Fraud and Security Presentation

Alan A. Hale – SVP; Payment Fraud Prevention Manager

Bank of America Merrill Lynch

Bank of America
Merrill Lynch

Agenda

- Evolving threat environment
- Fraud schemes and scams
- Security best practices

Evolving Threat Environment

Bank of America
Merrill Lynch

Current Threat Trends

Bank of America Merrill Lynch

57% of business leaders feel their organization is **MORE SUSCEPTIBLE** to cybersecurity threats in 2018 than previous year

$12.5 Billion
Business Email Compromise

$2.4 Million
Average organization cost from malware attack

22% of corporate ransomware victims had to to fully cease business operations during event

59% of malicious email sent contained a banking Trojan surpassing ransomware for the first time since 2016

Companies are hit by ransomware every **40 seconds**

90 % Of businesses were targeted and received emails related to Business Email Compromise (BEC)

$12M Average organization cost from cyber fraud

136% increase in reported fraud losses related to Business Email Compromise

hxxps://www[.]ic3[.]gov/media/2018/180712.aspx
hxxps://threatconnect[.]com/wp-content/uploads/ThreatConnect-Building-a-Threat-Intelligence-Program.pdf
hxxps://www[.]Malwarebytes[.]com/pdf/infographics/Malwarebytes_The_State_Of_Ransomware_Among_SMBs.pdf
hxxps://www[.]Proofpoint[.]com/sites/default/files/pfpt-us-tr-q118-quarterly-threat-report.pdf
Ponemon Institute 2018 State of Endpoint Security Risk Report

Fraud Schemes and Scams

Bank of America
Merrill Lynch

Ransomware Event

Fast Food Restaurant Chain - $400MM Annual Revenue - 100 Locations

Sequence of Events:

- Individual employee workstation observed to be infected at 12:20 AM in HQ location.
- Malware spreads rapidly, by 7:00 AM remaining workstations across the organization and files on multiple servers are encrypted.
- Standalone workstation purchased to conduct bank business.
- External I.T. firm engaged.
- Root cause infection email spam.
- Initial Bitcoin Ransomware of $10,000 paid to perpetrators.
- Second request for additional $5 000 received and paid.
- Encryption keys received.
- Restoration initiated.

Impacts

- Paralyzed business operations and financial transactions.
- $15,000 paid to perpetrators.
- Malware consultation expense impact.
- 10 business days to restore impacted systems.

Business Email Compromise

CEO Scam / Masquerading

Bank of America Merrill Lynch

Some Phishing schemes involve mimicking internal emails

- Perpetrators know key individuals and their roles in the company based on:
  information in social media sites, professional associations, company website, etc.
- Domain names may look similar to your company name but are intentionally misspelled
- Fraudulent message appears to be coming from senior executives within the company
- Urgency and confidentiality are key components of the email

From: Treasurer@mycompany.com
Sent: Tuesday, July 8, 2017 11:17a.m.
To: chris.smith@mycompany.com
Subject: FW: Wire Transfer

This is the third one. We are pulling the confirmation now and will send to you.

From: Treasurer@mycompany.com
Sent: Wednesday, June 11, 2017 11:30a.m.
To: chris.smith@mycompany.com
Subject: FW: Wire Transfer

FYI, this needs to get processed today. I checked with (insert name here) to get your help processing it along. I will assume we take care of any vendor forms after the fact. I can send an email directly to (insert name here) or let you drive from here. Let me know.

From: Treasurer@mycompany.com
Sent: Wednesday, June 11, 2017 9:59a.m.
To: chris.smith@mycompany.com
Subject: FW: Wire Transfer

Process a wire of $73,508.32 to the attached account information. Code it to admin expense. Let me know when this has been completed.

Thanks.

----------Forwarded message----------

From: CEO@rnycompany.com
Sent: Wednesday, June 11, 2017 6:45a.m.
To: Treasurer@mycompany.com
Subject: Wire Transfer

Insert name (Treasurer),

Per our conversation, I have attached the wiring instructions for the wire. Let me know when done.

