Cybersecurity Risks and Trends in Religious Organizations

Tales from the Dark Side: What Do We Have That The Hackers Want To Steal?

Disclaimers

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Housekeeping

- If you are experiencing technical difficulties, please dial: **800-422-3623.**

- **Q&A session will be held at the end of the presentation.**
  - Your questions can be submitted via the **Questions Function at any time during the presentation.**

- The **PowerPoint presentation,** as well as the **webinar recording,** will be sent to you within the next 10 business days.

- For future webinar invitations, subscribe at CLAconnect.com/subscribe.

- Please complete our online survey.

About CliftonLarsonAllen

- A professional services firm with three distinct business lines
  - Wealth Advisory
  - Outsourcing
  - Audit, Tax, and Consulting
- More than 5,000 employees
- Offices coast to coast
- Over 60 years of experience serving more than 6,000 nonprofit clients

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

Speaker Introduction

- **Randy Romes**
  - Principal
  - More than 19 years of experience
  - Leader of CLA's technology and industry group providing IT audits and security assessments
  - Certifications:
    - ◊ Information Systems Security Professional (CISSP)
    - ◊ Risk and Information System Controls (CRISC) professional
    - ◊ PCI-Qualified Security Assessor (PCI-QSA)
    - ◊ Microsoft Certified Professional (MCP)

Learning Objectives

- At the end of this session, you will be able to:
  - Describe factors that lead to successful phishing attacks
  - Identify strategies that can be used to mitigate risks related to phishing, ransomware, and other costly data breaches

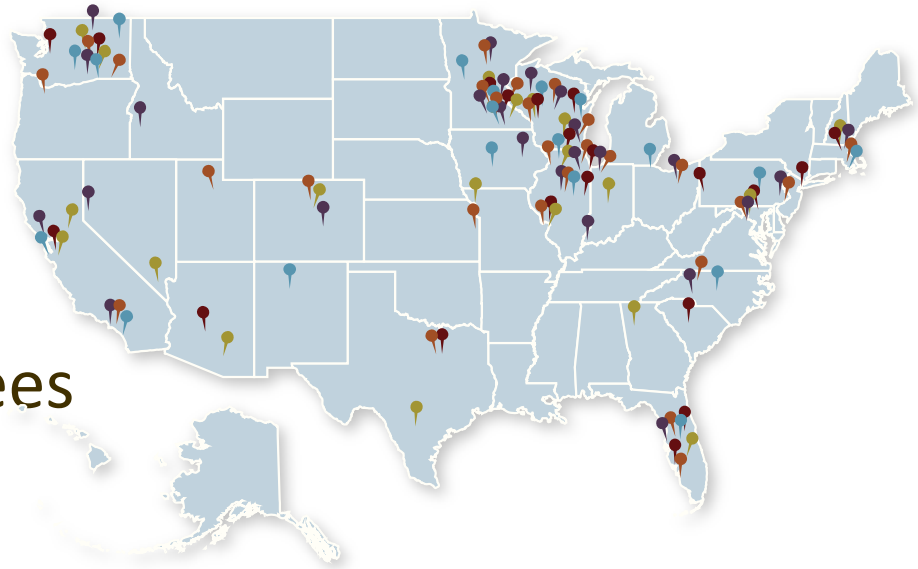
About CliftonLarsonAllen

- 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

WEALTH ADVISORY

OUTSOURCING

AUDIT, TAX, AND CONSULTING



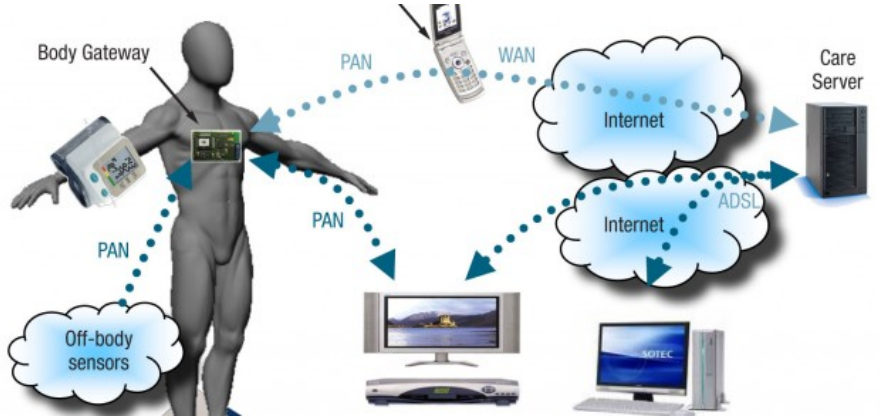
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.

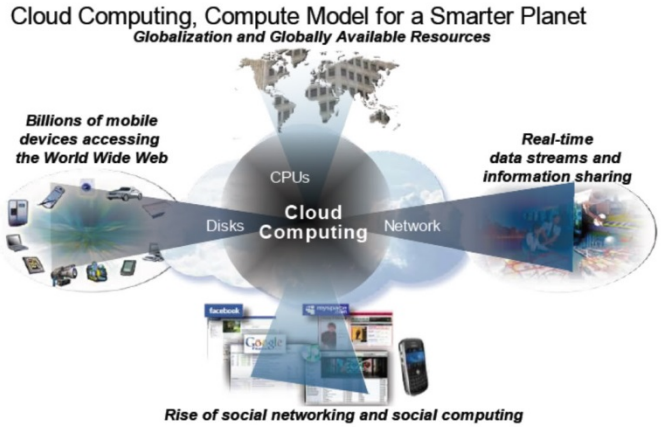
Information Security Services

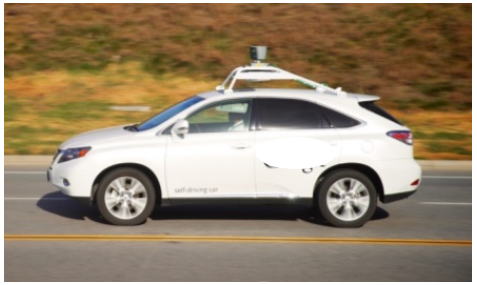
Information Security offered as specialized service for over 20 years

- Penetration Testing and Vulnerability Assessment
- IT/Cyber security risk assessments
- IT audit and compliance (NIST, PCI-DSS, GLBA, 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…







