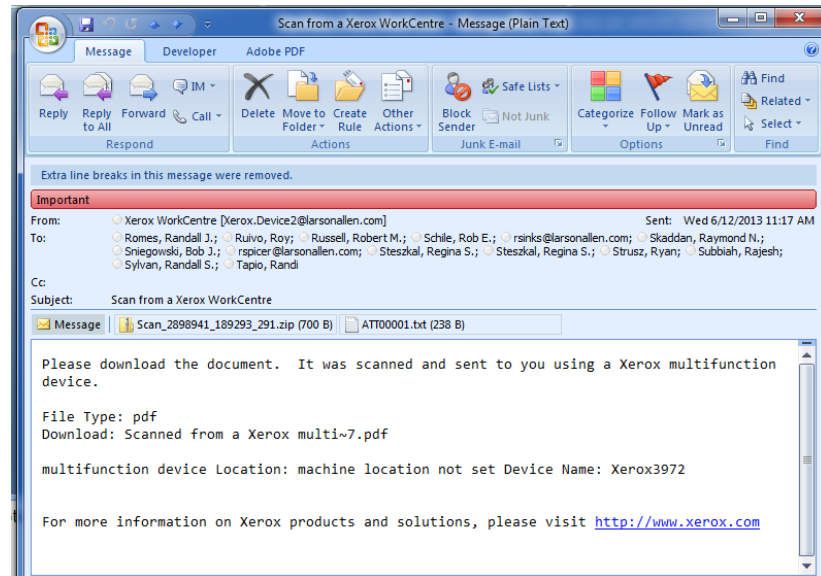
Ransomware

- Malware encrypts everything it can interact with



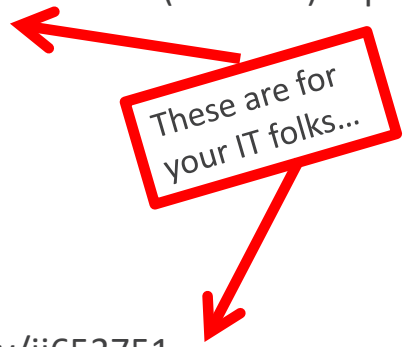
Ransomware Defensive Strategies

- Filtering capabilities
- Users that are aware and savvy



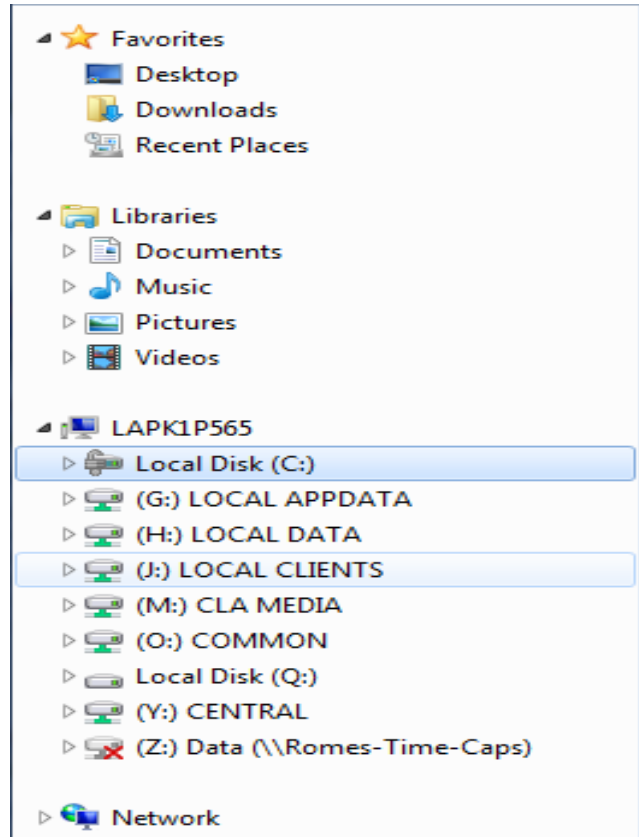
Ransomware Defensive Strategies

- Minimized user access
- Software Restriction Policies
 - Not allowing files/DLLs to run in AppData
 - [https://technet.microsoft.com/en-us/library/cc759648\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc759648(v=ws.10).aspx)
- Applocker
 - Similar to SRP
- EMET
 - <https://technet.microsoft.com/en-us/security/jj653751>

