Security and Fraud Prevention

Mary Rosendahl, Bank of America Merrill Lynch

May 2017

Bank of America
Merrill Lynch

Agenda

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

Bank of America
Merrill Lynch

The Threat Environment Is Evolving

$3.1 Billion

Paid by BEC victims since 2013

$1 Billion

Paid by ransomware victims in 2016

https://www.ic3.gov/media/2016/160614.aspx June, 2016

Fraud Schemes and Scams

Bank of America
Merrill Lynch

Email Fraud

Social Media

Bad guys rely on social media sites to gather details about a high level executive to impersonate along with a lower-level target.

Objective: make the target react to the approval power of spoofed executive

Domain Change

70% attacks involve domain spoofing[1]

Thieves register a domain that appears similar to the actual domain for a company.

Objective: the busy target does not notice the fake domain

Phishing Email

Recipient receives an email message with his name on it, as well as other details that make it look authentic (relevant details about impersonated executive and likely mentions a specific initiative.)

Objective: email looks authentic for user to act upon

User Assistance

Email looks authentic and prompts for specific action or transaction leading to a loss.

Objective: create a sense of urgency and may request that the individual bypass normal procedures

64% of IT security professionals regard email as a major cyber security threat[1]

65% don't feel fully equipped or up-to-date to reasonably defend against email based attacks[1]

1. https://www.mimecast.com/resources/press-releases/dates/2016/2/65-percent-of-global-businesses-ill-equipped-to-defend-against-email-based-cyber-attacks/

Why Email Fraud Works

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

Business Email Compromise

CEO scam

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, 2014 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, 2014 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, 2014 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, 2014 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)

Look at the spelling of the words and names *carefully*

CEO@mycompany.com

CEO@rnycompany.com

Business Email Compromise

Vendor email

Message

Someone posing as “supplier“ sends communication, requesting change to payment instructions or company account profile

Delivery

- **Email** - from company contact, but email address is not always correct
- **Postal mail** – usually sent with contact information for fraudster not the company
- **Phone call** - “Vishing=voice phishing”

Requests are typically are not consistent with established protocols:

- Change company profile within internal system
- Add a new contact representing the company
- Change the payment account
- Request to respond to requester once instructions are updated

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

Vendor Master File

Best Practices

- Establish written procedures for adding vendors
- Organize vendors into separate folders based on their business
- Categorize past and future payments on a month–to month basis
- Apply standard rules for names and addresses
- Ask for a W-9 from every vendor well before any payment is issued
- Perform regularly scheduled vendor maintenance
- **Verify all vendor changes via an out of band communication**

Vendor Master File

Best Practices for Initial Setup

- Establish clear standards for vendor setup and coding
- Implement a “look it up first” policy
- Create a fixed interval for clean-up
- Develop and use coding “standards”
- Institute Vendor Profile Form

PROOF OF EXISTANCE

- Corporate Charter
- Recent Audited Annual Report
- City/County Business License
- Sales Tax Certificate
- IRS Document/Notice
- Federal Tax Return
- Vendor Contract/Agreement
- Product Catalog
- 1099
- W-9

Best Practices for Business Email Compromise

Never reply to an email message, requesting a change to a beneficiary

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 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?

Non Financial Data Phishing Schemes

Tactic/Approach

- Target non-financial data
- Instructions to send personal information other than payments (i.e. IRS)