Echo dot

Add Alexa to a room

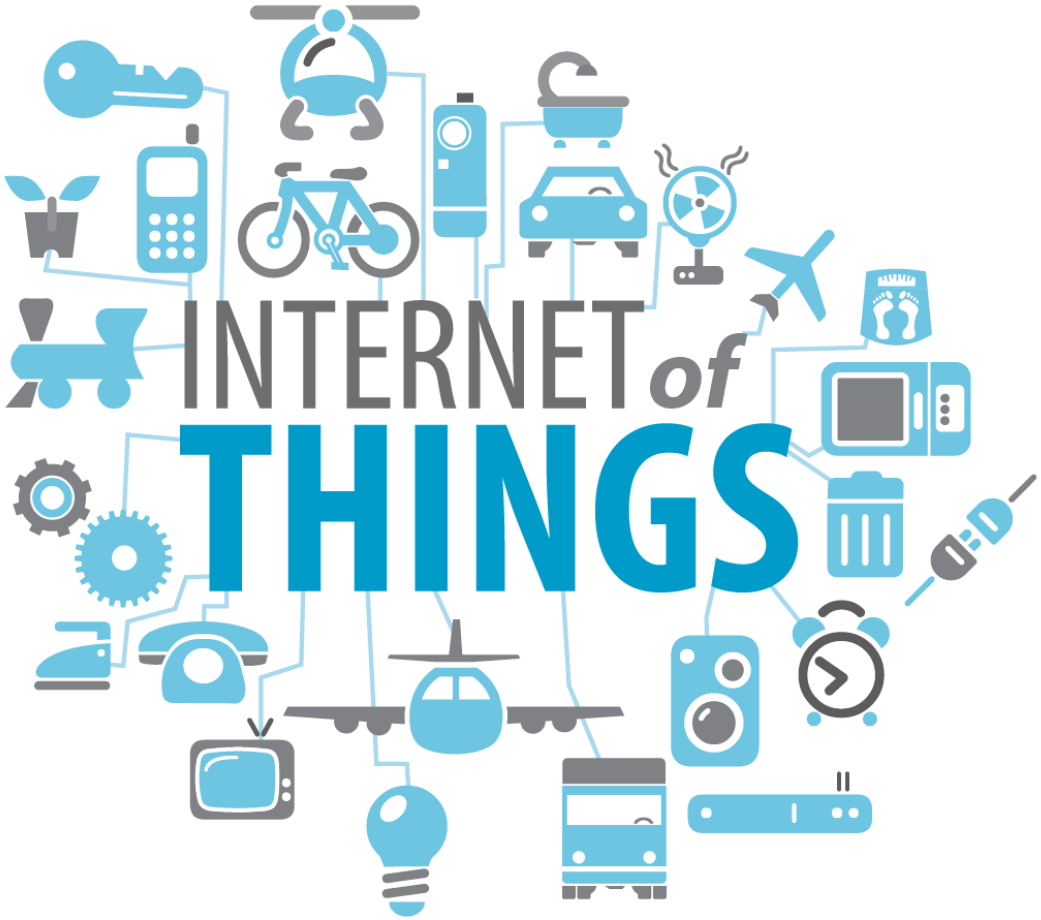
amazon tap

Alexa enabled portable speaker

JUST TAP & ASK

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)

http://krebsonsecurity.com/

Convert Select

Other — 45 comments

13 IoT Devices as Proxies for Cybercrime

OCT 16

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

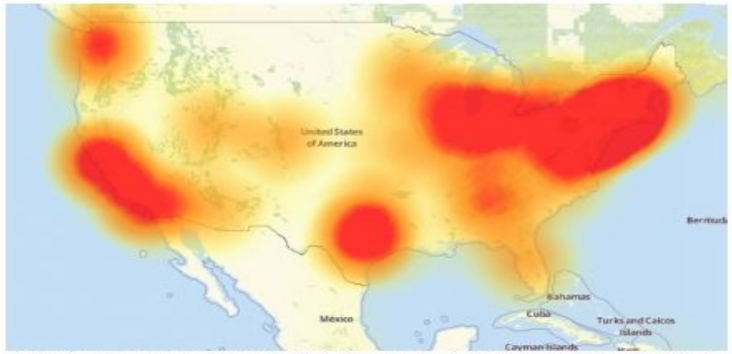
Recently, I heard from a cybersecurity researcher who'd created a virtual "honeypot" environment designed to simulate hackable IoT devices. The source, who asked to remain anonymous, said his honeypot soon began seeing traffic destined for **Asus** and **Linksys** routers running default credentials.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

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

OCT 16

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

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



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

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

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

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

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

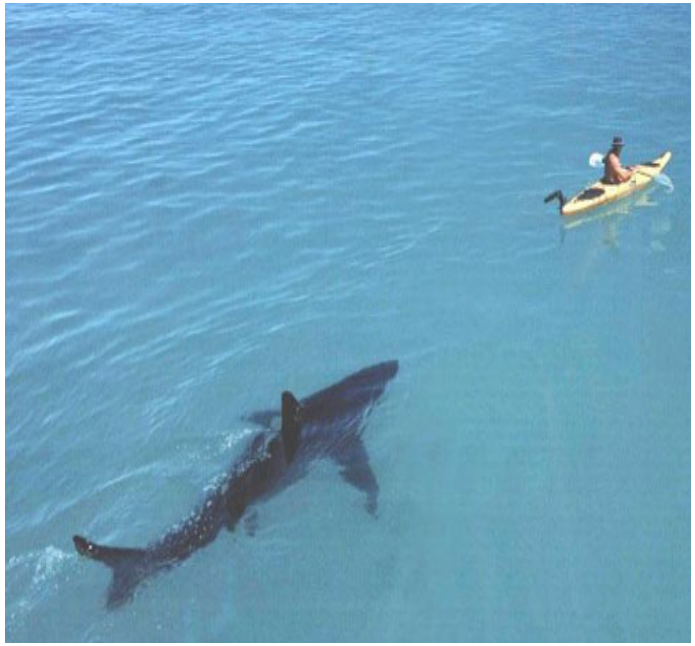
Largest Cyber Fraud Trends - Motivations

