



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

©2018 CliftonLarsonAllen LLP



**The Intersection of Data Analytics, Automated Controls, and Fraud
Prevention & Detection**

By: Andrew Laflin

Learning Objectives

- Identify key internal controls over significant transaction processes, specifically around revenues/receipts and expenses/disbursements
- Discern between manual controls and automated controls
- Understand how data analytics can be used to automate reconciliation processes and assist in identifying anomalies to investigate further



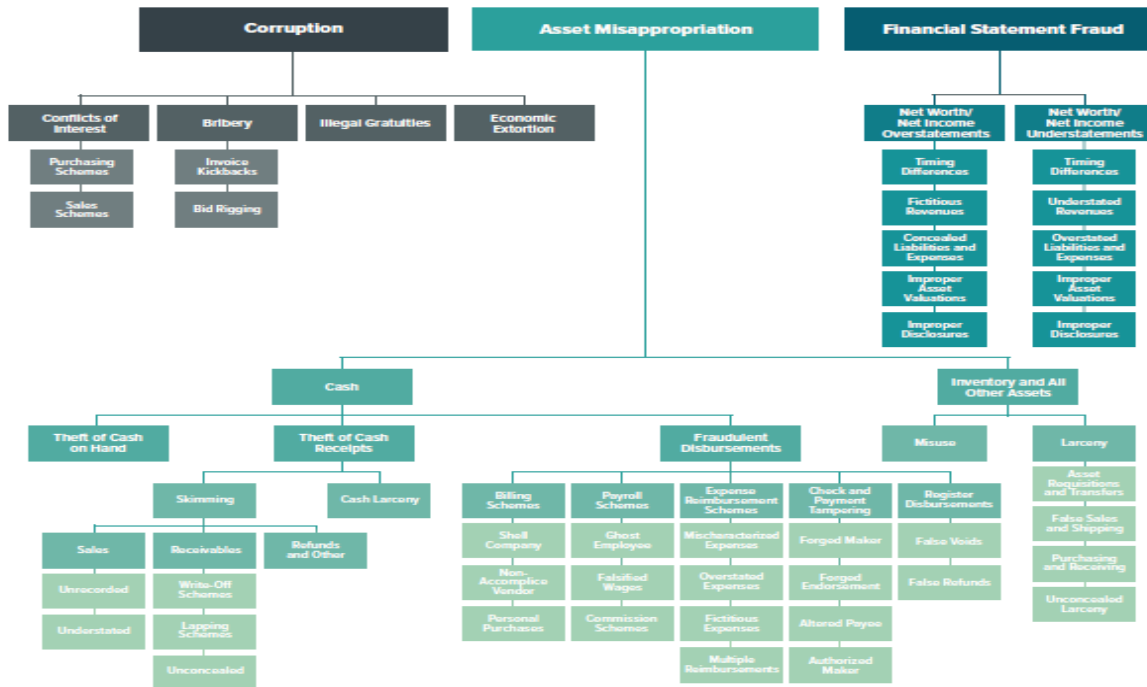
Types of Occupational Fraud - Definitions

- Occupational Fraud can be broken down into three main categories:
 - *Corruption* schemes, in which an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit (e.g., schemes involving bribery or conflicts of interest)
 - *Financial statement fraud* schemes, in which an employee intentionally causes a misstatement or omission of material information in the organization's financial reports (e.g., recording fictitious revenues, understating reported expenses or artificially inflating reported assets)
 - *Asset misappropriation* schemes, in which an employee steals or misuses the organization's resources (e.g., theft of company cash, false billing schemes or inflated expense reports)



Occupational Fraud Tree

FIG. 4 Occupational Fraud and Abuse Classification System (the Fraud Tree)⁶



Occupational Fraud by Category - Frequency



We promise to know you and help you.

Who Commits Fraud (All Industries)?

- Male or female?
- Over 40 or under 40?
- Employees, managers, or executives?
- What was the most common position held by the fraudster?
- High school graduate and some college, bachelor's degree, or post-graduate degree?



Multiple Choice Question #1

- Who perpetrated fraud more frequently, according to the 2018 ACFE Report to the Nations?
 - A. Males
 - B. Females

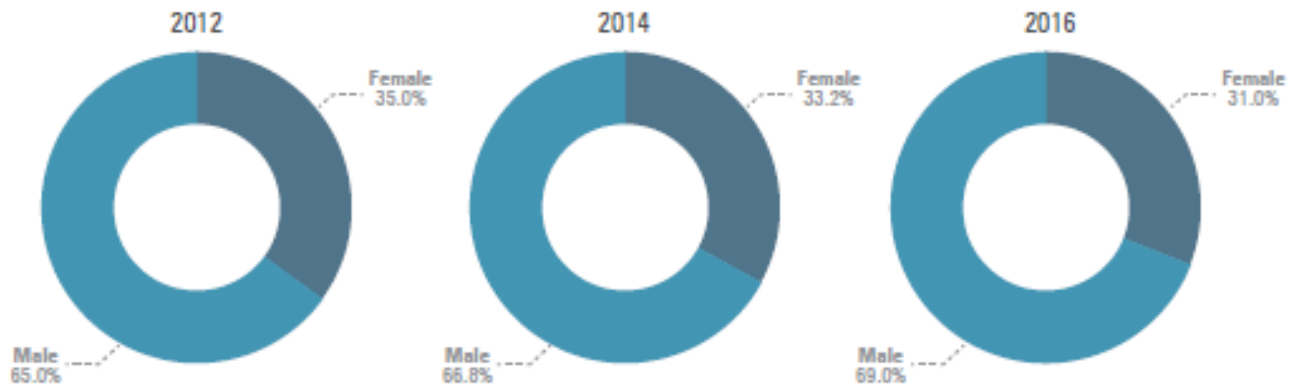


Answer: Perpetrator's Gender



Perpetrator's Gender

Figure 79: Gender of Perpetrator—Frequency



Who Commits Fraud (All Industries)?

- ~~Male or female?~~
- Over 40 or under 40?
- Employees, managers, or executives?
- What was the most common position held by the fraudster?
- High school graduate and some college, bachelor's degree, or post-graduate degree?