Request/scam

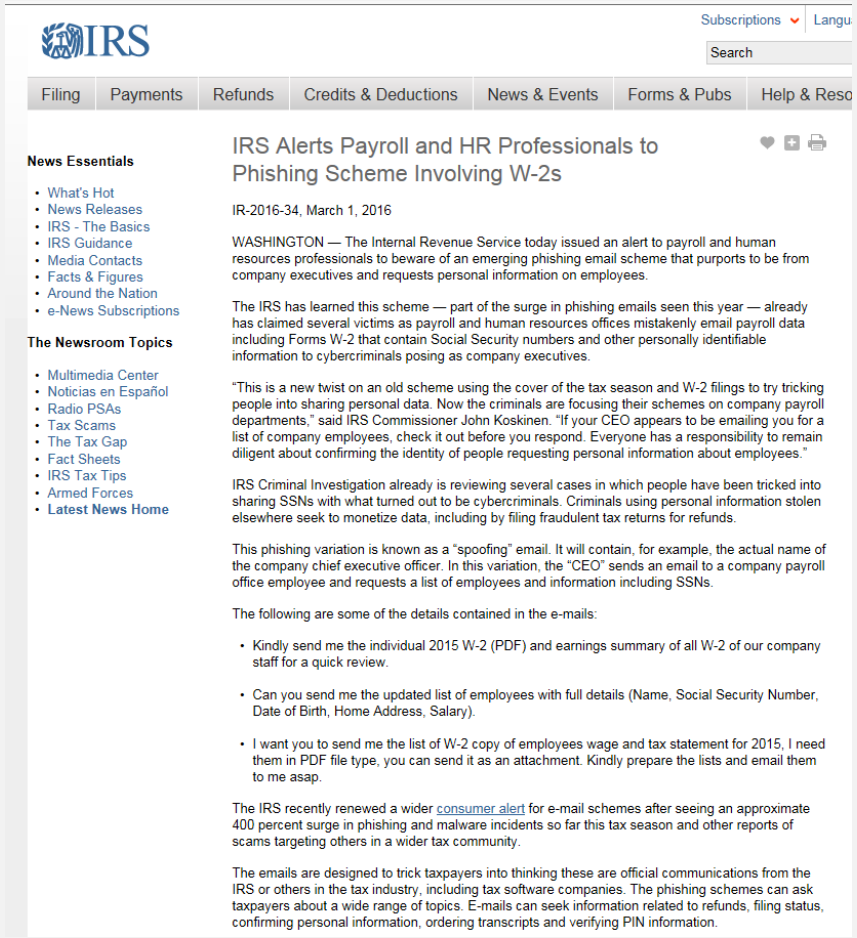
Request for sensitive private information

- Payroll files
- Employment information
- Employee Personally Identifiable Information (PII):
  - Drivers License
  - Social Security Number
  - Employee ID
  - Tax Information, W2

Creates opportunity for:

- Identity theft
- Fraudulent account opening
- False government Identification

IRS Alert



IRS

Subscriptions | Search

Filing | Payments | Refunds | Credits & Deductions | News & Events | Forms & Pubs | Help & Reso

News Essentials

- What's Hot
- News Releases
- IRS - The Basics
- IRS Guidance
- Media Contacts
- Facts & Figures
- Around the Nation
- e-News Subscriptions

The Newsroom Topics

- Multimedia Center
- Noticias en Español
- Radio PSAs
- Tax Scams
- The Tax Gap
- Fact Sheets
- IRS Tax Tips
- Armed Forces
- **Latest News Home**

IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s

IR-2016-34, March 1, 2016

WASHINGTON — The Internal Revenue Service today issued an alert to payroll and human resources professionals to beware of an emerging phishing email scheme that purports to be from company executives and requests personal information on employees.

The IRS has learned this scheme — part of the surge in phishing emails seen this year — already has claimed several victims as payroll and human resources offices mistakenly email payroll data including Forms W-2 that contain Social Security numbers and other personally identifiable information to cybercriminals posing as company executives.

"This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments," said IRS Commissioner John Koskinen. "If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees."

IRS Criminal Investigation already is reviewing several cases in which people have been tricked into sharing SSNs with what turned out to be cybercriminals. Criminals using personal information stolen elsewhere seek to monetize data, including by filing fraudulent tax returns for refunds.

This phishing variation is known as a "spoofing" email. It will contain, for example, the actual name of the company chief executive officer. In this variation, the "CEO" sends an email to a company payroll office employee and requests a list of employees and information including SSNs.

The following are some of the details contained in the e-mails:

- Kindly send me the individual 2015 W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review.
- Can you send me the updated list of employees with full details (Name, Social Security Number, Date of Birth, Home Address, Salary).
- I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.

The IRS recently renewed a wider consumer alert for e-mail schemes after seeing an approximate 400 percent surge in phishing and malware incidents so far this tax season and other reports of scams targeting others in a wider tax community.

The emails are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. The phishing schemes can ask taxpayers about a wide range of topics. E-mails can seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information.