- 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
  - Theft of credit card information
  - (Corporate) Account take overs
  - Ransomware and Interference
    - w/ Operations

Account Takeovers – CATO

- Catholic church parish
- Construction & property management
- Hospice
- Regional bank
- Public School District
- Electrical contractor
- Utility company
- Industry trade association
- Rural hospital
- Mining company
- Board members



- On and on and on and on……

CATO Lawsuits – UCC

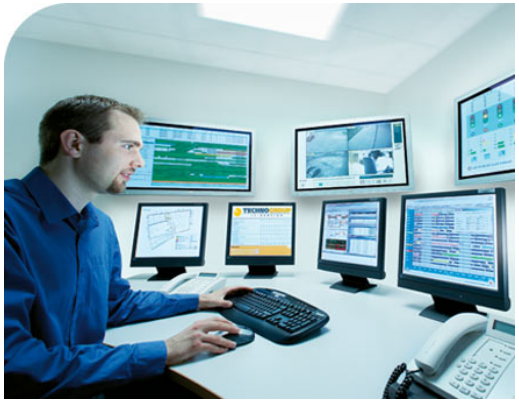
A payment order received by the [bank] is "effective as the order of the customer, whether or not authorized, **if the security procedure is a *commercially reasonable* method of providing security** against unauthorized payment orders, and the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer."

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

CATO Defensive Measures

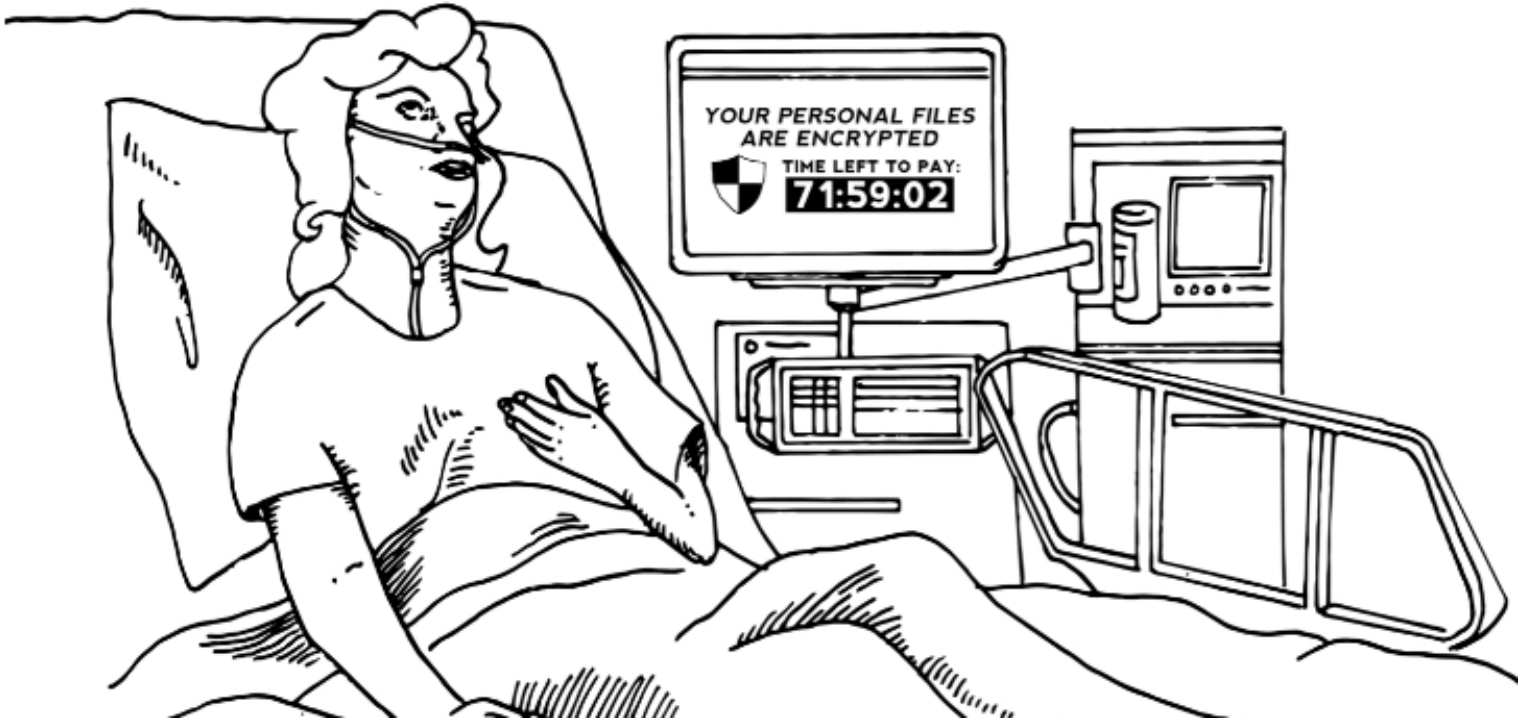
- **Authentication:**
  - Multi-layer authentication
  - Multi-factor authentication
  - Out of band authentication
- **Filtering (White Listing):**
  - Positive pay
  - ACH block and filter
  - IP address filtering
- **Monitoring:**
  - Dual control
  - Defined processes for payments
  - Activity monitoring / Anomaly detection
- Manual vs. Automated controls