Thanks. Insert name, (CEO)

If you receive an email such as this:

- Contact the sender by an alternative method to validate the instructions
- Follow your authentication procedures
- Validate that correspondence is legitimate
- Employ dual controls prior to making payment changes or processing payments

Look at the spelling of the words and names carefully

CEO@mycompany.com

CEO@rnycompany.com

Business Email Compromise

Vendor Email

Bank of America Merrill Lynch

HealthCare Specialty Company - $50MM Annual Revenue - Southeast regional coverage

Sequence of Events:

- Company receives email messages from the "sales person" of their vendor
- Message indicates the vendor is updating their accounts receivable system and changing bank account information
- Company replies to email as well as calls the phone number listed in the email provided for the sales person
- Phone number did not belong to the sales person
- Email address did not belong to the sales person
- Company changed beneficiary account information in AP system
- Six figure payment sent to new beneficiary account
- Vendor notified company of non-receipt of outstanding bill
- Company realized prior emails and phone call was not to the vendor

From: Chris Treasurer [mailto:chris_treasurer@lrxl.cc]
Sent: Monday, March 21, 2016 10:30a.m.
To: Joe@mycompany.com
Subject: Updated Banking Information

Attention: Accounts Payable – Updated Banking Information

Joe,

We have recently completed an update to our Accounts Receivable processing. As such, please remit all payables to our updated account beginning today.

Bank: ABC123Bank

Account Number: 123456789012
Routing Number: 987654321

Email all payment confirmations to chris_treasurer@lrxl.cc

Can you email me when this change is complete?

Thank You
Chris Treasurer,
Treasurer, Other Company
212.555.1212

Impacts:

- Company changed account information in AP system without appropriate verification
- Six figure payment sent to fraudulent beneficiary account
- Vendor notified company of non receipt of outstanding bill
- Company realized emails and phone call were with imposter posing as the vendor

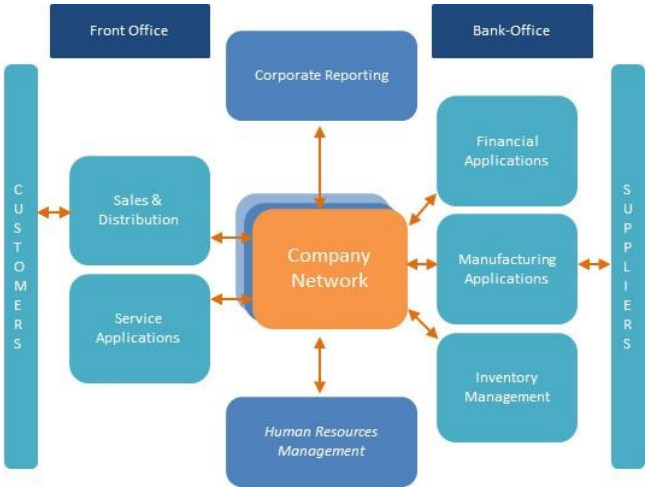
Business Email Compromise

Payroll Files Targeted

Bank of America Merrill Lynch

University - 5,000 + Students and Faculty - Southwest US

- Attackers sent phishing emails to employees of the university announcing benefits enrollment
- Attackers created a site which looked similar to university's prior year benefits research page
  - Site captured employee's Single Sign-on (SSO) ID and Password
- Attackers then logged-in to the university system
  - Determined which applications and functions were linked to the IDs that were harvested
  - Attacker able to explore the infrastructure and found access to the Payroll Platform
- Updated employee payroll account for Direct Deposit



Impacts

- Multiple employees did not receive their pay on Friday as funds were redirected to attackers accounts
- Payroll department conducted research on Monday and Tuesday
- Checks were presented to employees until employee payroll accounts could be restored
- ACH recall transactions were met with funds already removed from attackers' accounts
- University estimated loss plus research expense to be ~$70,000
- Employees needed to be issued new IDs and have access restored to university applications

Why Email Fraud Works

Bank of America Merrill Lynch

Messages Appear Highly Credible To User

- ✓ Well researched using social media
- ✓ Messages exploit the natural human tendency to trust and be helpful
- ✓ Emails use the right names & correct titles
- ✓ User similar domain names
- ✓ Custom-written to avoid spam filters

Appear From Senior Executive And Request Immediate Action

- ✓ Almost always under threshold required for a second signature
- ✓ Sometimes sent when key executive is on vacation- making an external or unknown domain name seem legitimate
- ✓ Sent when there is a company transition in the news, so taking advantage of current state of change