Ransomware

Emerging fraud trend

Ransomware is a type of malware that restricts access to the infected computer system

- Demands ransom to remove the restrictions
- Some forms systematically encrypt files on the system's hard drive
- Difficult or impossible to decrypt without paying the ransom for the decryption key, some may simply lock the system and display messages to coax the user into paying
- Most ransomware enters the system through attachments to an email message

For consideration

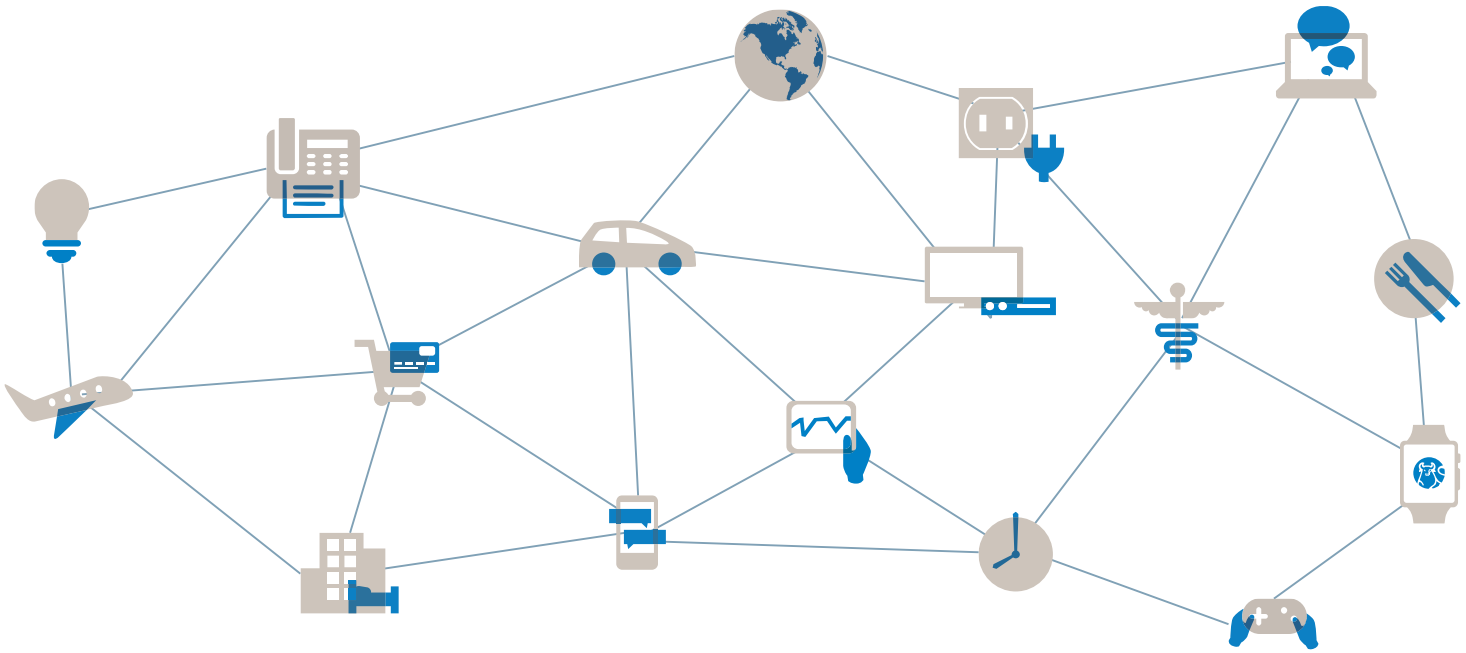
- Up to date anti-virus software
- Email gateway security products
- Employee education

Ransomware Brand Names

CryptoLocker 72:00:00 hours | Tescrypt | FakeBsod | CryptoWall | KRYPTERADE

Internet of Things (IOT)

As devices, systems and appliances increasingly communicate, verifying trust becomes a fundamental problem.