Ransomware

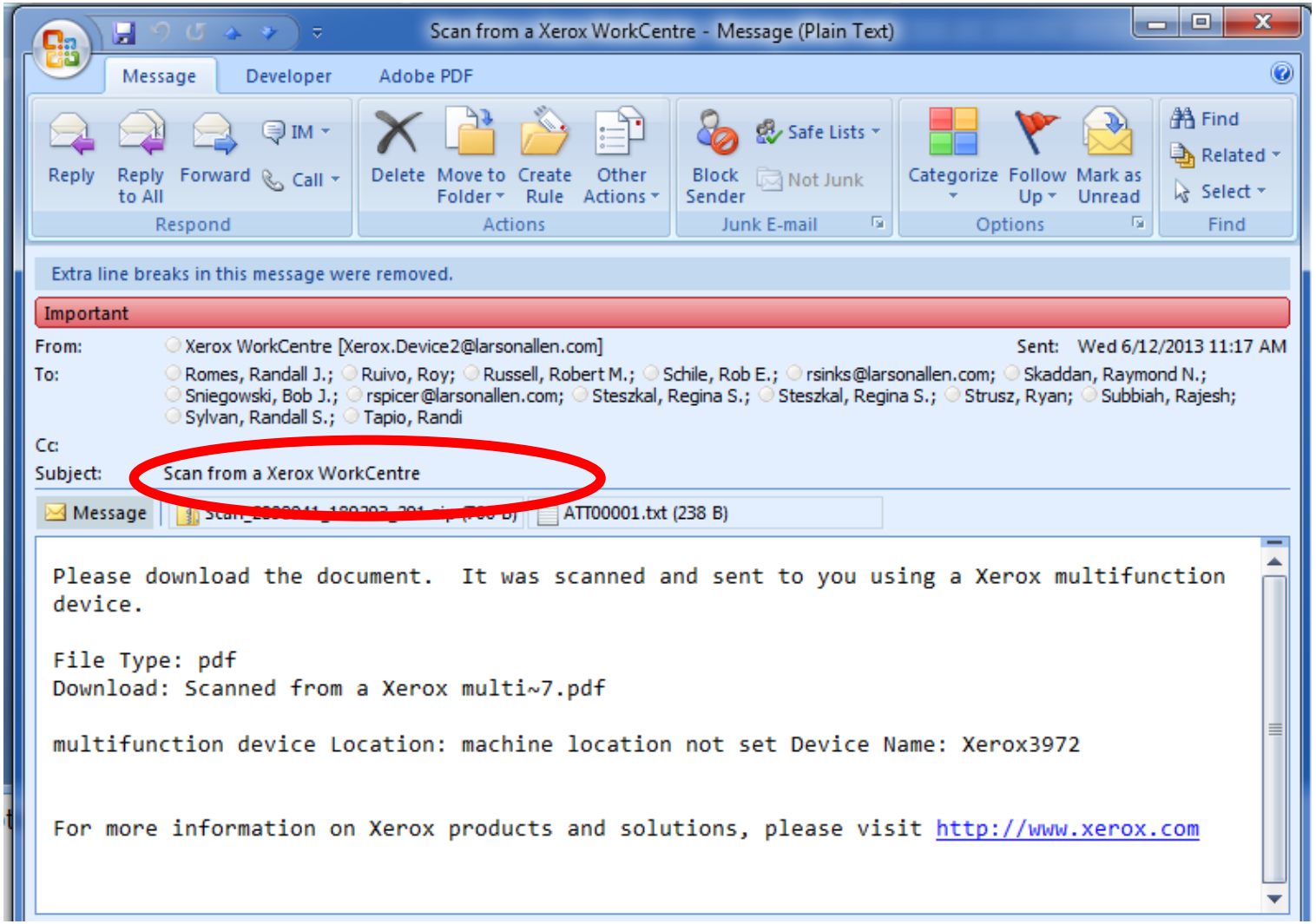
Hospital ransomware: A chilling wake-up call

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



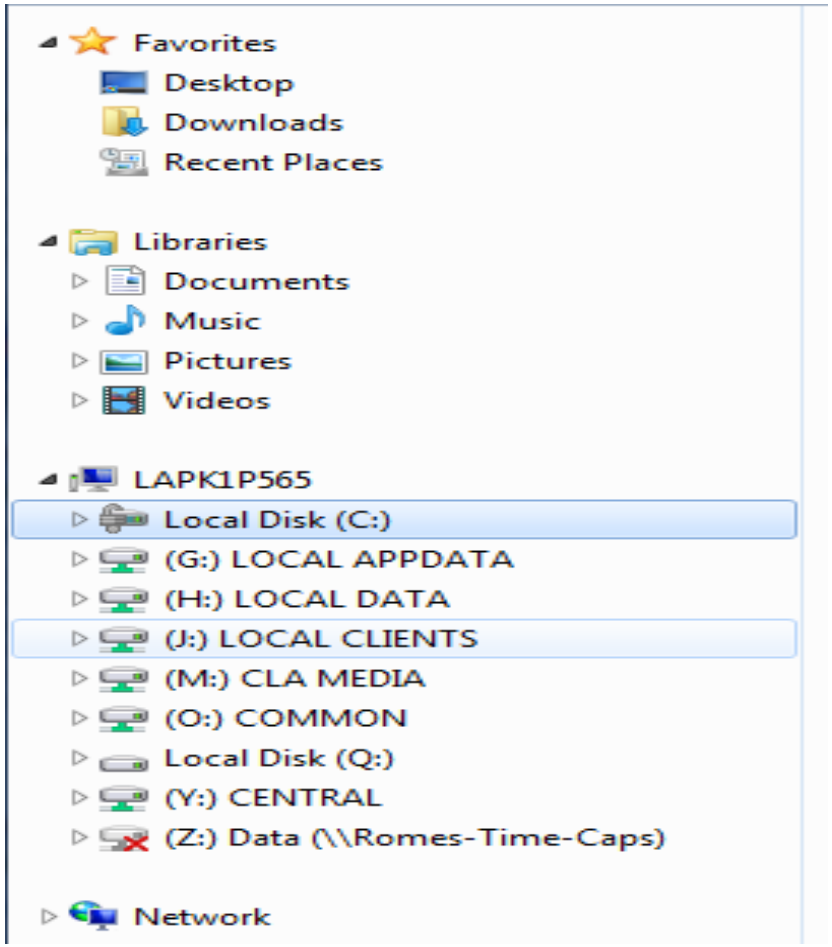
http://www.engadget.com/2016/02/19/hospital-ransomware-a-chilling-wake-up-call/

