Treasury Strategies' Quarterly Technology Briefing Cyber Security Risks to Treasury

December 11, 2014

Presented By

Jeff Diorio
Principal

with Special Guests

Linda Haddad
Global Integrated Product Manager
Bank of America

Bob Stark
VP Strategy
Kyriba

Treasury Strategies®

The Power of Experience®

Agenda

Recommendations

- General Process Recommendations
- Treasury Procedures and Technology Recommendations
- SaaS/Hosted Treasury Management System Recommendations
- SWIFT Service Bureau and AL2 Recommendations
- Bank Communications Security Recommendations

Summary

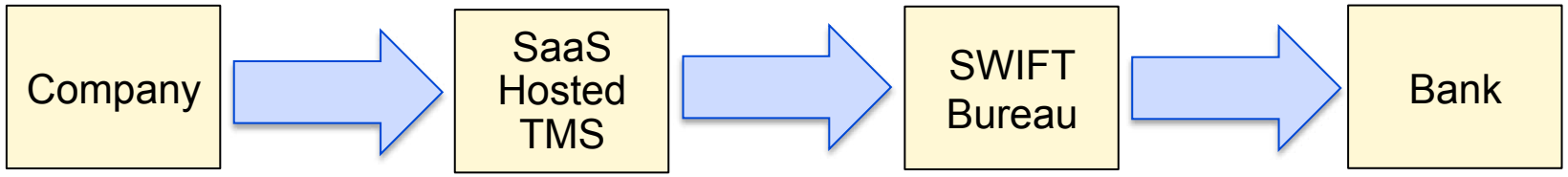
Speakers

Jeff Diorio
Principal
Jeff_Dioro@TreasuryStrategies.com

Linda Haddad
Director, Product Management
linda.haddad@baml.com

Bob Stark
VP Strategy
bstark@kyriba.com

General Recommendations Overview



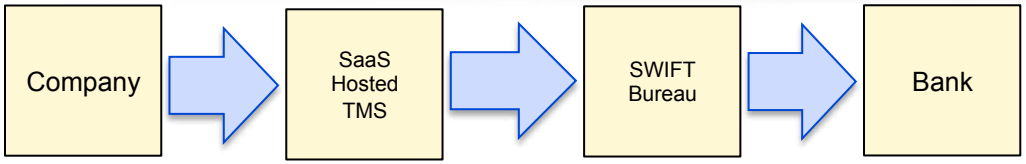
- Who has access to data?
- What users have permission to initiate?
- What are the physical security controls?

- Are transmissions encrypted?
- Are communications unreadable and unalterable?
- Robustness of connectivity

- Authentication of messages and sender
- Alternate initiation plans

Areas of vulnerability:
Boxes are areas you, vendors or banks must be sure are secured.
Arrows are communications channels to be protected.

General Recommendations



Encrypt, encrypt, encrypt

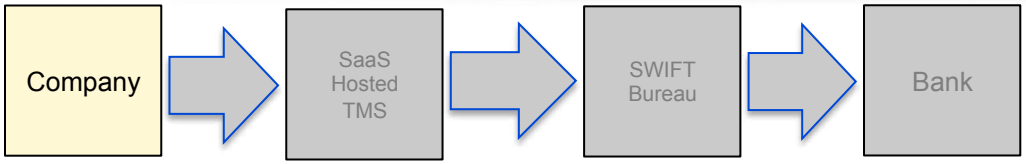
- Data at Rest must be encrypted.
- Data in Flight must be encrypted.

