Trends in Cyber Crime and How to Protect Your Institution

Mark Eich and Christina Bowman

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.

CPE Requirements

- Answer the polling questions

- If you are participating in a group, complete the CPE sign-in sheet and return within two business days
  - Contact webmaster@CLAconnect.com

- Allow four weeks for receipt of your certificate; it will be sent to you via email

* *This webinar, once recorded, has not been developed into a self study course. Therefore, watching the recording will not qualify for CPE credit.*

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
- With more than 60 years of experience in the nonprofit sector, we have one of the largest nonprofit practices in the country

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

Speaker Introductions

- **Mark Eich, CPA**

  Principal

- **Christina Bowman, CPA**

  Senior Manager

Learning Objectives

- At the end of this session, you will be able to:
  - Name current hacking trends and how they are enabled
  - Identify the key role employees / users play in security
  - Illustrate how to better defend your organization from these types of attacks

Cyber Crime in Action: A Case Story

Case Study- ABC Institution

- Request from President to CFO via email
- Payment for purchase of $75,000 of computer equipment is OVERDUE
- Several correspondence back and forth requesting additional documentation, all received timely and as requested
- International wire sent late afternoon on Day 1

Case Study- ABC Institution (continued)

- How could this happen?
  - Someone is on vacation that is usually involved in the process
  - Emails AT FIRST are masked to appear legit, including signature line

Case Study- ABC Institution (continued)

- Day 2- CFO follows up with IT and Procurement to verify computer purchases

- Request a stop payment with the Bank

- Case reported to Bank's fraud division, local FBI office as well as Internet Crime Compliant Center (IC3), a partnership between the FBI and the National White Collar Crime Center

2016 Trends in Cyber Crime

Themes

- Hackers have “monetized” their activity
  - More hacking
  - More sophistication
  - More “hands-on” effort
  - Smaller organizations targeted

What Are They Doing?

- Organized Crime
  - Wholesale theft of personal financial information
- CATO– Corporate Account Takeover
  - Use of online credentials for ACH, CC, and wire fraud
- Ransomware

Black Market Economy - Theft of PFI and PII

Active campaigns involving targeted phishing and hacking focused on common/known vulnerabilities.