Security Best Practices

Bank of America
Merrill Lynch

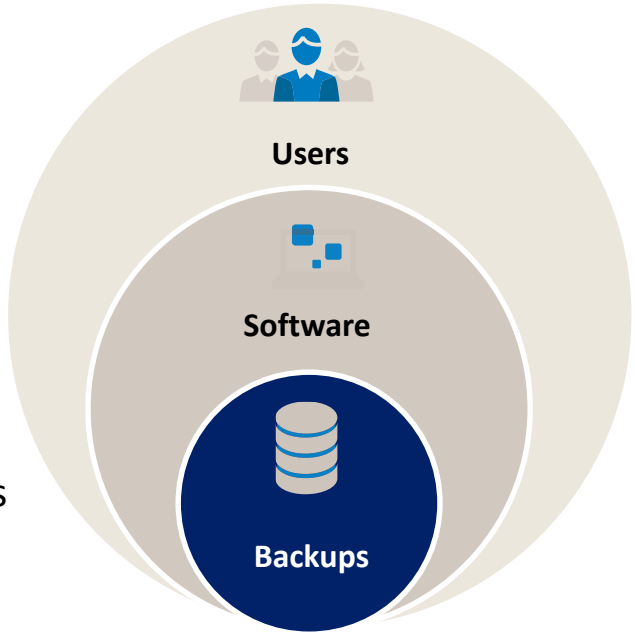
Lines of Defense for Ransomware

First Line of Defense: Users

- Security Awareness Training
- Simulated Phishing Attacks

Second Line of Defense: Software

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

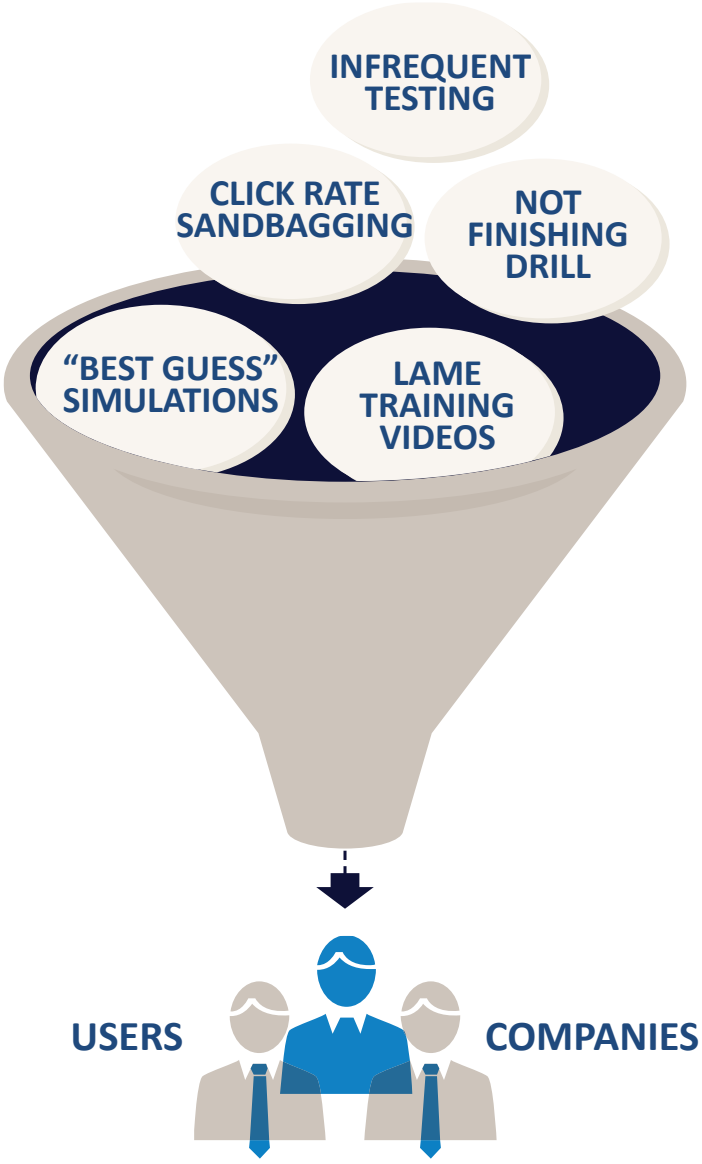


Third Line of Defense: Backups

- 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

Phishing Awareness Training Pitfalls

FIVE COMMON PITFALLS



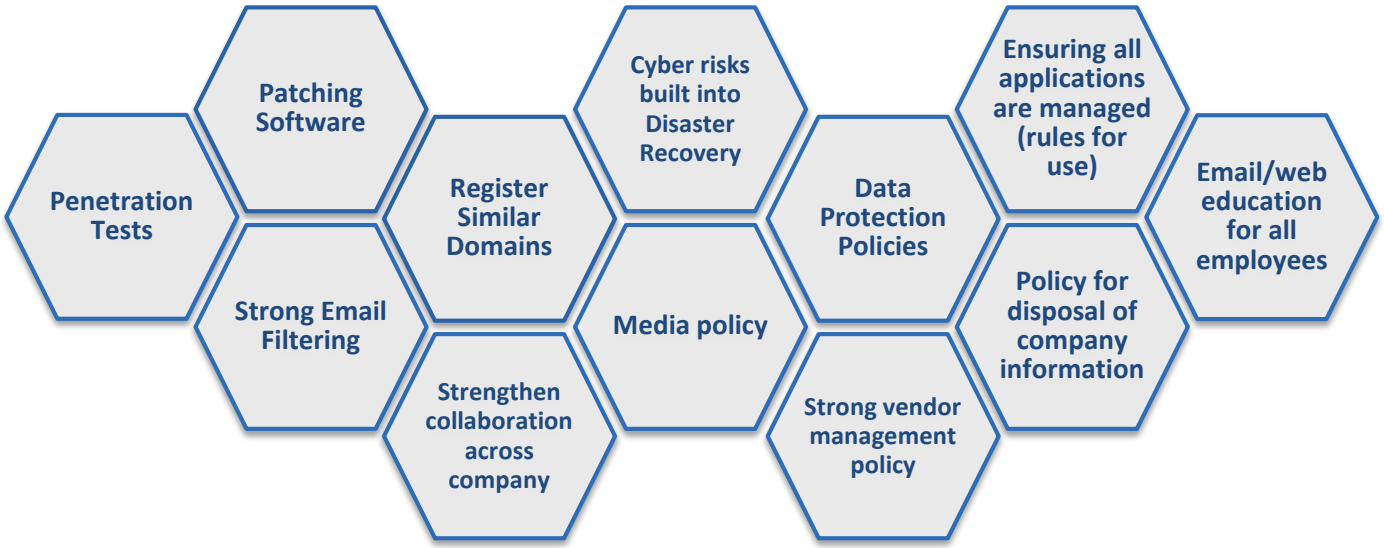
Over 90% of cyber attacks begin with email[1]

- ✓ Constantly sharpen skill level
- ✓ Report phishing emails in addition to detecting
- ✓ Focus effort on most likely risk
- ✓ Use effective videos

1. https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/

Ongoing Evaluation of Your Security Practices

Have you considered…



Passwords