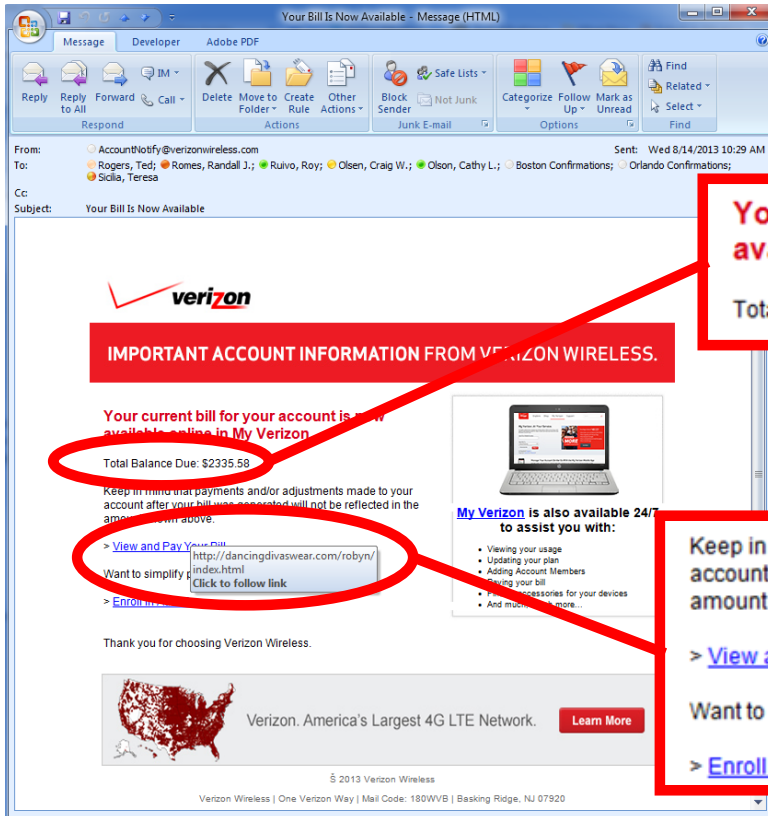


Ransomware Defensive Strategies

- Current operating systems
- Patched vulnerabilities
- Working backups are critical...



Phishing Examples



Your current bill for your account is now available online in My Verizon

Total Balance Due: \$2335.58

IMPORTANT ACCOUNT INFORMATION FROM VERIZON WIRELESS.

Your current bill for your account is now available online in My Verizon

Total Balance Due: \$2335.58

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> [View and Pay Your Bill](http://dancingdivaswear.com/robyn/index.html)
Want to simplify your bill payment?
Click to follow link



My Verizon is also available 24/7 to assist you with:

- Viewing your usage
- Updating your plan
- Adding Account Members
- Paying your bill
- Finding accessories for your devices
- And much more...

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> [View and Pay Your Bill](http://dancingdivaswear.com/robyn/index.html)
Want to simplify your bill payment?
Click to follow link

> [Enroll in Auto Pay](#)



Persuasion Attack – CEO Impersonation

- CEO asks the CFO...
- Common mistakes
 1. Use of private email
 2. “Don’t tell anyone”

- Safeguards

1. Never use email for sole method of authorization
2. Ensure recipient has VERBALLY validated with “source” of email for financial transactions

- <http://www.csoonline.com/article/2884339/malware-cybercrime/omahas-scoular-co-loses-17-million-after-spearphishing-attack.html>

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

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.



Persuasion Attack CEO Impersonation

Krebs on Security

In-depth security news and investigation

- <https://krebsonsecurity.com/tag/bec/>

18 Firm Sues Cyber Insurer Over \$480K

JAN 18

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 not speak with anyone by email or phone regarding this. Regards, Gean Stalcup."