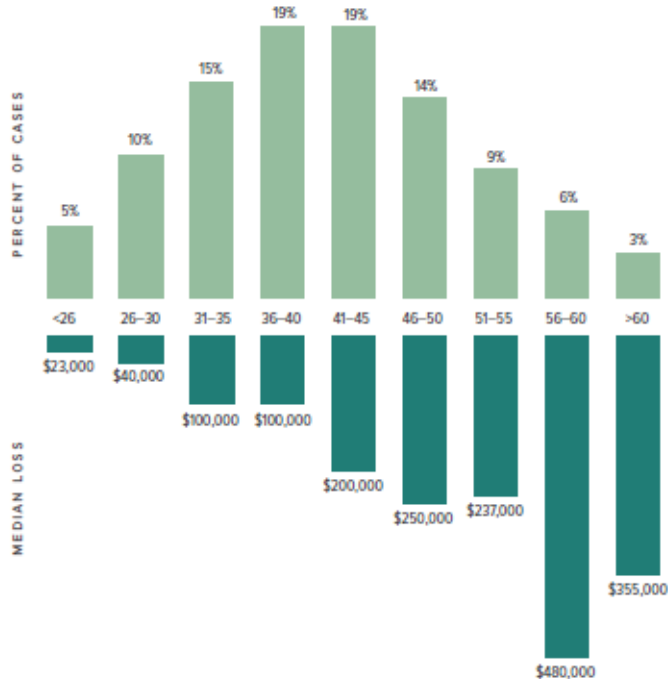
Multiple Choice Question #2

- Who perpetrated fraud more frequently, according to the 2018 ACFE Report to the Nations?
 - A. <26
 - B. 36-40
 - C. 41-45
 - D. 46-50
 - E. >65



Perpetrator's Age – Frequency & Median Loss

FIG. 33 How does the perpetrator's age relate to occupational fraud?



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

Who Commits Fraud (All Industries)?

- ~~Male or female?~~
- ~~Over 40 or under 40?~~
- Employees, managers, or executives?
- What was the most common position held by the fraudster?



Multiple Choice Question #3

- Who perpetrated fraud more frequently, according to the 2018 ACFE Report to the Nations?
 - A. Employees
 - B. Managers
 - C. Owners



Perpetrator's Position – Frequency & Median Loss

FIG. 32 How does gender distribution and median loss vary based on the perpetrator's level of authority?



Who Commits Fraud (All Industries)?

- ~~Male or female?~~
- ~~Over 40 or under 40?~~
- ~~Employees, managers, or executives?~~
- What was the most common position held by the fraudster?



Multiple Choice Question #4

- What was the most common position of the fraudster, according to the 2018 ACFE Report to the Nations?
 - A. Accounting
 - B. IT
 - C. HR
 - E. Operations
 - F. Purchasing



Fraud by Position

Department*	Percent of cases	Median loss
Accounting	14%	\$ 212,000
Operations	14%	\$ 88,000
Sales	12%	\$ 90,000
Executive/upper management	11%	\$ 729,000
Customer service	8%	\$ 26,000
Administrative support	8%	\$ 91,000
Other	6%	\$ 77,000
Finance	6%	\$ 156,000
Purchasing	5%	\$ 163,000
Facilities and maintenance	3%	\$ 175,000
Warehousing/inventory	3%	\$ 200,000
Information technology	3%	\$ 225,000
Marketing/public relations	2%	\$ 80,000
Manufacturing and production	2%	\$ 200,000
Human resources	1%	\$ 76,000

*Departments with fewer than ten cases were omitted.



Fraud Detection

**Figure 23: Detection Method by Region—
United States**

Detection Method	Percent of Cases
Tip	37.0%
Management Review	14.3%
Internal Audit	14.1%
By Accident	7.2%
Account Reconciliation	6.1%
Other	5.5%
Document Examination	4.8%
External Audit	4.0%
Notified by Law Enforcement	2.5%
Surveillance/Monitoring	1.9%
IT Controls	1.5%
Confession	1.2%



Prevalence in Local Government

FIG. 12 What types of organizations are victimized by occupational fraud?



FIG. 13 What levels of government are victimized by occupational fraud?



*Dollar amounts are median loss.



We promise to know you and help you.

Case Study #1A – Payroll Manual Process

- Personnel Action Forms (PAFs) are manually completed by the employee, signed by his/her supervisor and hand-delivered to HR/Benefits Department, who enters the updates into the payroll system
- Finance & Payroll employees also have access to make pay rate and other status changes as a backup when necessary



Case Study #1A – Payroll Manual Process

- Manual timesheets are prepared by all hourly employees and approved by applicable supervisors. Vacation leave forms are also prepared by all employees (both exempt and non-exempt) and contain supervisory review and approval
- Timesheets and leave slips are hand delivered to Finance where payroll technicians enter the information into the payroll system



Case Study 1A – Payroll Manual Process

- When all necessary information is entered for a given pay period, payroll is processed by the Payroll Analyst, and a pay register is printed and provided to the Payroll Manager, who physically signs the pay register, authorizing its release
- Payroll entries are then posted by the Payroll Analyst, and employees are paid by either direct deposit or manual check



Case Study #1B – Payroll Automated Process

- All employee status changes are initiated by the employee through the HR module of the entity's ERP system and submitted by HR team member; pay rate changes also approved by supervisor via workflow before submission
- Each pay period, HR module interfaces with Payroll/Financial module; exception report is generated and reviewed by Payroll and HR/Benefits team members



Case Study #1B – Payroll Automated Process

- Hourly employees enter their time and all employees enter PTO hours in electronic timekeeping system, which automatically interfaces with Payroll Module of ERP system
- Timekeeping system will not allow an employee's pay to be processed unless it is approved electronically by designated reviewer; Payroll Manager acknowledged that payroll technician will review and approve time as a last resort and will obtain documentation of approval (i.e. email from reviewer) after the fact



Case Study #1B – Payroll Automated Process

- Payroll Dept. runs a report comparing hours by employee per timekeeping system to hours by employee per Payroll Module for each pay group and signs off electronically within a step in the Payroll Module that the reconciliation has been performed with no outstanding exceptions
- Payroll processing is an entirely automated process, including generating a self-balancing journal entry to post into the system and sending a notification of any errors that may be encountered during payroll processing



Case Study #1 – Payroll Disbursements

- Any weaknesses in internal controls in Scenario 1A or 1B?
- Would the auditor test controls differently under Scenario 1A versus 1B?
- Any payroll and benefits reconciliations or verification procedures currently being performed at your local government entity that are time-consuming or ineffective? Or are not being performed but should be?



