Cyber Security Update

Bank of America Merrill Lynch

October, 2017

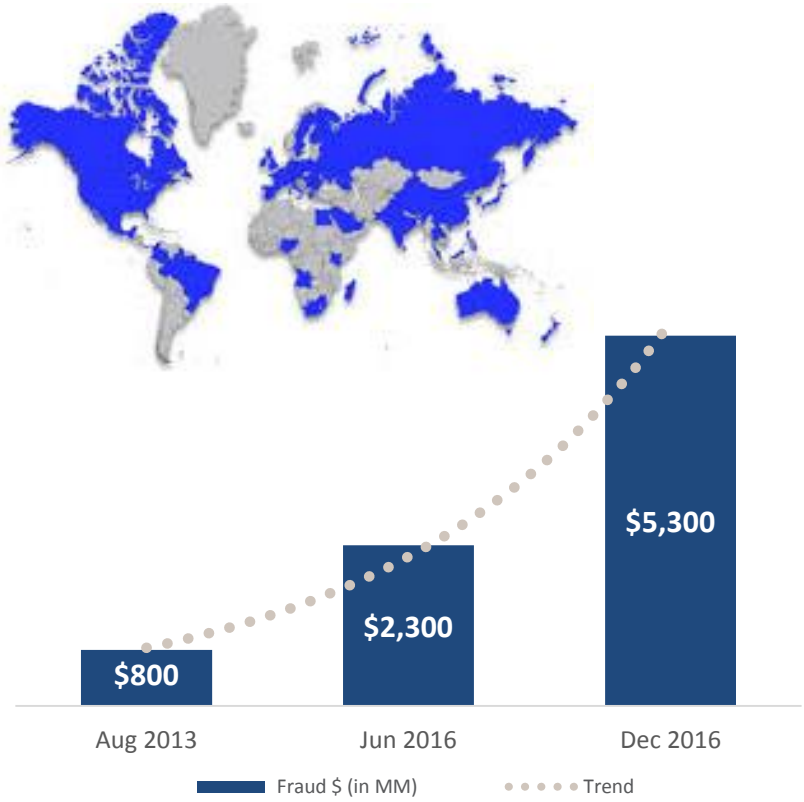
Bank of America
Merrill Lynch

The Threat Environment is Evolving

Bank of America Merrill Lynch

$5.3 Billion

Paid by BEC victims since 2013



Primary destination:
Asian Banks located in China and HK… financial institutions in UK have also been identified as prominent locations

$1 Billion

Paid by ransomware victims in 2016

*"Ransomware has rapidly emerged to become **one of the most serious threats** facing U.K. organisations today. Barely a day passes without fresh reports of yet another major infection, a new variant, or more dire warnings from the authorities.*

*Yet, despite the scale of the problem, **the level of awareness** among organisations and their ability to withstand attacks **is still not enough.**"*

https://www.ic3.gov/media/2017/170504.aspx

Trend Micro: "Ransomware: The Truth Behind the Headlines" September 2016

Fraud Risk in Finance Shared Service Centers

Mitigating the fraud risk

Bank of America Merrill Lynch

The foundation that makes FSSCs attractive -- a process-driven efficiency that rewards speed and volume -- may create blind spots that fraudsters can exploit.

Shared Service Centers Present Challenges

- Transaction mindset
- Mundane job
- Manual controls

Five Way to Mitigate Risk

- Test processes
- Implement fraud prevention training
- Automate manual controls
- Train employees
- Foster the right culture

Single Most Effective Barrier to Fraud

Global end-to-end oversight

https://www.kpmg-institutes.com/institutes/shared-services-outsourcing-institute/events/2013/10/podcast-fraud-risk-fssc.html

SWIFT – Customer Security Program

3 Objectives

YOU
Secure and Protect Your Environment

YOUR COUNTERPARTS
Know and Limit Access – prevent and detect fraud in your commercial relationships

YOUR COMMUNITY
Detect and Respond – continuously share information and prepare against future cyber threats in collaboration with others

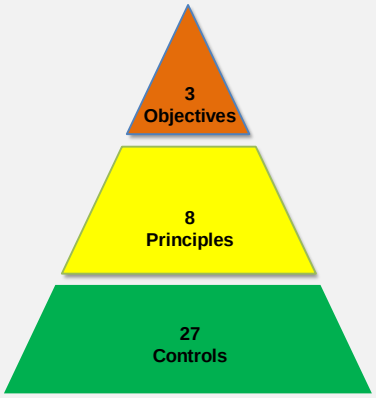
1. Restrict Internet Access
2. Protect Critical Systems from General IT Environment
3. Reduce Attack Surface and Vulnerabilities
4. Physically Secure the Environment

8 Principles

5. Prevent Compromise of Credentials
6. Manage Identities and Segregate Privileges

7. Detect Anomalous Activity to Systems or Transaction Records
8. Plan for Incident Response and Information Sharing

A series of security breaches at banks globally via SWIFT networks triggered the introduction of the CSP.