We promise
to *know you* and *help you.*

**Lessons Learned
When I Hacked a**

(you fill in the blank)

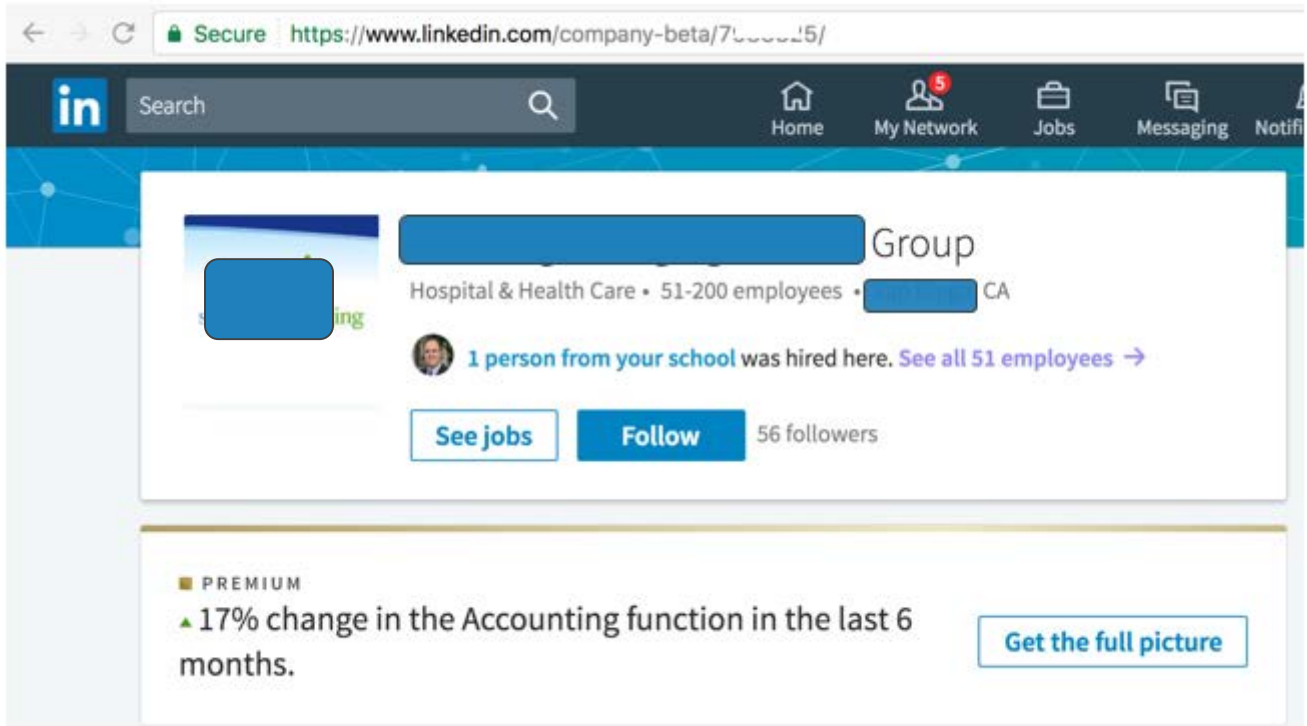
Attacking a Credit Union

Performing Reconnaissance

- Who's who in the company?
- Gather email addresses
- Understand what services are exposed to the Internet
 - Webmail
 - VPN
 - PACS



Attacking a Credit Union



The screenshot shows a LinkedIn company page for a "Hospital & Health Care" organization with 51-200 employees. The page includes a search bar, navigation icons for Home, My Network (with a notification badge), Jobs, Messaging, and Notifications. The main content area features a blue header with the company name, a profile picture placeholder, and a description: "Hospital & Health Care • 51-200 employees • [redacted] CA". Below this, it states "1 person from your school was hired here. See all 51 employees →". There are two buttons: "See jobs" and "Follow", with "56 followers" listed next to the "Follow" button. A "PREMIUM" badge is visible, along with a statistic: "▲ 17% change in the Accounting function in the last 6 months." and a button labeled "Get the full picture".



Attacking a Credit Union

Showing 428 results



William Murray, CPA • 2nd

Principal at CliftonLarsonAllen
Cedar Rapids, Iowa Area

Current: ...CliftonLarsonAllen (CLA... cliftonlarsonallen.com.