- Target
- Goodwill
- Jimmy Johns

- University of Maryland
- University of Indiana

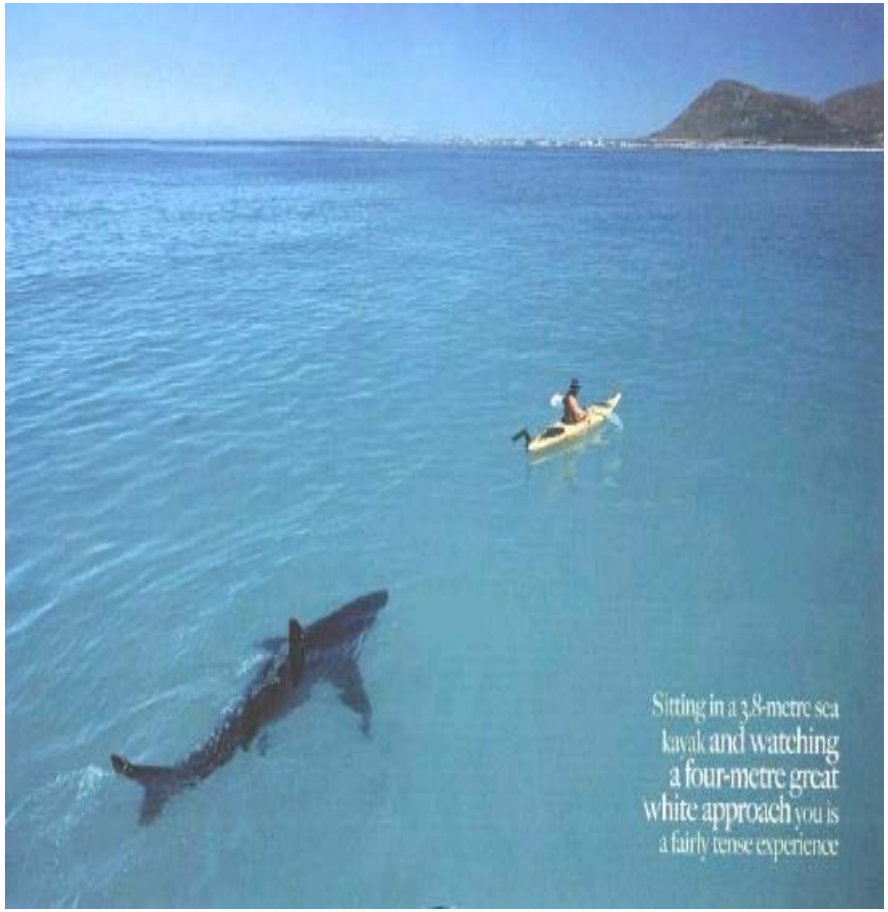
- Anthem
- Blue Cross Primera

- Olmsted Medical Center
- Community Health Systems

Corporate Account Takeover

- Catholic church parish
- Hospice
- Collection agency
- Main Street newspaper stand
- Electrical contractor
- Health care trade association
- Rural hospital
- Mining company

- On and on and on and on…….



CATO – Three Versions

- Deploy malware – keystroke logger
- Deploy malware – man in the middle
- Recon / email persuasion (“Whaling”)

CATO Defensive Measures

- Multi-layer authentication
- Multi-factor authentication
- Out of band authentication
- Positive pay
- ACH block and filter
- IP address filtering
- Dual control
- Activity monitoring