Ransomware



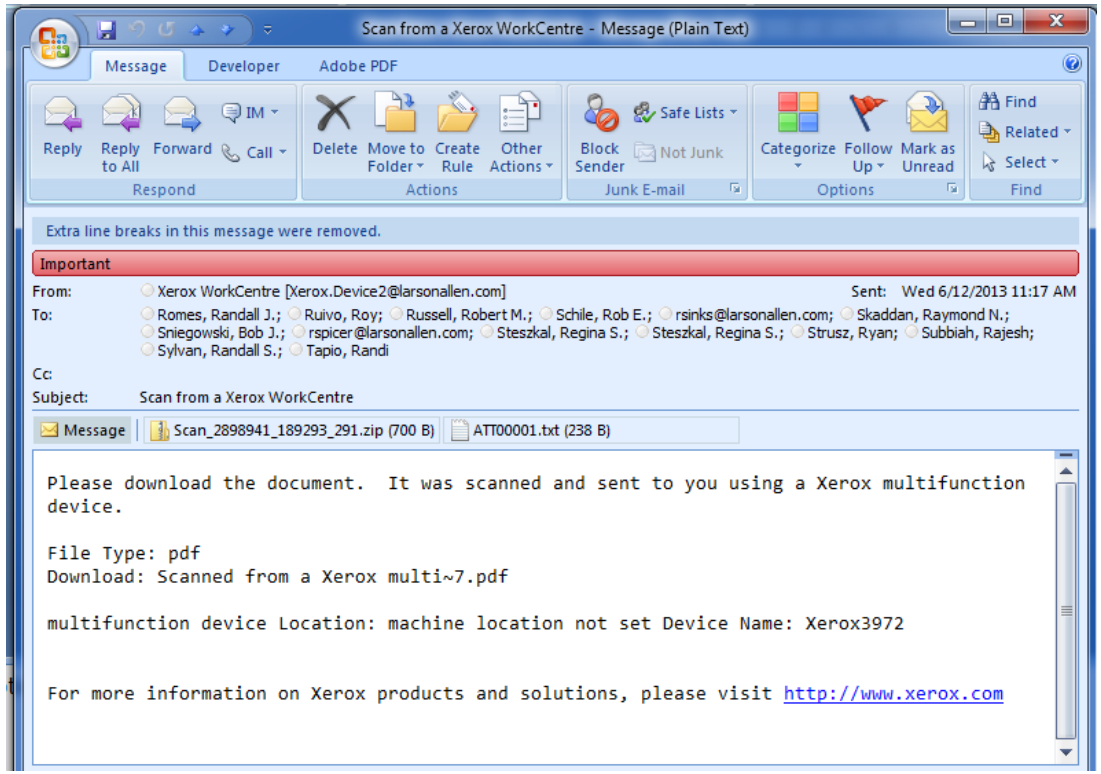
Ransomware

- Malware encrypts everything it can interact with



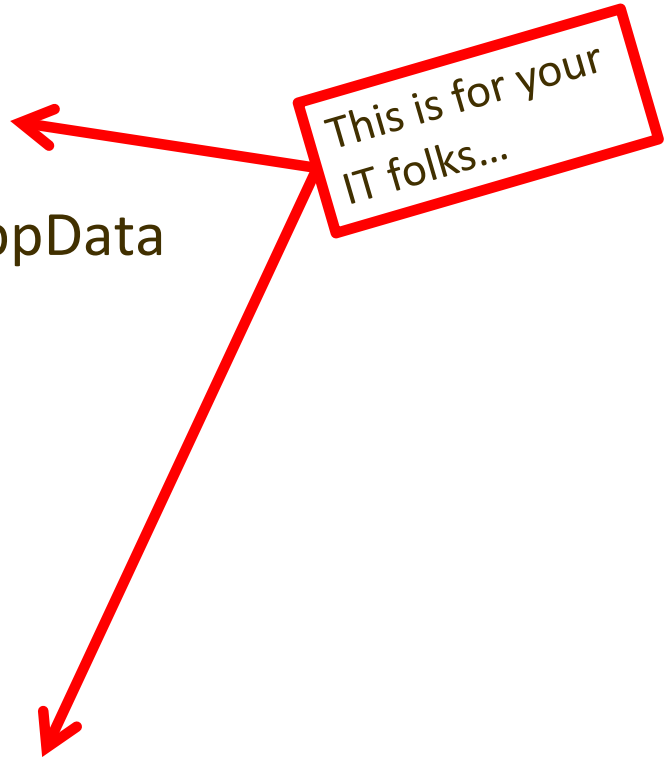
Ransomware Defensive Strategies

- Filtering capabilities
- Users that are aware and savvy



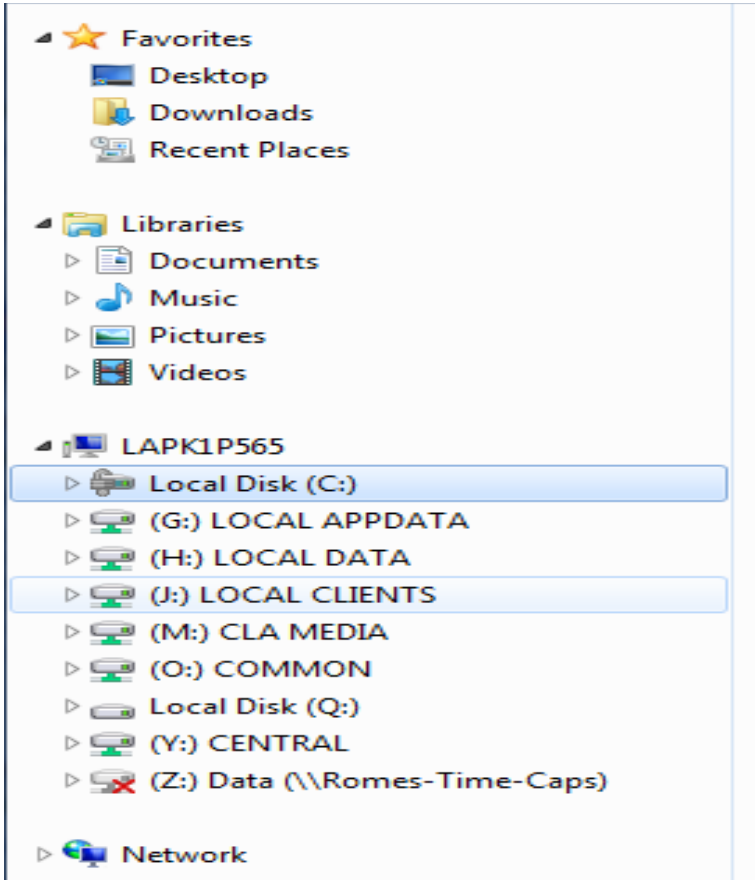
Ransomware Defensive Strategies

- 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
- Applocker
  - Similar to SRP
- EMET
  - https://technet.microsoft.com/en-us/security/jj653751