18 shared connections

Connect



Alex Hengel • 2nd

CPA, Senior at CliftonLarsonAllen
St. Cloud, Minnesota Area

Current: Senior at CliftonLarsonAllen



11 shared connections

Connect



Bill Vincent, CPA • 2nd

Principal at CliftonLarsonAllen LLP
Cedar Rapids, Iowa Area

Current: Principal, CPA at CliftonLarsonAllen



6 shared connections

Connect



Jo Eyberg, CPA • 2nd

Partner - Tax at CliftonLarsonAllen
St. Joseph, Missouri Area

Current: CliftonLarsonAllen is... www.cliftonlarsonallen.com.



3 shared connections

Connect



Robert Bollig, CPA • 2nd

Tax Manager at CliftonLarsonAllen, LLP
La Crosse, Wisconsin Area

Current: CliftonLarsonAllen is... www.cliftonlarsonallen.com.



13 shared connections

Connect

Job results for cliftonlarsonallen.com 659 results

See all



We promise to know you and help you.

Attacking a Credit Union

Let's Go Phishing

- Determine what you want
 - Remote access program
 - Credential harvesting
- Impersonate an internal employee
 - Most SPAM filters don't block this by default
 - Much higher success rate



Attacking a Credit Union

From: Ed [REDACTED]
To: Anderson, David J
Cc:
Subject: Webmail upgrade

We have performed an upgrade to our mail system and are looking at updating access to webmail. We need users to log into the webmail portal in order to activate their account. Once you log in, you should receive a message that your email account has "been confirmed." If you get this message, the upgrade worked. If you receive an error, please let IT know and we will look into the issue.

Webmail site: [https://\[REDACTED\]/owa](https://[REDACTED]/owa)

Thanks,
Ed



Attacking a Credit Union



Microsoft®
Outlook Web App

Exchange Email Account Update

This is a public or shared computer
 This is a private computer

Domain\user name:

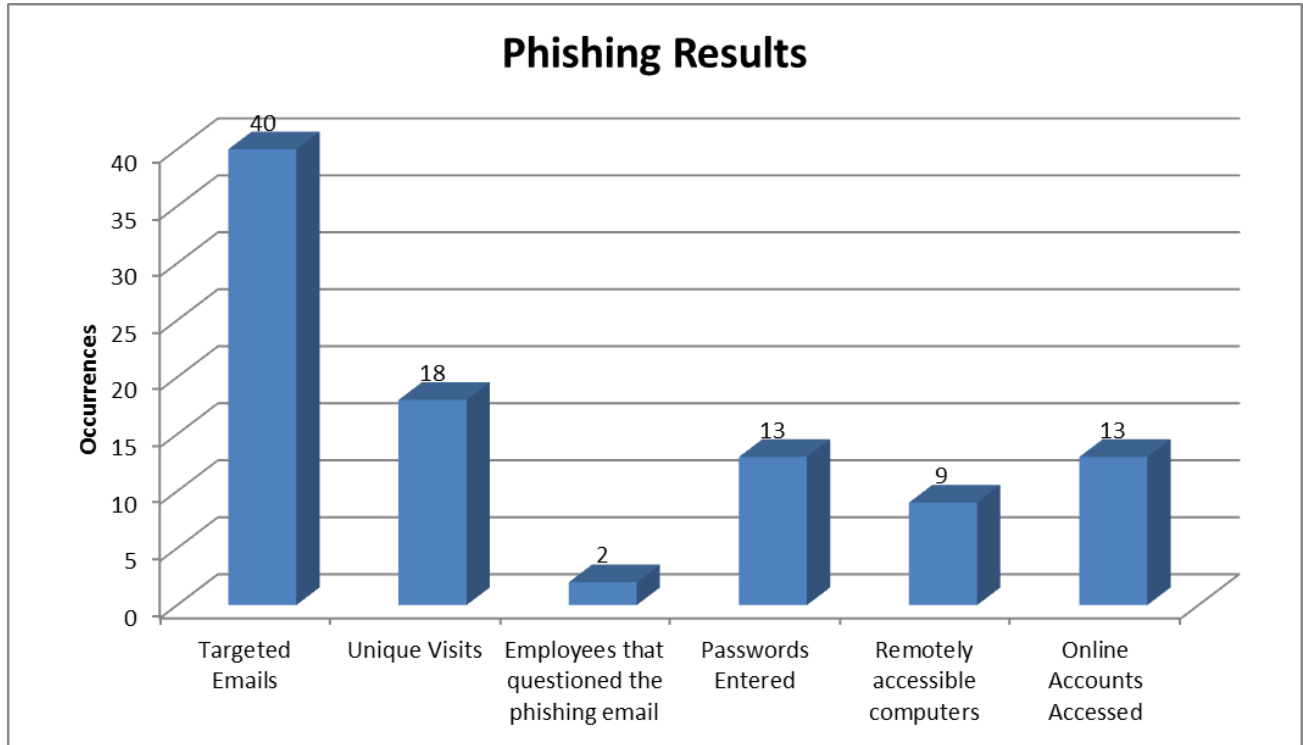
Password:

