Cybersecurity Fraud Trends: Spear Phishing, Ransomware and Defensive Strategies

Cyber Security Risk and Mitigation Strategies

- Randy Romes
- Principal
- CliftonLarsonAllen - Information Security

- Janet Scannell
- Chief Technology Officer
- Carleton College
About CliftonLarsonAllen

Information Security offered as specialized service offering for over 20 years

- Penetration testing
- Vulnerability assessment
- IT/Cyber security risk assessments
- IT audit and compliance
  - HIPAA, HITRUST, PCI-DSS
- Incident response and forensics
- Security awareness training
- Independent security consulting
About Carleton College

- Founded in 1866, Carleton College is a small, private liberal arts college in Northfield, Minnesota
- 2100 students and 500 faculty-staff
- Founding principle of shared governance, including faculty President sitting on President’s Cabinet
- Chief Technology Officer role created in 2013. Janet Scannell has 15 years in corporate world as engineer, software developer and project manager. 17 years in higher education.
Cyber Fraud Risk Themes

• Hackers have “monetized” their activity
  – More sophisticated hacking
  – More “hands-on” effort
  – Smaller organizations targeted
  – Black market economy

• Everyone is a target...

• Phishing is a root cause behind the majority of cyber fraud and hacking attacks
Cybercrime as an industry

- Suppliers
- Markets
- Service providers ("cybercrime as a service")
- Financing
- Trading systems
- Proliferation of business models
Black Market Economy - Theft of PFI and PII

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

- **RETAIL**
  - Target/Home Depot
  - Jimmy Johns/Goodwill

- **Higher Education**
  - University of Indiana
  - Rockhurst University

- **Large Personnel Breaches**
  - OPM
  - Blue Cross Primera

- **Health Care Systems**
  - Community Health Systems
Account Takeovers – CATO

- Catholic church parish
- Hospice
- Regional bank
- Public School District
- Main Street newspaper stand
- Electrical contractor
- Utility company
- Industry trade association
- Rural hospital
- Mining company
- Credit Union (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
Phishing – CATO – NACHA (ACH) Update

Phishing – CATO – NACHA (ACH) Update

• Employee clicked on a phishing email appearing to come from the National Automated Clearing House Association (NACHA)
  – Embedded link resolves to a Russian IP address
• Employee’s internet banking credentials were compromised
• Employee’s browser was hacked
  ➢ Injected with malicious HTML registry setting
  ➢ Pop-up asks for additional information when visiting banking site
  ➢ Employee also received call from supporting actor in attack
Phishing – CATO – NACHA (ACH) Update

- Lessons learned
  - Weak/missing filtering capabilities
  - Lack of employee awareness
  - Excessive user access (operating system)
  - No segregation of duties (application)
  - No incident response plan
  - IT indicated the employees system was “clean” – this was not the case (training/awareness)
  - Lack of log retention/server logging not enabled
  - System was powered off
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
Phishing and 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/
Phishing and Ransomware

Extra line breaks in this message were removed.

From: Xerox WorkCentre [Xerox.Device2@larsonallen.com]  
To: Romey, Randall J.; Ruiu, Roy; Russell, Robert M.; Schle, Rob E.; rsinks@larsonallen.com; Skaddan, Raymond N.; Sniegowski, Bob J.; rspeier@larsonallen.com; Steszkal, Regina S.; Steszkal, Regina S.; Strusz, Ryan; Subbiah, Rajesh; Sylvan, Randall S.; Tapio, Rand  
Cc:  
Subject: Scan from a Xerox WorkCentre

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

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

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

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

- Malware encrypts everything it can interact with

```
PAY
us
money
```
Phishing and Ransomware

• Filtering capabilities

• Users that are aware and savvy

• Minimized user access

• Working backups are critical...

• See appendix...
How do hackers and fraudsters break in?

“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...
Phishing Examples

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
  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

Phishing Emails – Malicious Office Document

• Attackers are embedding malware in Office documents (Macros)

• Enabling Macros on the document allows the malicious code to run

➢ Remediation
  – Don’t open attachments from unknown sources
  – Don’t open attachments you didn’t expect
  – Don’t enable Macros in unknown/untrusted documents
Pre-text Phone Calls (Phishing by phone)

- “Hi, this is Randy from Fiserv 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 Home Equity Line of Credit (HELOC) accounts, fraudulent ACH transactions,…
Email Phishing – Targeted Attack

Only one tell-tale sign
Key Defensive Strategies
Strategies

Our information security strategy should have the following objectives:

- Users who are savvy and engaged
- Networks that are resistant to malware and attacks – technology and policy.
- Be Prepared… Monitoring, Incident Response, Testing, and Validation
Call To Action – at Carleton College

Experts can **tell** users what to do
- Limit access from off-campus
- Use of two-factor authentication

Experts can **inspire** users
- Annual public presentation. DBIR data.
- Securing the Human training

Experts can **partner** with users
- Jointly created data risk guidelines
- Interviews to inform training approach
Call To Action – Technology and Policy

Thoroughly assess your risks
Three R’s: Recognize, React, Respond

Thoroughly validate your controls
- High expectations of your vendors
- Penetration testing
- Vulnerability scanning
- Controls to secure backups
- Social engineering testing
Strategies to Mitigate Phishing Risks

• Rescind messages at first notification!
• Minimized user access rights
• Two-factor authentication
• Networks that are resistant to attacks
• Preparedness... Monitoring, Alerting, Backups & Restoration and Incident Response Capabilities
• Hardest to “control” but most important: Users who are aware and savvy
Questions?
Randy Romes, CISSP, CRISC, MCP, PCI-QSA  
Principal  
Information Security Services  
randy.romes@CLAconnect.com  
888-529-2648

Jane Scannell  
Chief Technology Officer  
Carleton College  
jscannell@carleton.edu  
507-222-4077
Hardening checklists from vendors

- CIS offers vendor-neutral hardening resources
  

- Microsoft Security Checklists
  
  

Most of these will be from the “BIG” software and hardware providers
Industry Breach Analysis Security Reports

• Intrusion Analysis: TrustWave (Annual)

• Intrusion Analysis: Verizon Business Services (Annual)
  – http://www.verizonenterprise.com/DBIR/
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/](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 Defensive Strategies

• Software Restriction Policies
  – Not allowing files/DLLs to run in AppData

• Applocker
  – Similar to SRP

• EMET
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.