Case Study #2A – P-Card Manual Process

- Cardholders print monthly statement and staple receipts to statements and fill out approval form (collectively “cardholder package”)
- Each cardholder package hand delivered to department director who signs off on approval form
- Each department routes all cardholder packages for all employees in the department (including directors) to Finance to enter transactions in the accounting system



Case Study #2B – P-Card Automated Process

- Cardholders have access to bank's P-card application to verify all purchase transactions
- Payment Request Form submitted electronically with cardholders' monthly scanned statements, receipts, etc. to Approving Official for review and signature of approval
- A/P Processing team receives paperwork and verifies transactions in bank's p-card application and performs second review of Payment Request Form and supporting documentation
- P-card application file imported automatically into accounting system every 15 minutes



Case Study #2 – P-card Disbursements

- Any weaknesses in internal controls in Scenario 2A or 2B?
- Would the auditor test controls differently under Scenario 2A versus 2B?
- Any p-card reconciliations or verification procedures currently being performed at your local government entity that are time-consuming or ineffective? Or are not being performed but should be?



Case Study #3A – Customer Credits & Adjustments Manual Process

- All staff within the department have the ability to make an adjustment to a customer balance when necessary
- When the need arises, employee will make adjustment within the system and print the screen showing the adjustment and attach explanation and other relevant backup to support the reason for the adjustment
- The documentation is placed in the supervisor's bin for review and approval (evidenced by initials and date) and kept in a folder in accordance with entity's document retention policy



Case Study #3B – Customer Credits & Adjustments Automated Process

- Only authorized individuals can initiate adjustments within the system; supervisory personnel have authorization to approve adjustments but cannot initiate
- An adjustment will not be formally entered into the system until the initiation and review process are completed via workflow
- Memo field must be completed with explanation of adjustment before initiation process can be completed; system also allows for attachments to be added if other backup documentation is needed



Case Study #3 – Recording Customer Adjustments

- Any weaknesses in internal controls in Scenario 3A or 3B?
- Would the auditor test controls differently under Scenario 3A versus 3B?
- Any void, refund, adjustment transaction reconciliations or verification procedures currently being performed at your local government entity that are time-consuming or ineffective? Or are not being performed but should be?



CLA Outsourced Services – Data Analysis

- CLA's data analytics tools that can simplify periodic (daily, weekly, monthly, quarterly, annually) reconciliation procedures
- Traditional practice has been to utilize pivot tables and other macros in Excel to combine, disaggregate, and reconcile data
- The larger the data set and more complex the objectives of the reconciliation, the more complicated and time-consuming the exercise can be
- Looking for more efficient ways to streamline your reconciliation process without the need for excessive file manipulation and obtain results in a hurry? CLA can help using sophisticated data analytics tools.



CLA Outsourced Services - Interim and Project Roles

- Gov't can't or doesn't need to hire permanent role right away
- Will take a while to hire the permanent employee
- Can be for full-time on-site for several months or years



Personnel change

Maternity leave or other medical leave
Terminated or sudden exit of employee
Succession planning

Peak Workload

Monthly or quarterly financial close
Year-end assistance
Audit and/or budget preparation



Other major changes

New capital projects
System implementation



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
 - NIST, PCI-DSS, CJIS, etc...
- Incident response and forensics
- Security awareness training
- Independent security consulting
- Internal audit support

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

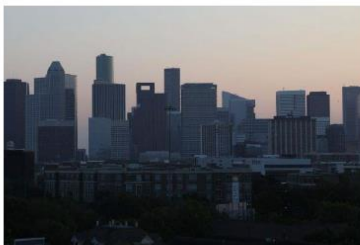


Cybersecurity Protection

POLITICS | NATIONAL SECURITY

More U.S. Cities Brace for 'Inevitable' Hackers

Majority of top 25 U.S. cities have, or are looking to buy, cybersecurity insurance



Houston has three \$10 million cyberinsurance policies from different insurers. PHOTO: LOREN ELLIOTT/GETTY IMAGES

By Scott Calvert and Jon Kamp

Updated Sept. 4, 2018 5:20 p.m. ET

Hackers are constantly probing for "the one flaw overlooked" in Houston's computer networks, the official responsible for safeguarding the fourth-largest U.S. city's system said.

"Compromise is inevitable," said Christopher Mitchell, chief information security official, at a Houston City Council hearing last month. His presentation helped persuade local lawmakers they needed a \$30 million cybersecurity insurance plan with a \$471,400 premium, an example of a burgeoning trend across the country. Policies vary, but

Multiple Choice Question #5

- What is a typical County Sheriff's response when faced with threats from criminals in a hostage situation?
 - A. We don't ever negotiate with terrorists! Never. Never. Never.
 - B. We'll give them what they want if they ask nicely.
 - C. We will give in to their demands if there are no other options available.



Is This The Right Answer?





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

Any Questions?

Thank you for your participation.



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

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

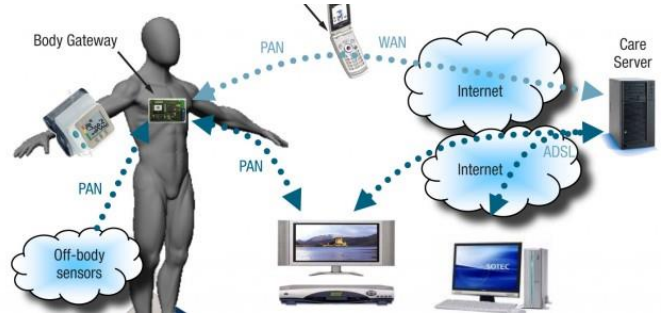
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC,
an SEC-registered investment advisor

©2018 CliftonLarsonAllen LLP



Today's Cybersecurity Risks

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

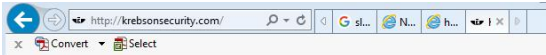


We promise to know you and help you.

Everything Can Talk to Everything....

- My product or system can talk to yours!
- They all have...
- How do we manage that???

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.