Sign in

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.



Attacking a Credit Union



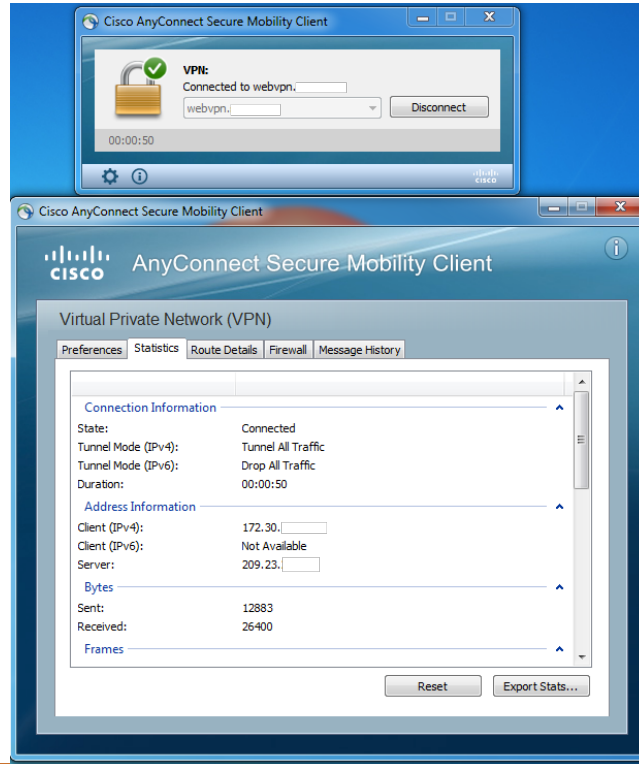
We promise to know you and help you.

What Does The Internet Perimeter Look Like (The Attack Surface)

- Externally Exposed Services
 - Webmail
 - VPN
 - Helpdesk Portal
 - VMware Desktop
 - Clinical Studio
 - Lexmark Diagnostic Viewer
 - Merge PACS



Attacking a



We Are Inside – Now What Do We Do

Internal network access... now what?

- Find sensitive information
 - Most employees have direct access to sensitive info
 - File shares and applications that are too open
- Elevate privileges
 - Often find administrative privilege issues
 - Abuse weak password policies