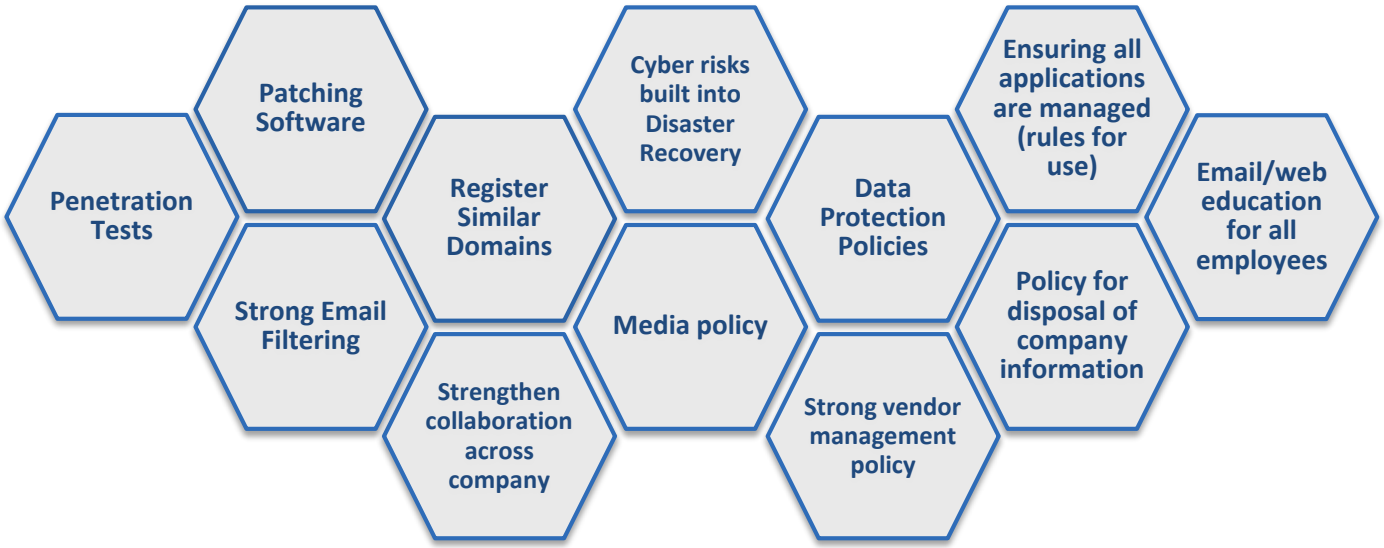


Vendor Best Practices

Bank of America Merrill Lynch

Ongoing Evaluation of Your Security Practices

Have you considered…



Vendor Best Practices

Bank of America Merrill Lynch

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

Firm Wide Planning – Incident Response Plans

Bank of America Merrill Lynch

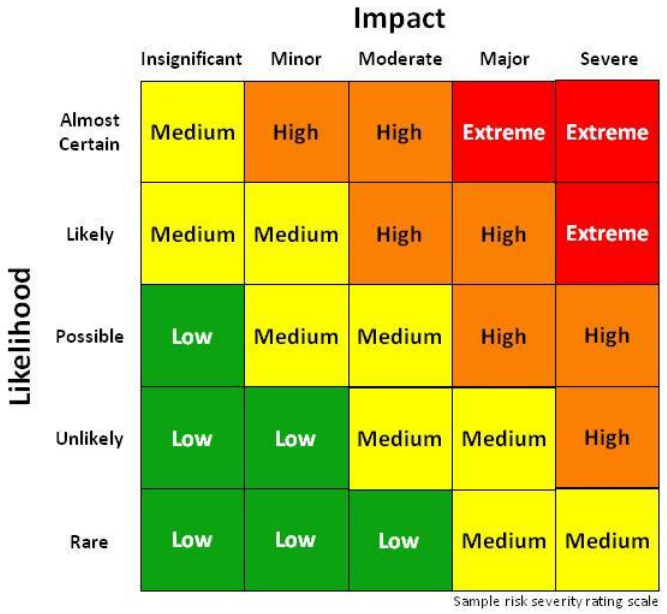
Create plan

- 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



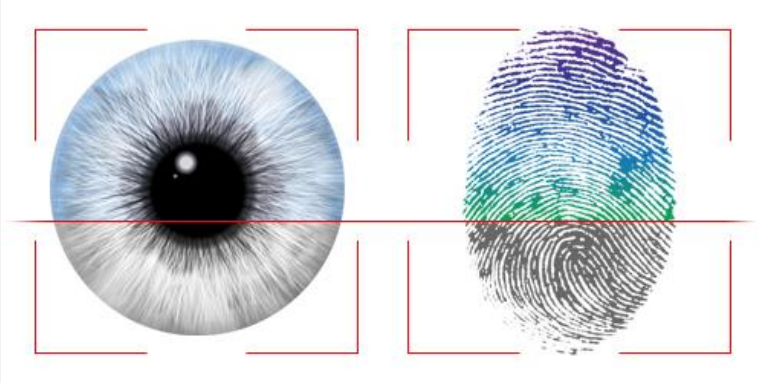
Security and Newer Technology

Bank of America Merrill Lynch

Bitcoin

Cloud computing

Biometrics



Machine learning - AI

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, 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