Targeted Company Lacks Essential Authentication And Controls

- ✓ Such as signature or sign-off on key controls
- ✓ Recipient ignores key procedures for fear of raising the ire of the CEO or CFO
- ✓ Employees are duped into thinking that checking on transaction might slow things down and derail a key deal

Organizations May Lack Essential Security Safeguards To Protect

- ✓ Controls such as endpoint security
- ✓ Data Encryption
- ✓ Email gateway technology to identify suspicious email

Security Best Practices

Bank of America
Merrill Lynch

Best Practices for Business Email Compromise

Bank of America Merrill Lynch

Never change beneficiary account information based solely on an email

Validate using other communication channels

Be alert to sudden changes in business practices

Develop procedures for non-standard requests

- Pick up the phone and call the individual – using the company directory or vendor information Another option is to have another associate create a new email from another PC to validate the instruction
- Validate instructions by having the sender provide the old payment instructions to include beneficiary and account along with the new payment instruction and account
- Ask for the number of an old invoice and the dollar amount
- Ask for the sender to send the new payment instructions from the company letterhead and validate the letterhead

Contact your vendors and partners -- are your payments up-to date?

Payment Fraud

Key elements

Bank of America Merrill Lynch

Best Practice

Simple, practical business controls significantly reduce risk:

- ✓ Use a bookmark to access the bank's site
- ✓ Hover over a link before clicking on it to reveal the true address to which you will be sent
- ✓ Avoid opening attachments that you were not expecting
- ✓ Be wary of pop-up messages asking you to update your computer
- ✓ Spot behaviour anomalies in the payment requests received via email
- ✓ Always be suspicious of communication from people or organizations that you don't recognize
- ✓ Be particularly wary of emails that warn of some dire consequence unless you take action
- ✓ Scrutinize emails: Carefully review email headers, domain names in the "from" field of the email, and the "reply-to" field of emails

Enterprise Phishing Susceptibility Report
An Inside Look at Employee Behavior Pertaining to Highly-Effective Phishing Scenarios

Lines of Defense for Ransomware

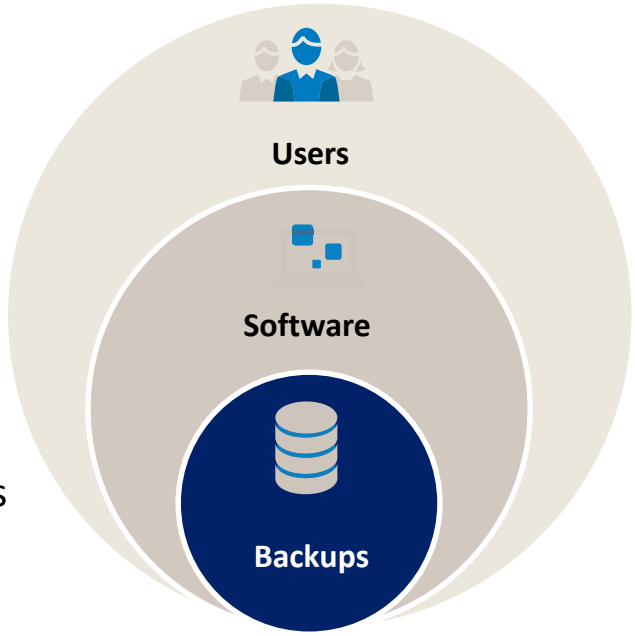
Bank of America Merrill Lynch

First Line of Defense: Users

- Security Awareness Training
- Simulated Phishing Attacks

Second Line of Defense: Software

- Firewall
- Antispam/anti-phishing
- Up-to-date antivirus software or advanced endpoint protection
- Software restriction policies on your network to prevent unauthorized applications from running
- Disciplined patch procedures



Third Line of Defense: Backups

- Backup Solution – software/hardware or both
- Ensure all data is backed up
- Ensure data is safe, redundant and accessible once backed up
- Regularly test the recovery function of backup/restore procedures

Mobile & Wireless

Bank of America Merrill Lynch

Attacks against mobile devices and wireless networks continue to rise as employees and consumers use mobile devices and connect to public Wi-Fi

Enable device access security

Enable a passcode, fingerprint or other authentication feature on all mobile devices

Keep OS & apps updated

Recent mobile threats targeted devices with unpatched mobile OS & apps. Apply updates as soon as they are available

Use official app stores

Apps available via untrusted app stores have a higher risk of malware. Only download from official mobile device vendor and corporate app stores

Turn off Wi-Fi & Bluetooth if not in use

Unless needed for a specific purpose, limit access to your location – rogue apps may track you – disable image geo-tagging

Practice mobile & wireless security daily to help protect your information and assets

Global wireless carrier networks are more secure than public Wi-Fi. Connect through your carrier when available.