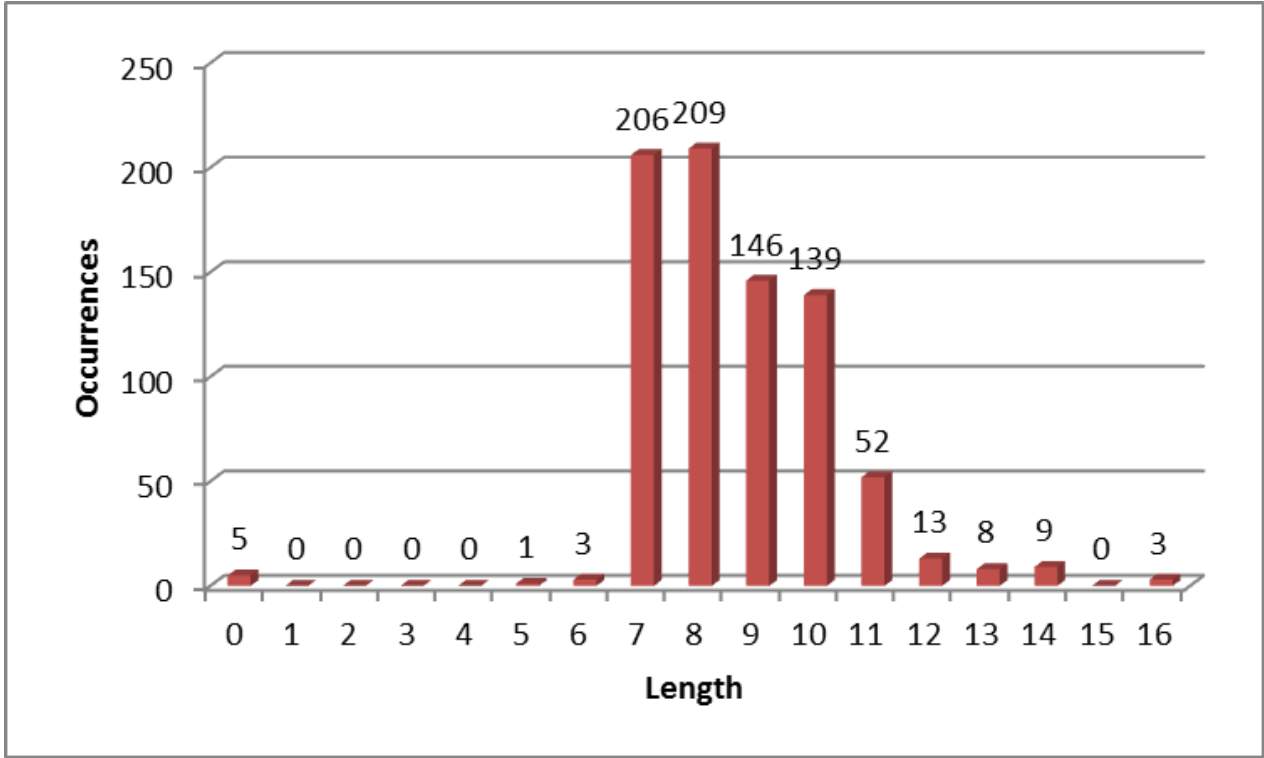


Password Cracking (I mean auditing...)

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



Password Cracking (I mean auditing...)



We promise to know you and help you.



We promise
to *know you* and *help you.*

Strategies & Action Items

**How Can Organizations
Protect Themselves**

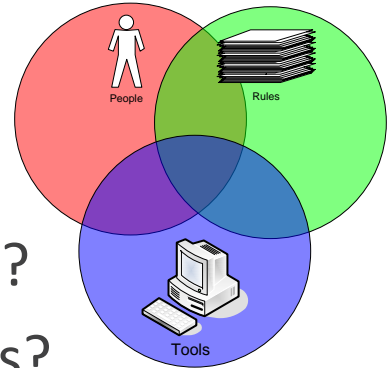
Strategies

Our information security strategy should have the following objectives:

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



Policies



- People, Rules and Tools
 - What do we expect to occur?
 - How do we conduct business?
- Standards Based, Disciplined, Change Management, operating from a Governance or Compliance framework:
 - FFIEC/GLBA
 - CIS Critical Controls
 - PCI – DSS

CIS (SANS) Critical Controls

First 5 CIS Controls

Eliminate the vast majority of your organisation's vulnerabilities

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

All 20 CIS Controls

Secure your entire organization against today's most pervasive threats

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

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



We promise to know you and help you.

Defined Standards

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

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

CSC 3: Secure Configurations for Hardware and Software				
Family	CSC	Control Description	Foundational	Advanced
System	3.1	Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.	Y	
System	3.2	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.	Y	



Defined Standards

- Secure Standard Builds
- Hardening Checklists



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



Operational Discipline

- Disciplined Change Management
- Consistent Exception Control & Documentation
 - Should include risk evaluation and acceptance of risk
 - Risk mitigation strategies
 - Expiration and re-analysis of risk acceptance



Vulnerability and Patch Management Standards

- Define your standard
 - How soon should critical updates be applied???
 - TWO Answers...
- Manage to your standard
- Document and manage your exceptions