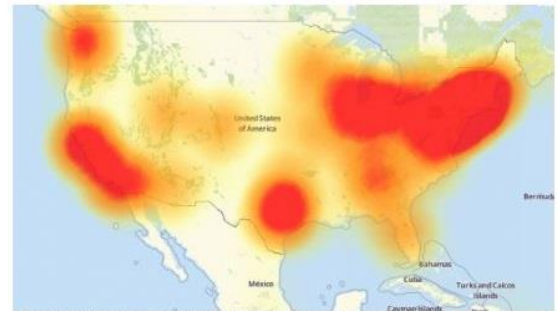
Recently, I heard from a cybersecurity researcher who'd created a virtual “honeypot” environment designed to simulate hackable IoT devices. The source, who asked to remain anonymous, said his honeypot soon began seeing traffic destined for **Asus and Linksys** routers running default credentials. When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



We promise to know you and help you.



We promise
to know you and help you.

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

Multiple Choice Question #6

- Of the ten ways to lose everything, which is the most prevalent cause?
 - A. Users clicking links
 - B. Users not changing their passwords more frequently
 - C. Users letting the pizza delivery guy in the server room within their office building (but he's not really the pizza delivery guy)



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](#)



We promise *to know you and help you.*

10 Ways to Lose EVERYTHING

2. Users clicking links

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



We promise to *know you and help you.*

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 [redacted]

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.



We promise to know you and help you.

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](#)



We promise to know you and help you.

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



We promise to know you and help you.

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/>



We promise to *know you and help you.*

10 Ways to Lose EVERYTHING

10. Users opening attachments

Dennis Johnson <dennis_@gmail.com>

to 

Hi,

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

Thanks,

Dennis Johnson



We promise to know you and help you.



We promise
to know you and help you.

Current State of Cybercrime

How to Manage your Cybersecurity Program

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
 - Theft of Credentials & Account take overs
 - Ransomware and Interference w/ Operations



Payment Fraud

- Most people perform payments 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



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/>



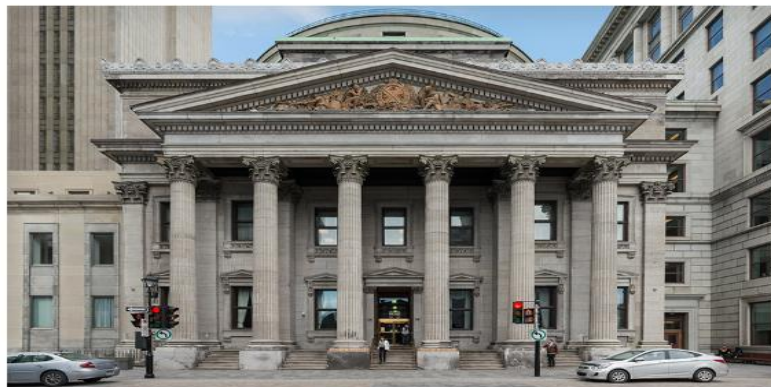
We promise to know you and help you.

Ransomware

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](#)).



We promise to know you and help you.

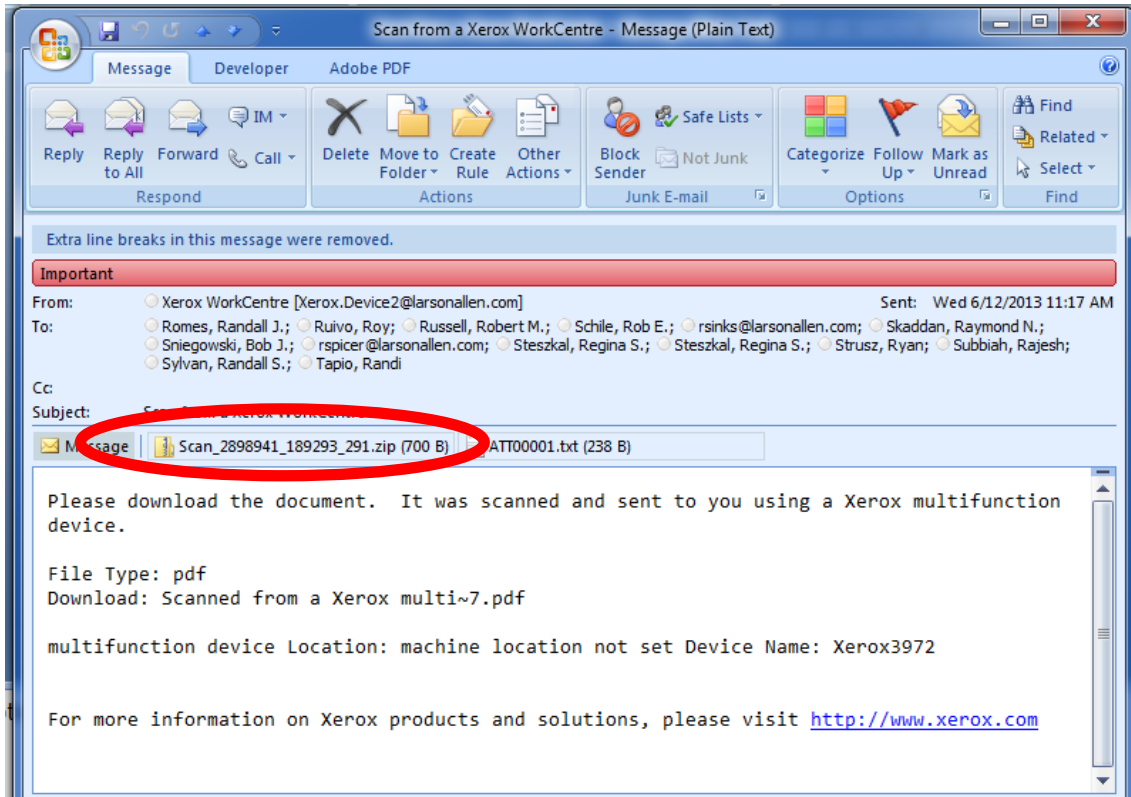
Ransomware



- 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)