Social Engineering

USE STRONG PASSWORDS

- Use at least 3 random words or 1st letter of expression or poem
- Lower and uppercase letters, numbers and symbols
- Minimum of 8 characters
- Use different passwords for different online and system accounts

NEVER USE PUBLICLY AVAILABLE INFO

- Pet's name
- Other family members' name
- Favorite holiday
- Spouse's name
- Child's name
- Place of birth
- Something related to your favorite sports team

Top Ten Passwords most commonly used

1. 123456
2. Password
3. Welcome
4. Ninja
5. Abc123
6. 123456789
7. 1345678
8. Sunshine
9. Princess
10. Qwerty

EDUCATE your team on best practices

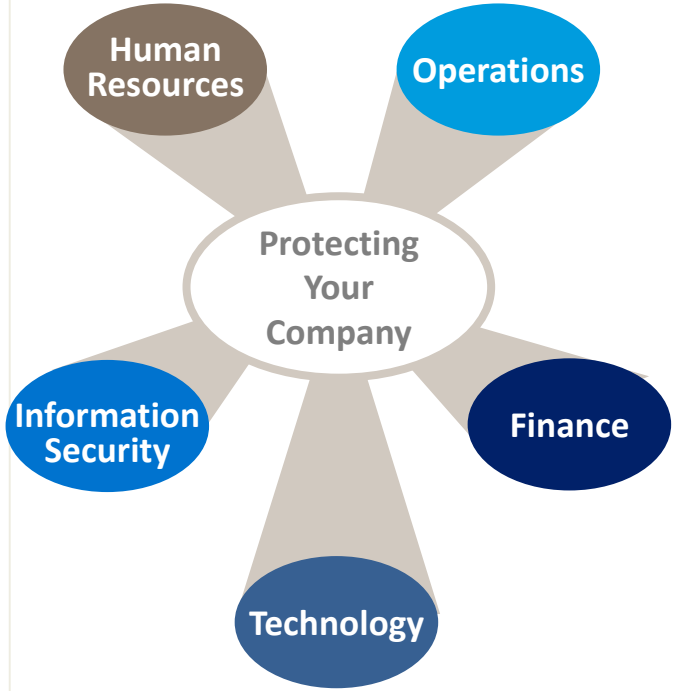
Vendor best practices

What you should know about your vendor

- Who is responsible if information is breached due to vendor action or inaction?
- Who is financially liable?
- Can you shift vendors/resources and recover quickly?