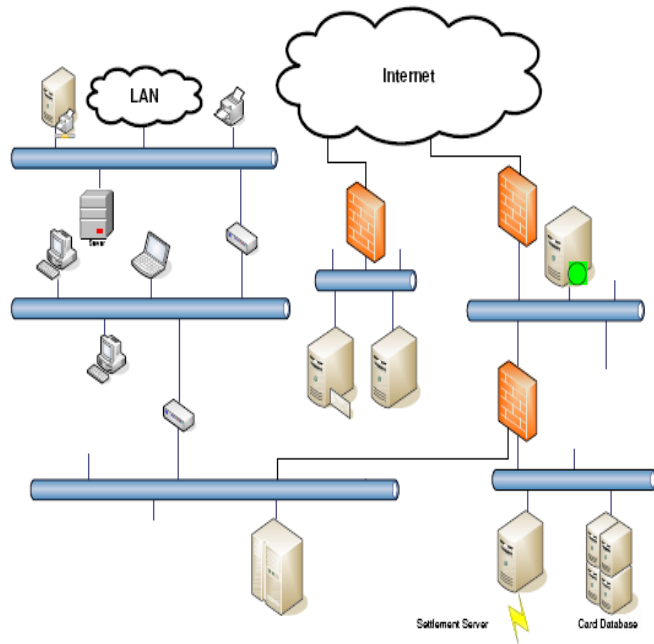


Know Your Network

Know What “Normal” Looks Like

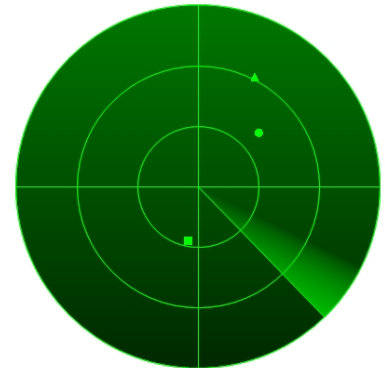
Alignment of centralized audit logging, analysis, and automated alerting capabilities (SIEM) & DLP

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



System and Vulnerability Management and Monitoring

- Monitoring
 - System logs and application “functions”
 - Accounts
 - Key system configurations
 - Critical data systems/files
- Scanning
 - Patch Tuesday and vulnerability scanning
 - Rogue devices



Protect Against Email Phishing

- Harden email gateway (spam filter)
 - Block potentially malicious file attachments (e.g. ZIP, RAR, HTA, JAR)
 - Flag Office documents that contain Macros as suspicious
 - Prevent your organization’s domain from being spoofed
 - ◇ Sender Policy Framework (SPF)
 - ◇ Custom rule to evaluate SMTP Letter FROM field
 - Flag emails that originate from the Internet
 - ◇ E.g. Modify subject line to say ‘External’



Protect Against Email Phishing

- Continue to Train Employees and Members
 - Train employees how to spot odd wire requests
 - ◇ Politely challenge the request and ask if it has been verified through proper channels (NOT email)
 - Provide educational material and training to business members
 - ◇ Provide sample policies/guidelines for organizations that don't have them
 - ◇ Hold events for business members that discuss cyber security
 - ◇ Explain simple controls to implement (limits, two-step/two-factor, etc.)
 - ◇ Make sure request is not authorized via email



Action Items

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



Action Items

- Test backup systems
 - Periodically test backup systems to ensure you can recover from ransomware
 - Have IT perform a full, bare-metal recovery of main file share
 - Have IT document how long it takes to recover various files or systems
 - PRACTICE...



Action Items

- Audit systems for default/weak passwords
 - Most systems have default passwords and they are all documented online
 - Don't overlook “simple” systems
 - ◇ E.g. Printers, IP cameras, etc.



Action Items

- Validate that your expectations are being met for cybersecurity
 - Penetration Testing
 - ◇ Informed/White Box
 - ◇ Uninformed/Black Box
 - Social Engineering Testing
 - True Breach Simulation
 - ◇ Red Team/Blue Team



Questions?





Thank you!

**Randy Romes, CISSP, CRISC, MCP, PCI-QSA
Principal, Information Security,
Direct: 612-397-3114
Randy.Romes@claconnect.com**