Connect through a wireless carrier

When public Wi-Fi is only option, verify name of site Wi-Fi network with staff or posted signage before connecting

Verify Wi-Fi name before connecting

When connecting a business device, always use your corporate VPN or other security tools to protect your data

Connect through corporate VPN

Passwords

When creating passwords:

- Be creative, complex and meaningful. Find inspiration in personal memories.
- Make your password methodology a secret.
- Start with a phrase or sentence and transform it.
- String a series of random words together to create a strong password.

Do any of your passwords:

- Honor your first or current pet by including their name?
- Follow any common pattern on your keyboard?
- Make it easy for your partner or family to remember?
- Change only one character across different uses?
- Something related to your favorite sports team?

If you answered **YES** to any of the questions above, you should revise your password methodology

2018 Top Passwords:

1. 123456
2. Password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. Sunshine
9. Qwerty
10. iloveyou

https://www.welivesecurity.com/2018/12/17/most-popular-passwords-2018-revealed

Notice to Recipient

Bank of America Merrill Lynch

"Bank of America Merrill Lynch" is the marketing name for the global banking and global markets businesses of Bank of America Corporation. Lending, derivatives, and other commercial banking activities are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Securities, strategic advisory, and other investment banking activities are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

Investment products offered by Investment Banking Affiliates: Are Not FDIC Insured • May Lose Value • Are Not Bank Guaranteed.

This document is intended for information purposes only and does not constitute a binding commitment to enter into any type of transaction or business relationship as a consequence of any information contained herein.
These materials have been prepared by one or more subsidiaries of Bank of America Corporation solely for the client or potential client to whom such materials are directly addressed and delivered (the "Company") in connection with an actual or potential business relationship and may not be used or relied upon for any purpose other than as specifically contemplated by a written agreement with us. We assume no obligation to update or otherwise revise these materials, which speak as of the date of this presentation (or another date, if so noted) and are subject to change without notice. Under no circumstances may a copy of this presentation be shown, copied, transmitted or otherwise given to any person other than your authorized representatives. Products and services that may be referenced in the accompanying materials may be provided through one or more affiliates of Bank of America, N.A.
We are required to obtain, verify and record certain information that identifies our clients, which information includes the name and address of the client and other information that will allow us to identify the client in accordance with the USA Patriot Act (Title III of Pub. L. 107-56, as amended (signed into law October 26, 2001)) and such other laws, rules and regulations.
We do not provide legal, compliance, tax or accounting advice.
For more information, including terms and conditions that apply to the service(s), please contact your Bank of America Merrill Lynch representative.
Investment Banking Affiliates are not banks. The securities and financial instruments sold, offered or recommended by Investment Banking Affiliates, including without limitation money market mutual funds, are not bank deposits, are not guaranteed by, and are not otherwise obligations of, any bank, thrift or other subsidiary of Bank of America Corporation (unless explicitly stated otherwise), and are not insured by the Federal Deposit Insurance Corporation ("FDIC") or any other governmental agency (unless explicitly stated otherwise).
This document is intended for information purposes only and does not constitute investment advice or a recommendation or an offer or solicitation, and is not the basis for any contract to purchase or sell any security or other instrument, or for Investment Banking Affiliates or banking affiliates to enter into or arrange any type of transaction as a consequent of any information contained herein.
With respect to investments in money market mutual funds, you should carefully consider a fund's investment objectives, risks, charges, and expenses before investing. Although money market mutual funds seek to preserve the value of your investment at $1.00 per share, it is possible to lose money by investing in money market mutual funds. The value of investments and the income derived from them may go down as well as up and you may not get back your original investment. The level of yield may be subject to fluctuation and is not guaranteed. Changes in rates of exchange between currencies may cause the value of investments to decrease or increase.
We have adopted policies and guidelines designed to preserve the independence of our research analysts. These policies prohibit employees from offering research coverage, a favorable research rating or a specific price target or offering to change a research rating or price target as consideration for or an inducement to obtain business or other compensation.