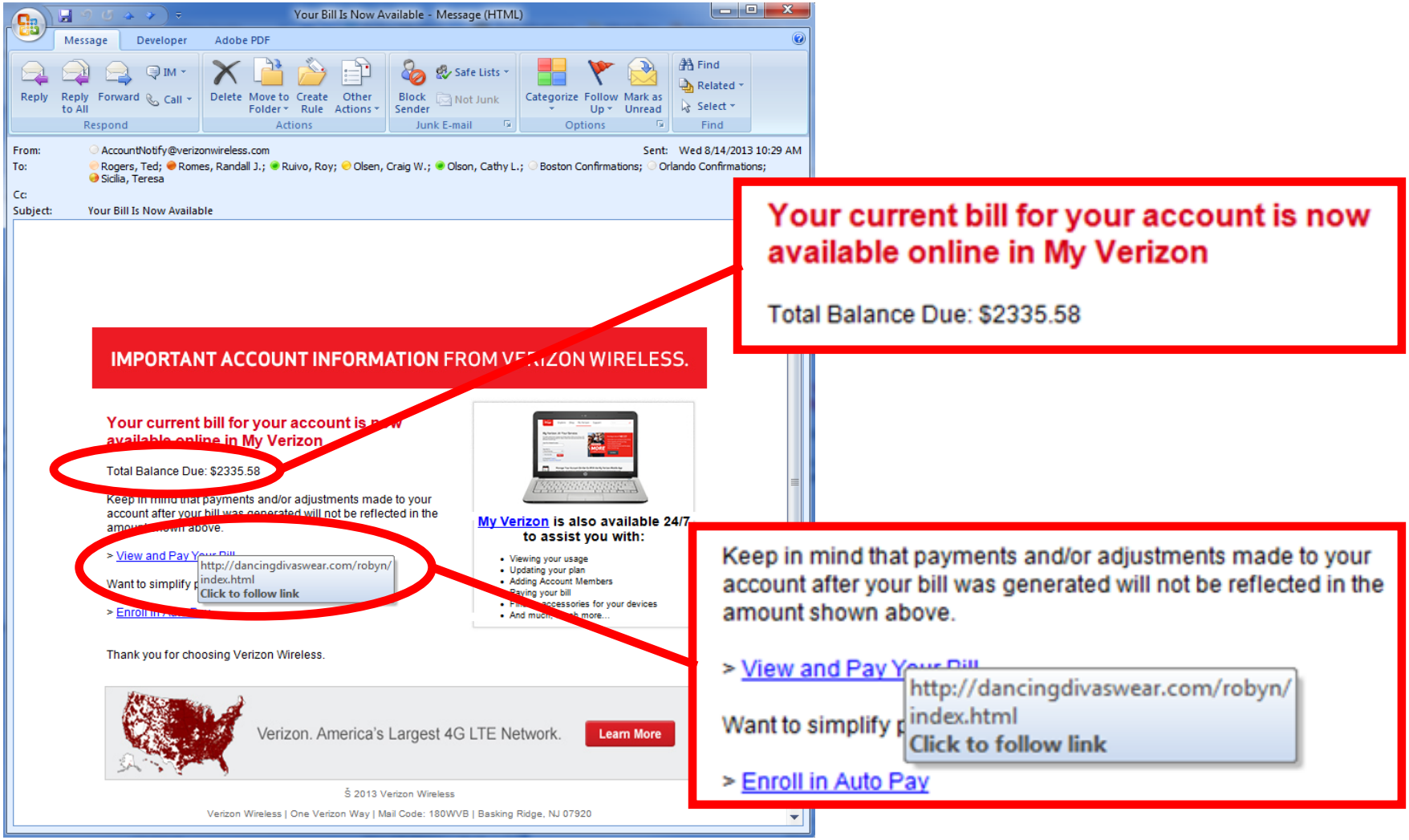


Ransomware Defensive Strategies

- Current operating systems
  - Windows XP?
  - Windows 2003 server?
- Patched vulnerabilities
- Working backups are critical…

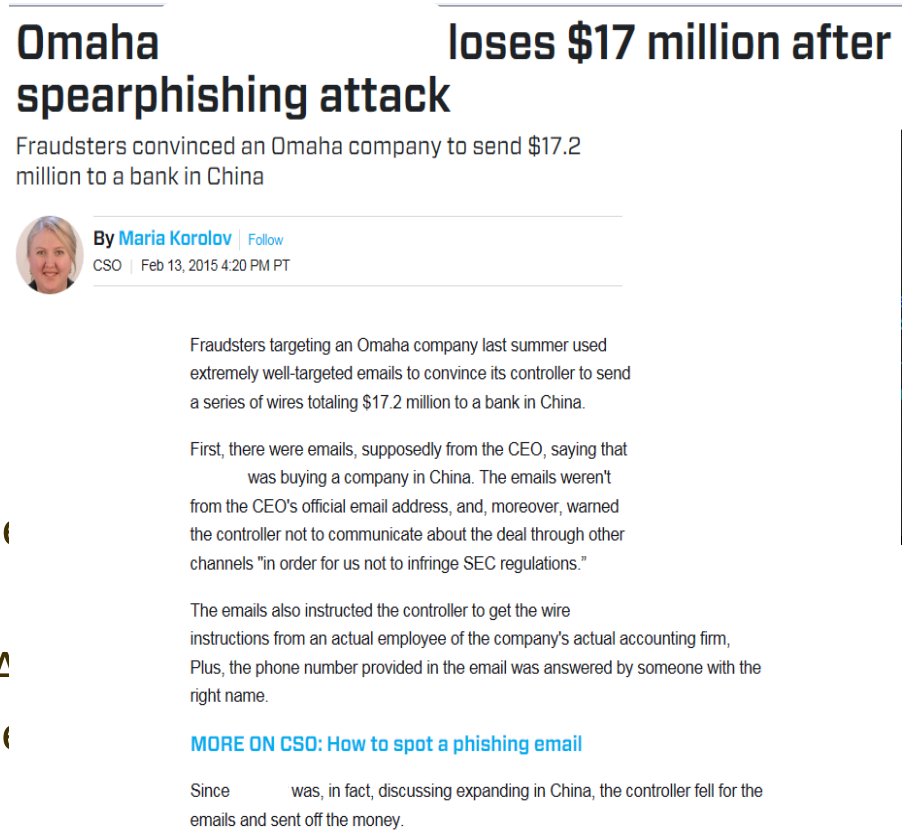


Phishing Examples



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 me of authorization
  2. Ensure recipient has VERBA validated with "source" of for financial transactions