Best Practices

- Perform site review; leverage security and process experts in your company
- Allow vendor access only to required data
- Limit and segregate log-ins to mitigate potential breaches
- Address responsibilities and liability if your vendor becomes compromised and impacts your business
- Understand vendor's loss recovery processes and service level agreements currently in place
- Do your homework – check references, awards, company standards regarding product, data security processes, procedures to ensure balanced risk-reward decision
- Hold your vendor to the same "Best Practice" standards you adopt internally



Incident Response Plan

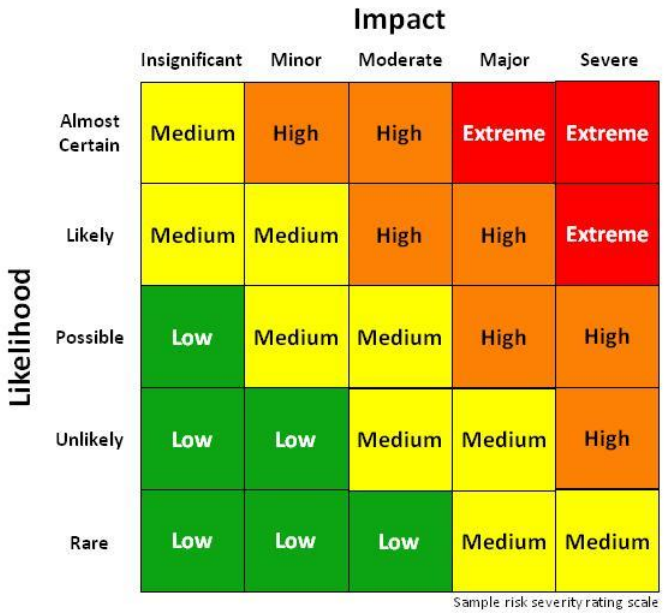
Create plan

- Identify Key Stakeholders
  - Define the role of each Stakeholder
  - Identify event owner
  - Create fraud event playbook

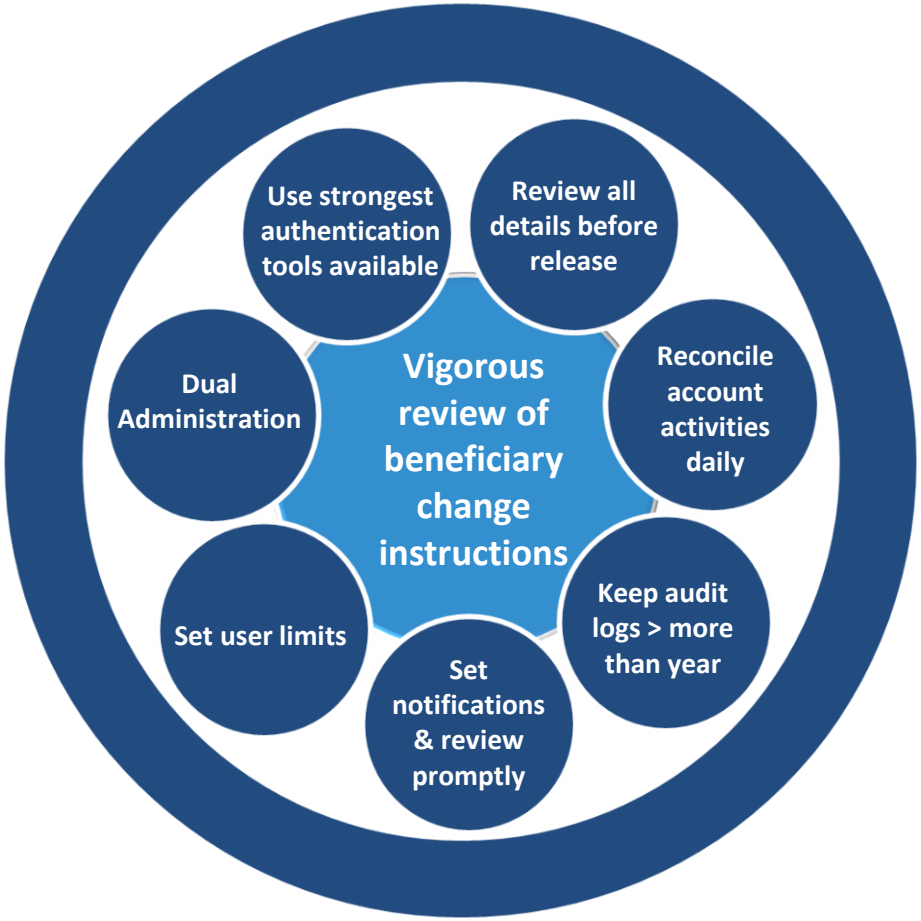
Senior Management	Information Technology	Risk Management
Business Controls	Media Relations	Treasury/ Finance
Legal	Internal Audit	Other Staff