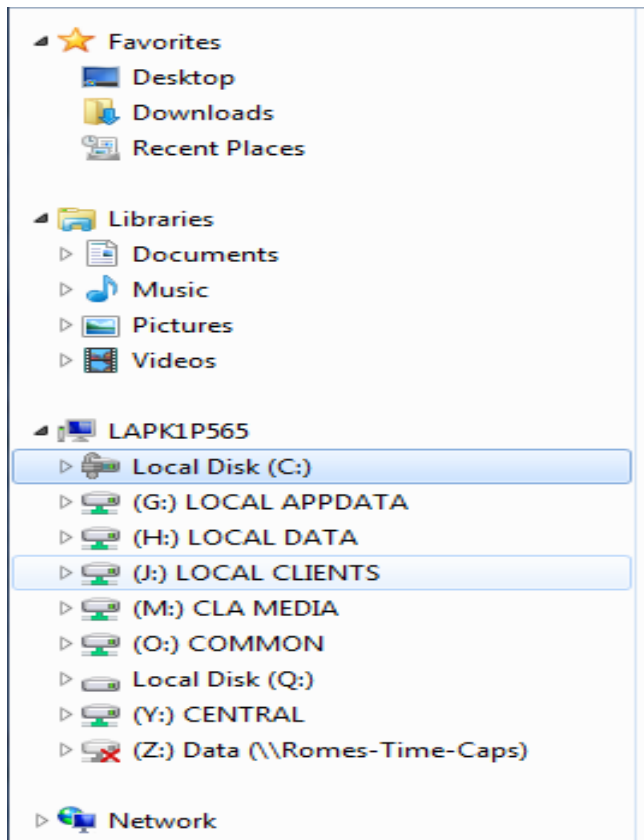


Ransomware



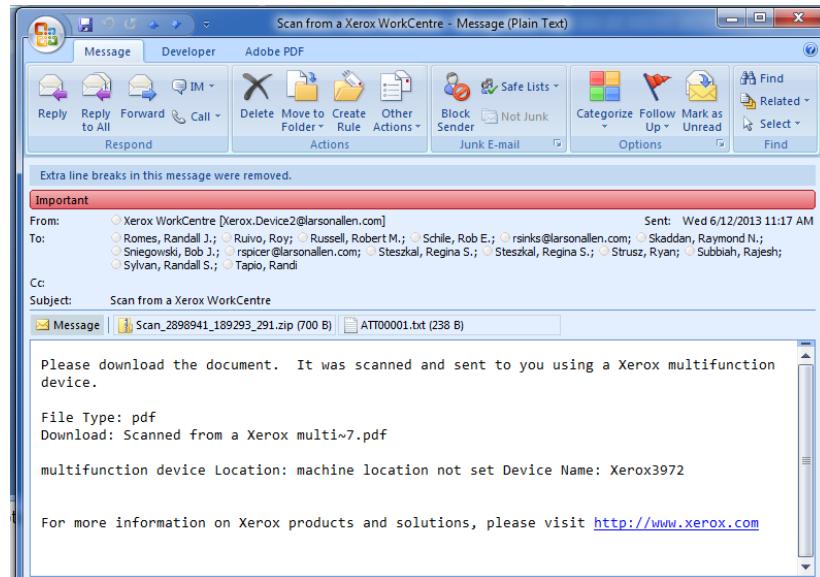
Ransomware

- Malware encrypts everything it can interact with



Ransomware Defensive Strategies

- Filtering capabilities
- Users that are aware and savvy



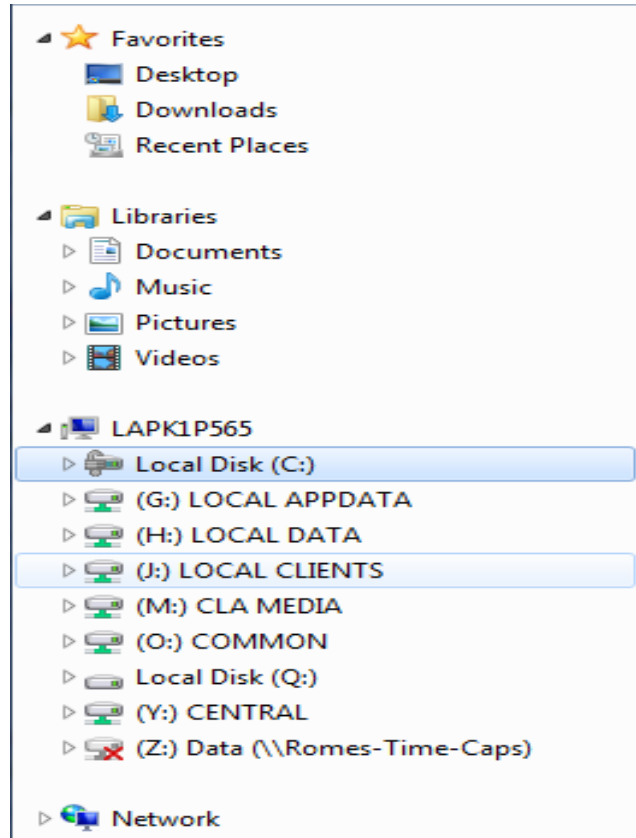
Ransomware Defensive Strategies

- Minimized user access
- Software Restriction Policies
 - Not allowing files/DLLs to run in AppData
- Applocker
 - Similar to SRP
- EMET

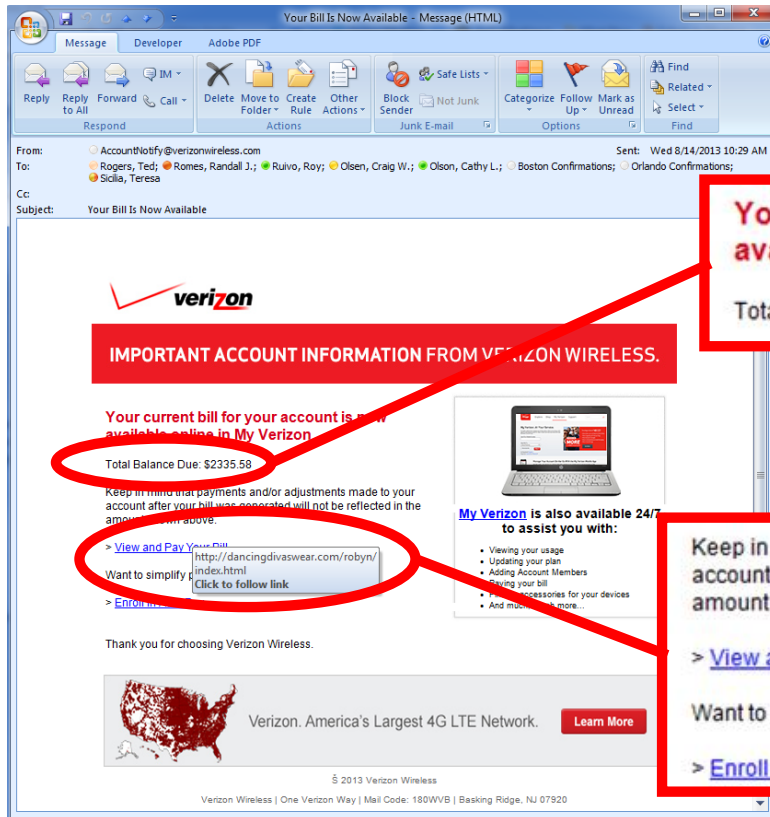


Ransomware Defensive Strategies

- 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

Thank you for choosing Verizon Wireless.



