Friend or Foe –
Do You Know Who You’re Talking To?

Anne Tell and Rafael Martinez-Chapman
May 5, 2016
Executive Summary

• Cybersecurity is growing problem for banks, Treasury and finance professionals

• Attacks are increasing in
  • Sophistication – from false checks to fake voicemails (really!!)
  • Number of events – driven by automation and digital systems
  • Cost to the system – estimated by the FBI at $2B over two years

• Treasury team from Level 3 via this presentation will provide
  • Awareness of types of attack
  • Framework used to manage risk
    • Communication
    • Process
    • People

• Objective is to leverage information to derive your own plan
Company Overview

Over $8B FY 2015 Total Revenue

Over $2.6B FY 2015 Adjusted EBITDA

~12,500 Employees

Connecting 60+ Countries and Counting

200,000+ Route Miles of Fiber Globally

Approx. 350 Multi-tenant Data Centers
Global Reach

- Corporate headquarters – Broomfield, CO (near Flatiron Mall)
  - Regional HQ in London, UK, Buenos Aires, Argentina, Broomfield and Littleton
  - Sales and technical locations in over 60 countries
Finance Organization Background

- Consist of ~1,650 employees
  - Includes treasury, accounting, payroll, accounts receivable, accounts payable, internal audit, tax, procurement teams
  - ERP – single, global system

- Treasury is responsible for policy creation and implementation
  - Manage over 250 bank accounts across 100 legal entities
  - Use approximately 30 currencies

- Treasury work station – Wall Street Systems Treasura
Financial Cyber

CRIMINAL NINJA ATTACK!!

Beware, reference section approaching
What is Cyber Crime?

• A crime committed through use of the internet
  • Cyber criminals exploit the same systems that have made it easier for people and companies to conduct online business
What is Cyber Crime?

- A crime committed through use of the internet
  - Cyber criminals exploit the same systems that have made it easier for people and companies to conduct online business

- **Cyber crimes may be committed by a single person, do not require the criminal to be physically present**
  - Committed from remote locations, even outside the country
  - Makes it difficult for law enforcement to locate, charge criminals
What is Cyber Crime?

• A crime committed through use of the internet
  • Cyber criminals exploit the same systems that have made it easier for people and companies to conduct online business

• Cyber crimes may be committed by a single person, do not require the criminal to be physically present
  • Committed from remote locations, even outside the country
  • Makes it difficult for law enforcement to locate, charge criminals

• What started primarily as hacking and installing malicious software has evolved into more skillful and clever ways to victimize others
What is Cyber Crime?

• A crime committed through use of the internet
  • Cyber criminals exploit the same systems that have made it easier for people and companies to conduct online business

• Cyber crimes may be committed by a single person, do not require the criminal to be physically present
  • Committed from remote locations, even outside the country
  • Makes it difficult for law enforcement to locate, charge criminals

• What started primarily as hacking and installing malicious software has evolved into more skillful and clever ways to victimize others

• Presentation will focus on crimes occurring in business settings
  • Harder to achieve but typically produces larger payout
  • Firm may decide not to investigate if amount is low
    • Average crime = $120k, but has been as high as $90M (FBI data)
Financial Cyber Scams

• *Attacks on computer systems*

• *Email spam and phishing*

• *Spoofing attacks*

• *Unexpected money or prize scams*

• *Threats or extortion*
Attacks on Computer Systems

- **Unauthorized access, or hacking**
  - Gaining access to a computer or network without permission

- **Malware**
  - Software that can monitor activity, steal data or cause damage to a computer or network
  - Include viruses, worms, spyware, trojans or bots

- **DDoS or Distributed Denial of Service**
  - Floods a computer, network or website with data
  - Overloads system and prevent it from functioning properly

IT primarily manages this risk
Email Spam and Phishing

• **Spam**
  - Unsolicited electronic junk mail, often containing offers of money or other prizes, website links or phone numbers

• **Phishing**
  - Tricks people into giving out private personal or company information
  - Often appear to come from legitimate businesses
  - 1 in 392 emails are phishing attempts (Source: Internet Security Threat Report 2014, Symantec Corporation)

**Individuals across the entire organization primarily manage this risk**
Spoofing Attacks

• **Spoofing**
  • When a person or program successfully masquerades as another by falsifying data
  • Potentially spoofed data: emails, caller ID or GPS location

• **Email address spoofing**
  • Forgery of an email header so that it appears to come from someone trustworthy
  • Possible because the main email protocol does not include a mechanism to authenticate the source of the email
  • More malicious varieties can cause serious problems, security risks and theft of property

IT may screen, but individuals primarily manage this risk
Unexpected Money or Prize Scams

• *Unexpected money scams*
  • Include inheritance scams, money reclaim scams, ‘Nigerian’ scams or other upfront payment schemes
  • Generally request advance fees, bank account information or to transfer money with the promise of receiving money

• *Unexpected prize scams*
  • Include lottery scams, travel scams or the promise of prizes
  • Generally request the advance fees, bank account information or the transfer of money to claim the prize

If it sounds too good to be true, it probably is
Threats or Extortion

• May include ransomware, malware or ‘hit man’ scams
  • Places harmful software on your computer or network
  • Demands payment to allow regaining access
  • ‘Hit man’ scams involve death threats unless payment is made to the hired ‘hit man’ sending the email

• Extortion may threaten to expose confidential personal or company information publicly unless payment is made

IT, risk management and individual behavior help mitigate this risk
Cyber Crime Trends
Losses on the Rise

- Email Spoofing has cost businesses around the globe more than $2 billion in slightly over two years (Source: US Federal Bureau of Investigation)
  - More than 12,000 victims
  - Average loss of $120,000, but up to $90 million