Engage and respond

- Event triggered - fraud action plan engagement
  - Assess the Fraud Risk
    - Is this an active event?
    - What is the severity?
    - What is the financial exposure?
  - Assemble broader team
    - Stop the event – prevent further impact
    - Manage event based on complexity and severity
- Engage external resources where appropriate
  - Financial Institution
  - Forensic Accountant, Security Expert
  - Law Enforcement
  - Vendor



Treasury Best Practices



For the highest level of security, conduct all online banking activities from a standalone, hardened and completely locked-down computer.

Appendix

Bank of America
Merrill Lynch

Social Media, Email and Web Sites

- Don’t reply or click on links in emails, pop-ups or websites that ask for personal, financial, or health information
- Don’t click on links or open files from people you do not know
- PDF files are a very popular way of distributing viruses. Before opening a PDF, be sure you know where it came from
- Don’t send highly sensitive information through unsecure email or texts
- Assume that no public email or text service is secure and that all communication will be stored and potentially viewed by others
- Do not forward internal email, documents or other information to a personal email address or download to personal devices for access outside of your employer’s systems. Your employer can’t protect information outside their domain
- When submitting sensitive information on a website, make sure you see the site’s address begins with “HTTPS” as the “s” stands for secure. HTTPS uses encryption to send information across the internet, thus reducing the risk of being improperly accessed
- Always THINK before you submit. Once you submit to a website the information is public
- There is no such thing as deleting information on the internet as the information is there forever
- Before posting pictures and videos online, remember they may contain GPS data showing where the picture was taken

Be Vigilant

- Be suspicious of calls from unrecognized numbers alleging to be security or other officials asking for confidential information, including account access credentials and passwords. Look up the person calling and call them back at their published number
- Never reveal personal or business account access credentials or passwords in email or telephonically. No valid security personnel will ever ask you to reveal that information using either of these methods
- Be wary of urgent requests to issue checks or take action to avoid some issue without confirming the source
- Monitor the physical security of laptops, smartphones, and other mobile devices.
- Avoid using public internet Wi-Fi to access company systems without use of a secure virtual private network.
- Do not use your personal computer for company business
- If something is suspicious, report it.

Authorized Software

- Do not download or install unauthorized or unapproved software or applications from the Internet
- In particular, never install encryption software, remote access, backup or other similar software without the express approval of your information security personnel.
- Always be certain of the source of downloaded software (i.e., you are actually getting the software from the true creator of the software)
- It is common for hackers to create fake web sites and even “hijack” visitors from official web sites where applications can be downloaded. In some instances, the top search results for a piece of software on Google and other search engines point to disguised hacker web sites where your personal information may be stolen and viruses propagated.
- For your personal computers, make sure you have antivirus and firewall software installed. There are many inexpensive complete security packages available for home systems
- Also, always promptly install security and other updates to your personal computer and mobile device operating systems
- Be mindful of backup applications running on personal devices (e.g., Dropbox, iCloud, Carbonite, etc.) making copies of sensitive company information and storing them online.

Fraud and Security Education

Bank of America
Merrill Lynch

Notice to Recipient

"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, capital markets, 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, 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.

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 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.

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.

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor. No information contained herein alters any existing contractual obligations between Bank of America and its clients

Disclaimer for Brazil

Disclaimer for Latin America