Verizon. America's Largest 4G LTE Network.

[Learn More](#)

© 2013 Verizon Wireless

Verizon Wireless | One Verizon Way | Mail Code: 180WVB | Basking Ridge, NJ 07520

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”

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.

- 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.csoononline.com/article/2884339/malware-cybercrime/omahas-scoular-co-loses-17-million-after-spearphishing-attack.html>



Persuasion Attack CEO Impersonation

KrebsonSecurity

In-depth security news and investigation

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

18 Firm Sues Cyber Insurer Over \$480K

JAN 15

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.



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

**Lessons Learned
When I Hacked a**


(you fill in the blank)


Performing Reconnaissance

The screenshot shows a web browser window with the LinkedIn URL <https://www.linkedin.com/company-beta/70000015/>. The LinkedIn navigation bar is visible at the top. The main content area displays the profile of a company named "Group", which is in the "Hospital & Health Care" industry and has "51-200 employees". The location is listed as "CA". A profile picture of a person is shown next to the text "1 person from your school was hired here. See all 51 employees →". Below this, there are two buttons: "See jobs" and "Follow", followed by the text "56 followers". At the bottom, a "PREMIUM" badge is displayed next to the text "▲ 17% change in the Accounting function in the last 6 months." and a button labeled "Get the full picture".

Secure <https://www.linkedin.com/company-beta/70000015/>

in Search Home My Network Jobs Messaging Notif

 Group
Hospital & Health Care • 51-200 employees • CA

 1 person from your school was hired here. [See all 51 employees →](#)

[See jobs](#) [Follow](#) 56 followers

PREMIUM
▲ 17% change in the Accounting function in the last 6 months. [Get the full picture](#)



Performing Reconnaissance

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 (municipality)

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 (municipality)

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

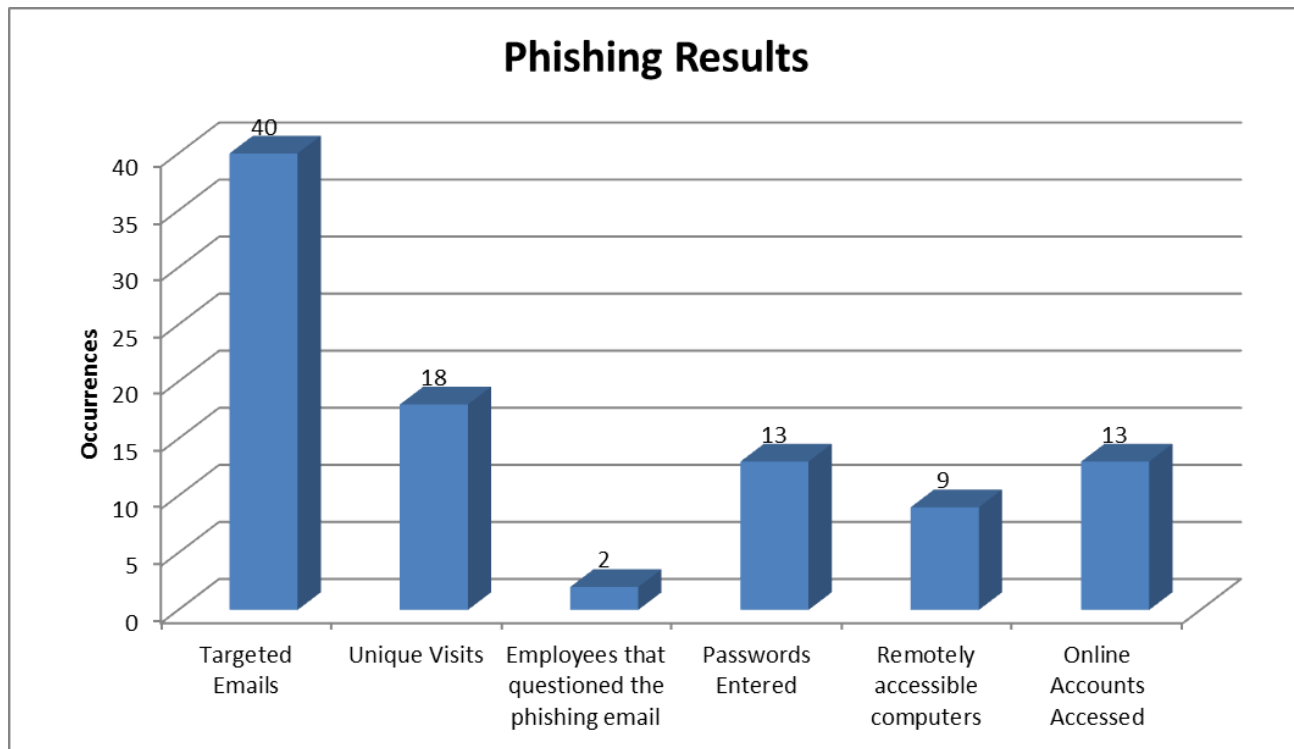
We have performed an upgrade to our mail system and are looking at updating access to webmail. We need users to log into the webmail portal in order to activate their account. Once you log in, you should receive a message that your email account has "been confirmed." If you get this message, the upgrade 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 (municipality)



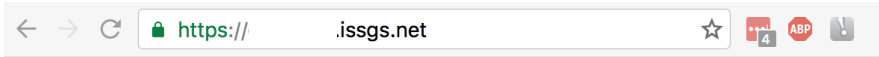
We promise to know you and help you.