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

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

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…

- https://www.youtube.com/watch?v=jwqV5L9fr60

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:

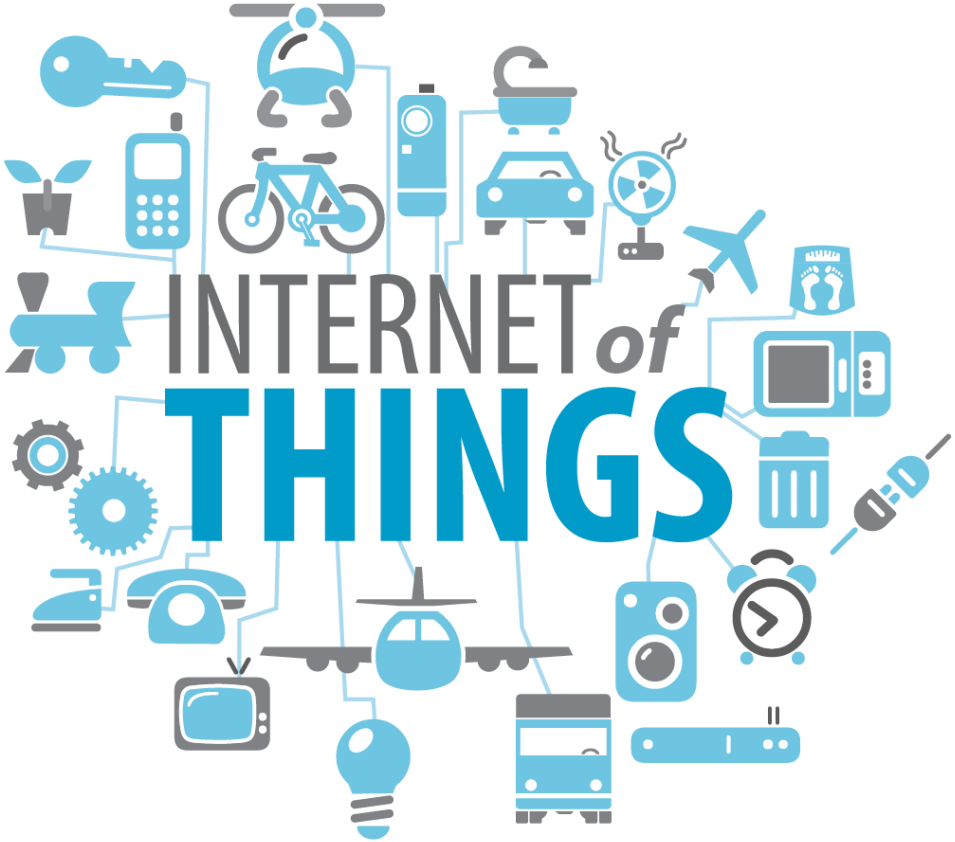
- "Hi, Sally said she would let you know I was coming to fix the printers…"

Plant devices:

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

Everything Can Talk to Everything….

- Environmental controls
- Smart grids/meters
- Security/monitoring systems



Key Defensive Strategies

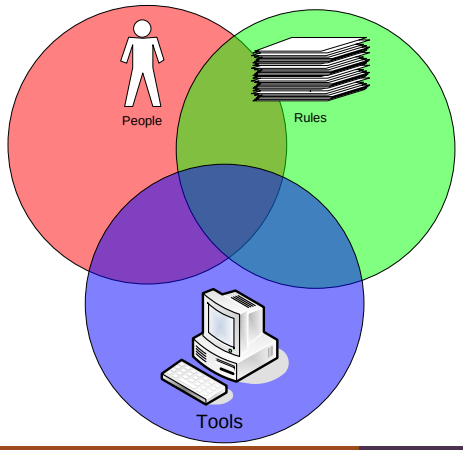
Strategies

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

- What do we expect to occur; how do we conduct business
- Standards Based Change Management
- Ex: CIS Critical Controls



CSC 1: Inventory of Authorized and Unauthorized Devices

CSC 2: Inventory of Authorized and Unauthorized Software

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

CSC 4: Continuous Vulnerability Assessment and Remediation

CSC 5: Controlled Use of Administrative Privileges

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

CSC 7: Email and Web Browser Protections

CSC 8: Malware Defenses

CSC 9: Limitation and Control of Network Ports, Protocols, and Services

CSC 10: Data Recovery Capability

CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

CSC 12: Boundary Defense

CSC 13: Data Protection

CSC 14: Controlled Access Based on the Need to Know

CSC 15: Wireless Access Control

CSC 16: Account Monitoring and Control

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

CSC 18: Application Software Security

CSC 19: Incident Response and Management

CSC 20: Penetration Tests and Red Team Exercises

Defined Standards

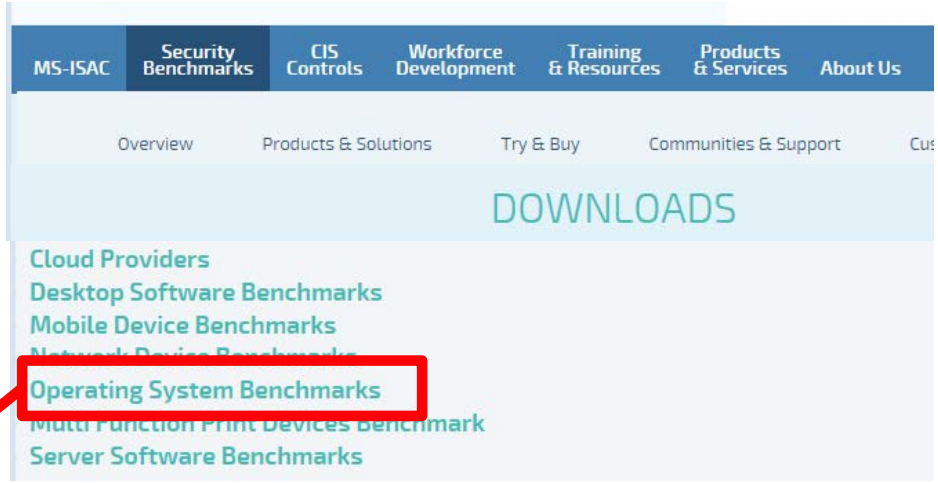
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