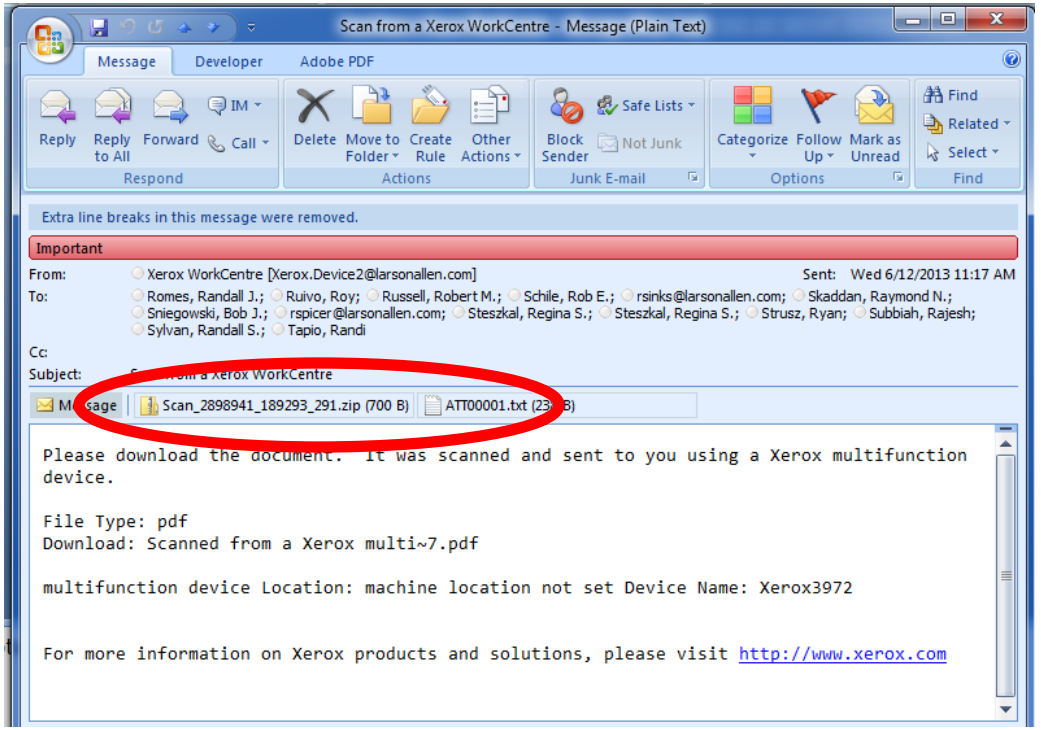
Ransomware

- Malware encrypts everything it can interact with
  - V1: Everything where it lands
  - V2: Everything where it lands plus everything user has rights to on the network
  - V3: Everything where it lands plus everything on the network

- CryptoLocker / Cryptowall

Ransomware

- Zip file is preferred delivery method
  - Helps evade virus protection
- Working (tested) backups are key



The Cost?

Norton/Symantec Corp:

- Cost of global cybercrime: $388 billion
- Global black market in marijuana, cocaine and heroin combined: $288 billion

Social Engineering

"Amateurs hack systems, professionals hack people."

Bruce Schneier

- Pretext phone calls
- Building penetration
- Email attacks

10 Key Defensive Measures

Attacks Are Preventable!

- Intrusion Analysis: TrustWave
- Intrusion Analysis: Verizon Business Services
- Intrusion Analysis: CERT Coordination Center
- Intrusion Analysis: CLA Incident Handling Team

Strategies

Our information security strategy should have the following objectives:

- Users who are more aware and savvy
- Networks that are resistant to malware
- Relationship with our FI is maximized

Ten Keys to Mitigate Risk

1. Strong Policies

- Email use
- Website links
- Removable media
- **Users vs Admin**
- **Insurance**

Ten Keys to Mitigate Risk

2. Defined user access roles and permissions

- Principal of minimum access and least privilege
- **Users should NOT have system administrator rights**
  - **"Local Admin" in Windows should be removed (if practical)**

Ten Keys to Mitigate Risk

3. **Hardened internal systems (end points)**
   - Hardening checklists
   - Turn off unneeded services
   - **Change default password**
   - **Use strong passwords**
   - **Consider application white-listing**
4. **Encryption strategy – data centered**
   - Email
   - Laptops and desktops
   - Thumb drives
   - **Email enabled cell phones**
   - Mobile media

Ten Keys to Mitigate Risk

5. Vulnerability management process

- Operating system patches
- **Application patches**
- Testing to validate effectiveness –
  - "belt and suspenders"

Ten Keys to Mitigate Risk

6. **Well defined perimeter security layers:**
   - **Network segments**
   - Email gateway/filter
   - Firewall – “Proxy” integration for traffic in AND out
   - Intrusion Detection/Prevention for network traffic, Internet facing hosts, AND workstations (end points)
7. **Centralized audit logging, analysis, and automated alerting capabilities**
   - Routing infrastructure
   - Network authentication
   - Servers
   - Applications

Ten Keys to Mitigate Risk

8. Defined incident response plan and procedures

- **Be prepared**
- Including data leakage prevention and monitoring
- Forensic preparedness

Ten Keys to Mitigate Risk

9. Know / use Online Banking Tools

- Multi-factor authentication
- Dual control / verification
- Out of band verification / call back thresholds
- ACH positive pay
- ACH blocks and filters
- Review contracts relative to all these
- Monitor account activity ***daily***
- **Isolate the PC used for wires/ACH**

Ten Keys to Mitigate Risk

10. Test, Test, Test

- "Belt and suspenders" approach
- Penetration testing
  - ◊ Internal and external
- Social engineering testing
  - ◊ Simulate spear phishing
- Application testing
  - ◊ Test the tools with your bank
  - ◊ Test internal processes

Questions?

Hang on, it's going to be a wild ride!!

Mark Eich, Principal

Information Security Services Group

mark.eich@CLAconnect.com

612-397-3128

Christina Bowman, Senior Manager

christina.bowman@CLAconnect.com

410-308-8064