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

- Externally Exposed Services
 - Webmail
 - VPN
 - Helpdesk Portal
 - VMware Desktop
 - Lexmark Diagnostic Viewer
 - Other applications exposed to the Internet



Attacking a (municipality)



Microsoft®
Outlook® Web App

Exchange Email Account Update

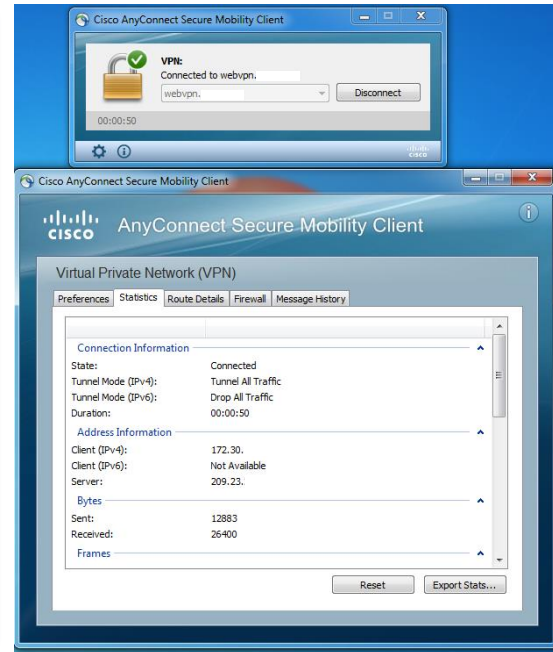
☒ This is a public or shared computer
☐ This is a private computer

Domain\user name:

Password:

Sign in

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



We promise to know you and help you.

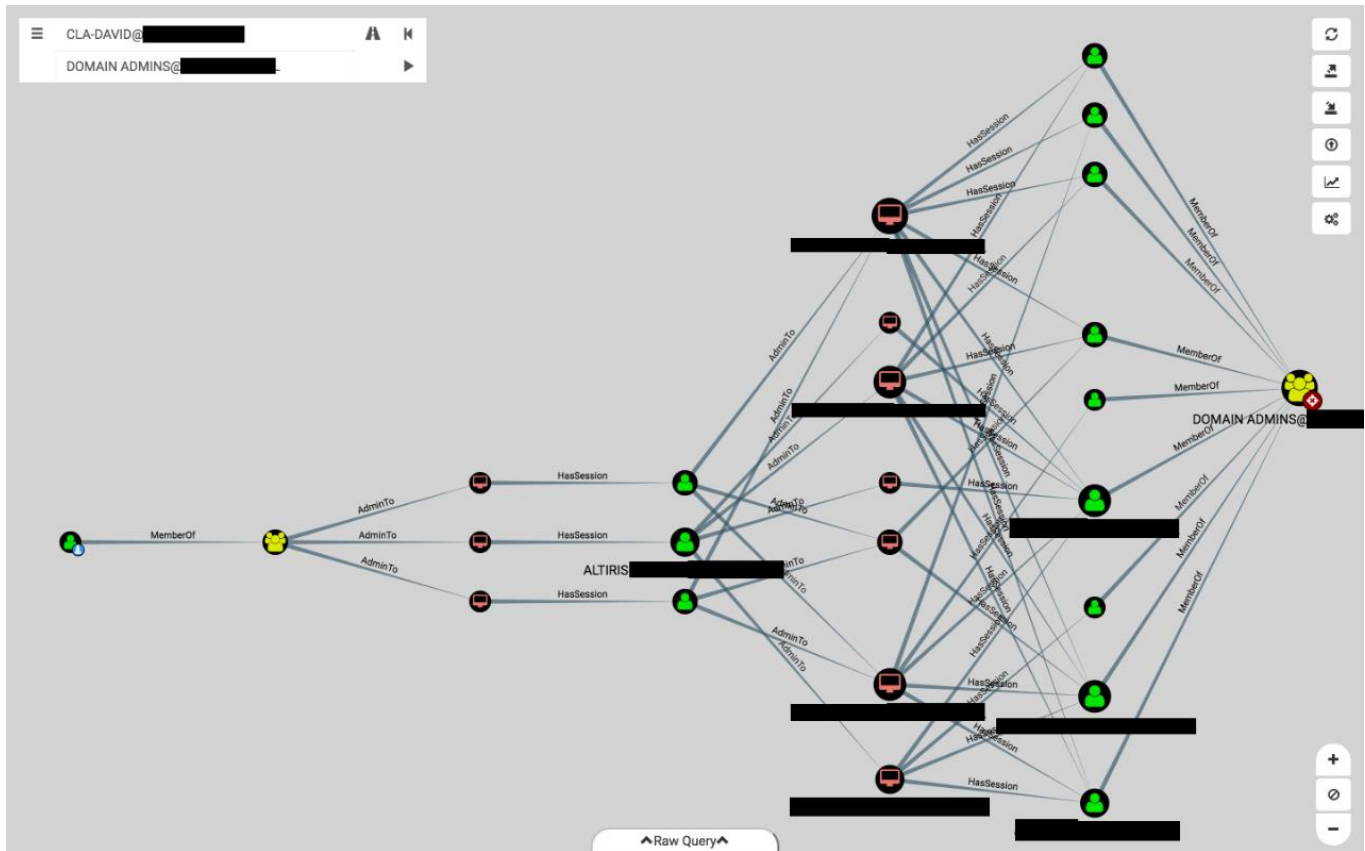
We Are Inside – Now What Do We Do

Internal network access... now what?