- DDoS attacks are increasing, and can result in revenue loss, reputational damage, customer turnover and lost intellectual property
  - DDoS attacks that targeted Yahoo and Amazon in 2000 were estimated to have cost over $1.2 billion in damages and was launched by a 15 year old Canadian boy (Source: Yankee Group)

Level 3 monitors DDoS attempts: estimates there are several attempts per second on the network
Losses on the Rise, continued

- Advent of Bitcoin has increased ransomware attacks
  - Easy to use, publicly available, decentralized and provides strong anonymity
  - Ransomware has become a ‘cash cow’ for cyber thieves
    - Continue to invest in better attack techniques to evade detection from advanced security systems (Source: Security Week)

- Social media is providing new ways to perpetrate cyber crimes
  - Creates risks such as exposure to sensitive information, oversharing, loss of brand control, non-compliance and vulnerabilities
  - Cyber thieves can cause even greater damage by launching malicious campaigns, coordinating attacks, conducting research and using it as a mechanism to release stolen content and defacement (Source: Security Week)
Losses on the Rise, continued

- Every 3.6 seconds a webpage is being infected  
  (Source: InfoNetics, Sophos Security Threat Report)

- A 24 hour outage for a large E-Commerce vendor costs ~$30 million  
  (Source: Estimated by Forrester, IDC and Yankee Group)

- There has been a 660% increase in cyber security incidents from 2006 – 2010  
  (Source: The Internet Crime Complaint Center IC3)

- In a survey of 2,300 IT Executives in Canada, France, Germany, UK and US, 25% admitted they suffered a security breach during the past year  
  (Source: Forrester)

Listed as a top issue for Board of Directors to address, particularly for “retail” enterprises
Increasing Sophistication

• Spear phishing  (Source: Kyriba)
  • Scam where thieves hack into a company’s internal network to impersonate employees and gain confidential information
    • Study and learn company processes
    • Access Outlook calendars
    • Quickly delete fraudulent email created from an employee’s account
    • Gain access to vendor, customer and other third party names and email
    • Insert themselves into a conversation or process, such as directing payments to a fraudulent bank account

• Voice mail fraud  (Source: Kyriba)
  • Leverages online corporate recordings, such as earnings calls, to manipulate voices to create fraudulent voicemail usually requesting an urgent payment

Always be suspicious, particularly of requests outside regular process
What Can We Do?
# Level 3’s Approach

## COMMUNICATION
- **Raise awareness across organization**
  - Corporate newsletter is printing a 6-piece article on topic
- **Bring attention that risk is company wide and to the reputation of the firm**
  - Deception can impact employees, vendors, customers and other that interact with the company

## PROCESS
- **Review and adjust policies and procedures**
  - Augment existing processes, such as adding supervisor review of vendor changes to payment address, wire instructions or ACH information
- **Ensure adequate controls from front line employees to management**
  - Add topic to internal audit plans
  - Self audit on an ongoing basis

## PEOPLE
- **Provide cross-functional education**
  - Focus on teams more likely to be targeted (AP, vendor management)
  - Leave reference materials to enable individuals to act
  - Materials define the threat (“what the risk is“) and provide a plan of action (“what to do”), along with contact details
  - Make it easy for people to report and act once threat is suspected

© 2016 Level 3 Communications, LLC. All Rights Reserved. Proprietary and Confidential.
Level 3’s Tactics

• Be suspicious
  • Be wary of any urgent payment request, especially when it is an exception to the normal, approved way to pay

• Always double check/confirm before making changes to current payment instructions, one time payments and new vendor set up
  • Require strong controls for vendor set up and payment instruction changes for existing vendors
  • Regardless of who is requesting payment, confirm the request with a known contact
  • Use more than one method of contact – if changes are requested via email, confirm the request with a phone call or different contact method to a known contact
  • Watch for spoofed email addresses and new contact phone numbers
  • For added security, require changes to payment instructions to be put in writing
Level 3’s Tactics, continued

• Make it a routine
  • Managers should allow their teams to routinely double check payment requests and requests for changes
  • Process exceptions and urgent requests should be questioned

• Do not buy into the drama and emotion of the moment
  • Fraudsters attempt to create urgency, panic or perceived risk for not acting quickly
  • Remain calm and stick to processes and procedures, and double check with known contacts
Level 3’s Tactics, continued

- Be cautious about what information you share
  - Limited information, which is already public, is all that should be shared with unknown parties
  - This includes what is said in voice mail and out-of-office replies

- Train and test
  - Create a process to train and test each other
  - Periodically work with your security team to conduct simulations and review results
  - Practice makes you more ready to handle a real scam
2016 RSA Security Conference

Chris Richter
Senior Vice President, Global Security Services
Level 3 Communications
Conclusion
Conclusion

• Cyber crime is getting worse
  • Cyber thieves continue to create new methods of exploiting individuals and companies, and are striking more frequently

• Understand, recognize and take the threats seriously
  • Treasury needs to take an active role in risk management

• Review and update policies and procedures
  • Include auditors, business partners and security team

• Focus on teamwork and communication
  • When in doubt, ask
  • Report suspicious activity
Conclusion

• Case Study – Level 3 communications to employees
  • Treasury, Legal, Security and Communications published an article on the internal employee website regarding financial scams
    • Part of 6-piece article series (saying it differently and saying it often)
    • Included an outline of the tactics previously outlined in this presentation
    • Provided instructions for how to report an incident or suspicious activity
    • Had a link to an internally developed security awareness training course which all employees are required to complete annually

• Added bonus of Case Study – Treasury can leverage this work for an RMAFP Summit Presentation!!

Success depends on all employees recognizing and reporting threats, and taking steps to ensure the company does not become a victim of cyber crime
Questions?