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**	**Foun-dational**	**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**	

Operational Discipline

- 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
- Documentation

Vulnerability and Patch Management Standards

- Define your standard
  - Internet facing critical updates will be applied within ___ Days
  - Internal system critical updates will be applied within ___ Days

- Manage to your standard

- Document and manage your exceptions

Vulnerability Management Monitoring

- Monitoring
  - System logs and application “functions”
  - Accounts
  - Key system configurations
  - Critical data systems/files

- Scanning
  - Patch Tuesday and vulnerability scanning
  - Rogue devices

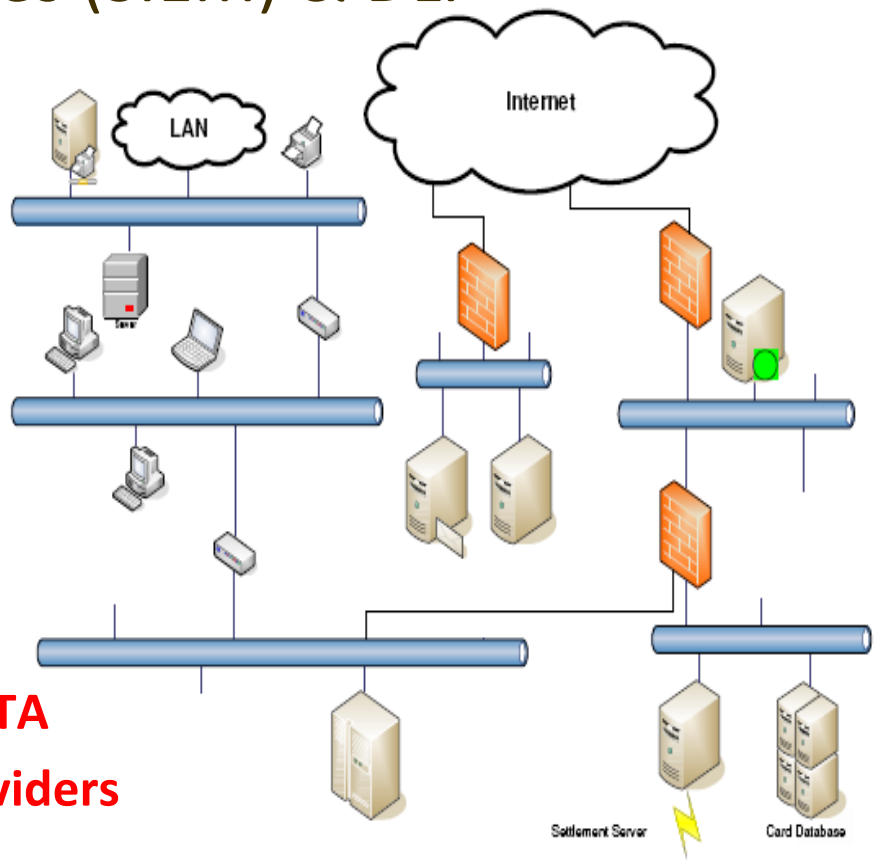
Incident Response & Forensic Resilience

- Response program prepared ahead of time
  - The Boy Scout's moto – Be Prepared
- Periodic testing of the program
  - Table top exercises
  - DRP and BCP plan testing
  - Penetration testing
- Table top exercises to practice
  - NIST 800-61
- Consideration of service providers and business partners

Know Your Network
Do You Know What is "Normal?"

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

- Infrastructure
- Servers & Applications
- Archiving vs. Reviewing



- **Know your: Network, Systems, DATA**
- **Monitor and review of service providers**

Validate You Are as Secure as You Hope

Test Your Cyber Security - How Vulnerable Are We?

- Penetration Testing
  - Informed/White Box
  - Uninformed/Black Box
- Social Engineering Testing
- True Breach Simulation
  - Red Team/Blue Team

Questions?

Randy Romes, CISSP, CRISC, MCP, PCI-QSA
Principal
Information Security Services
randy.romes@CLAconnect.com
888-529-2648

To receive future webinar invitations, subscribe at CLAconnect.com/subscribe.

Resources – Hardening Checklists

Hardening checklists from vendors

- CIS offers vendor-neutral hardening resources

  http://www.cisecurity.org/

- Microsoft Security Checklists

  http://www.microsoft.com/technet/archive/security/chklist/default.mspx?mfr=true

  http://technet.microsoft.com/en-us/library/dd366061.aspx

Most of these will be from the “BIG” software and hardware providers

Industry Breach Analysis Security Reports

- Intrusion Analysis: TrustWave (Annual)
  - https://www.trustwave.com/whitePapers.php
- Intrusion Analysis: Verizon Business Services (Annual)
  - http://www.verizonenterprise.com/DBIR/

Ransomware Safeguards

- Software Restriction Policies are one good way to prevent this.
  - https://technet.microsoft.com/en-us/library/cc759648(v=ws.10).aspx

Ransomware Safeguards

- Stopping .exe launch from AppData locations and $temp$.
  - Malware we were looking at the other day dropped .bat, .vbs, and .exe in appdata folder.
  - Restricting what applications can run from appdata/temp is very important.
  - Webroot had a good write up on this a few days ago.
    - ◊ http://www.webroot.com/blog/2016/02/22/locky-ransomware/
    - ◊ Apparently the executable only runs in $temp$. Restricting what gets run from there that would help.

Ransomware Safeguards

- Do an audit of file permissions where backups are stored.
  - Identify what users could encrypt backups if they were to become infected.
  - Generally, you would want the location very restrictive – read only access even for most administrators.
  - Backups should be done with a service account.
  - Users should not have access to the backup location.
  - You could also restrict the backup network access temporally similar to a bank vault.
    - ◊ That could be done with a simple script that would disable the port during the day and then re-enable just before the backup starts.