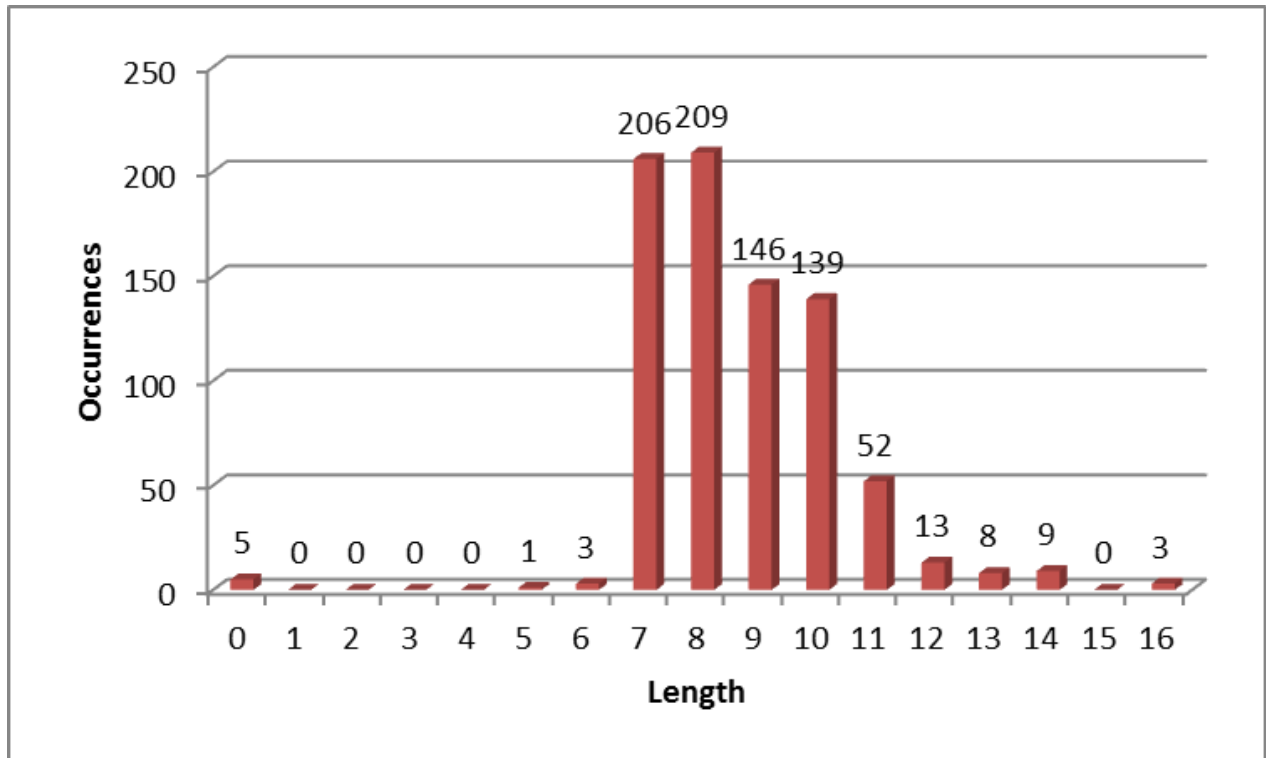
- Find sensitive information
 - Most employees have direct access to sensitive info
 - File shares and applications that are too open
- Elevate privileges
 - Often find administrative privilege issues
 - Abuse weak password policies



We Are Inside – Now What Do We Do



Password Cracking (I mean auditing...)



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





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

Strategies & Action Items

**How Can Organizations
Protect Themselves**

Strategies

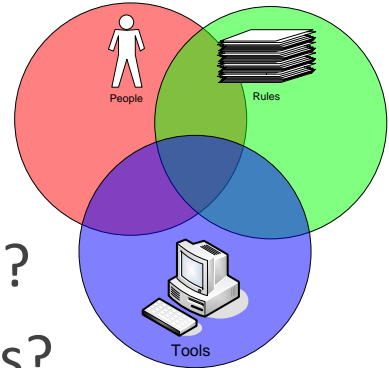
Our information security strategy should have the following objectives:

- 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:
 - NIST
 - PCI – DSS
 - CIS Critical Controls



PCI DSS – “Digital Dozen”

• PCI – DSS version 3.2

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel





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/>



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

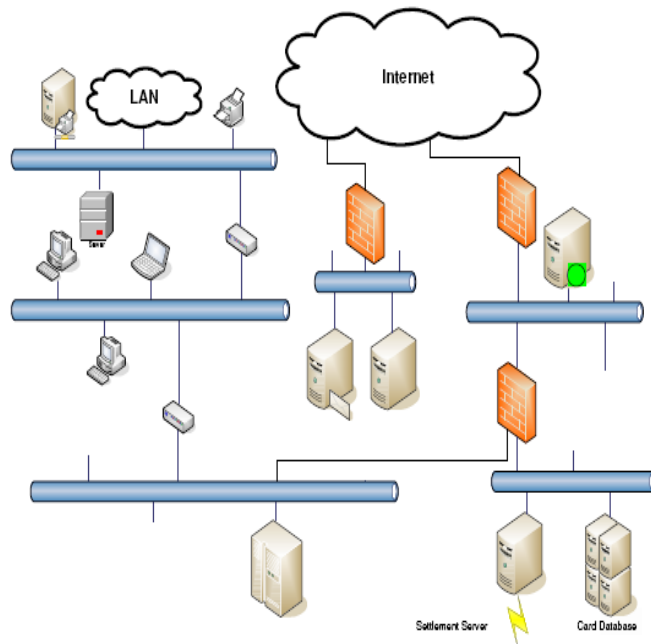


Know Your Network

Know What “Normal” Looks Like

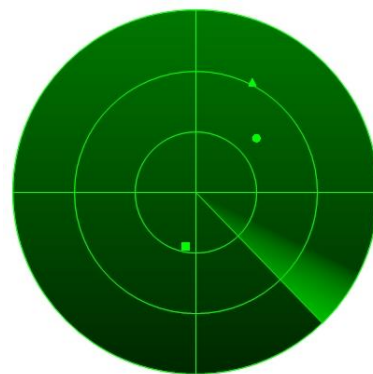
Alignment of centralized audit logging, analysis, and automated alerting capabilities (SIEM) & DLP

- 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 system 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
- 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

- 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**

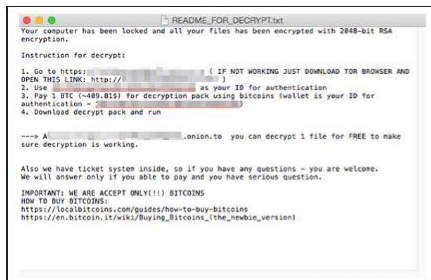


Action Items

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



Questions?





CLAconnect.com

©2018 CliftonLarsonAllen LLP

Thank you!

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



[linkedin.com/company/
cliftonlarsonallen](https://www.linkedin.com/company/cliftonlarsonallen)



[facebook.com/
cliftonlarsonallen](https://www.facebook.com/cliftonlarsonallen)



[twitter.com/
CLAconnect](https://twitter.com/CLAconnect)



[youtube.com/
CliftonLarsonAllen](https://www.youtube.com/CliftonLarsonAllen)