Verification

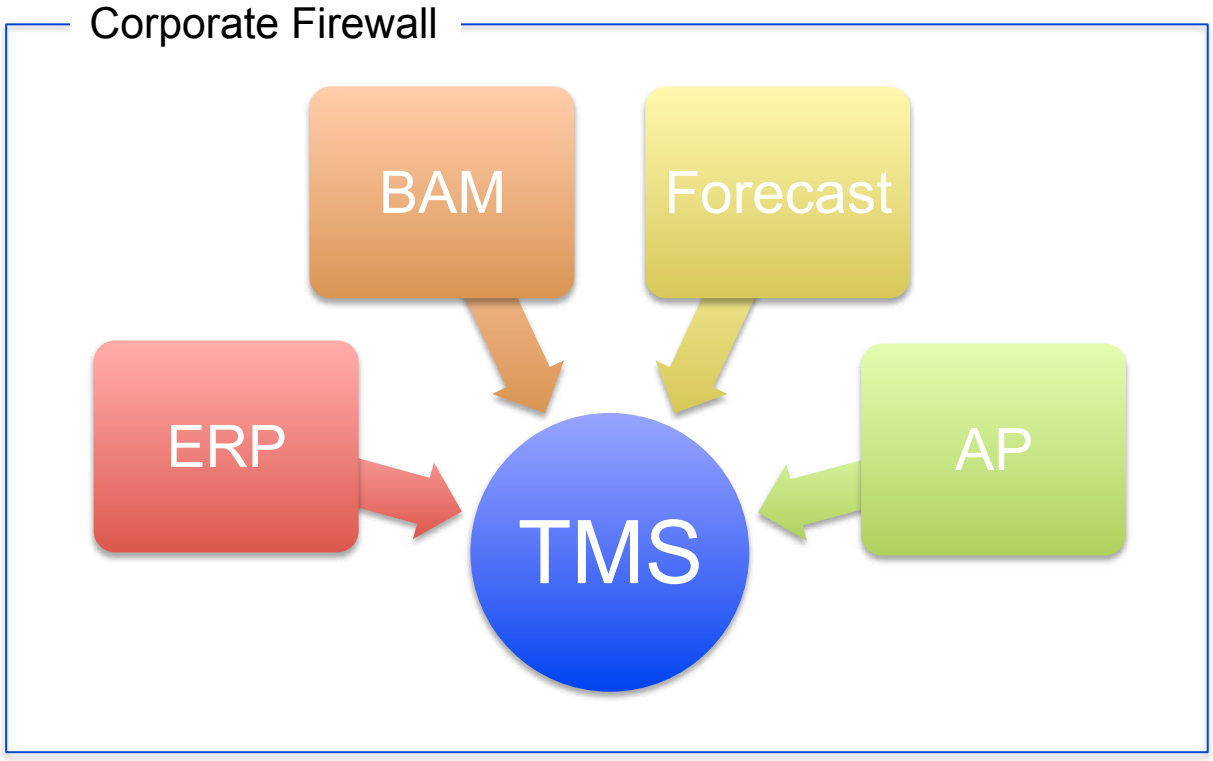
- Acknowledgements/confirmations
- Central frequent monitoring of data and workflows
- Digital signatures (e.g., SWIFT 3SKey), checksum and secondary validation to authenticate payment files

Action plan for breach or incident

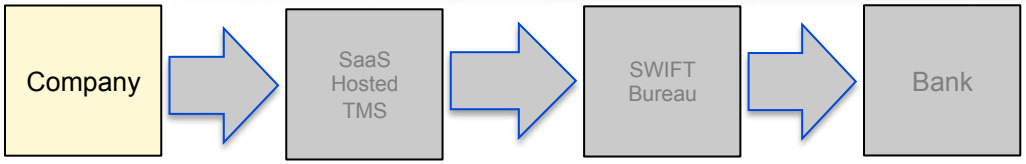
Treasury Recommendations



Analyze security of all systems and locations where you receive or send data.



Treasury Recommendations



Control employee access/visibility in every data location and system.

- Who has rights to change or modify data?

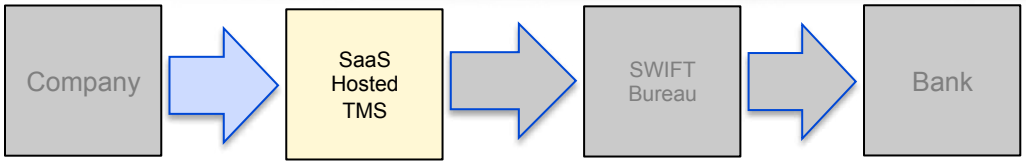
Encrypting inside your firewalls

- Is data encrypted at rest? Databases and files on disk
- Is data encrypted in flight? System backups, email encryption, BAM data

Audit firewalls, data controls, IT Security procedures

- Partner with IT Security and your auditors.
- Consider audits and penetration testing that you will require of a vendor.

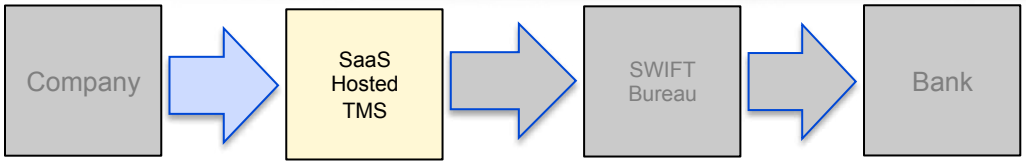
TMS Recommendations
SaaS/Hosted benefits



Benefits of the Cloud

- Physical separation of data from organization's employees
- Encryption of data – in transit and at rest
- Hosting within SOC1-certified data centers (24/7 security, biometric access, etc.)
- Separation of duties and other policy-driven protections to restrict access to hosting infrastructure and client data
- Numerous firewalls to protect externally and between tiers

TMS Recommendations
Hosting security and controls

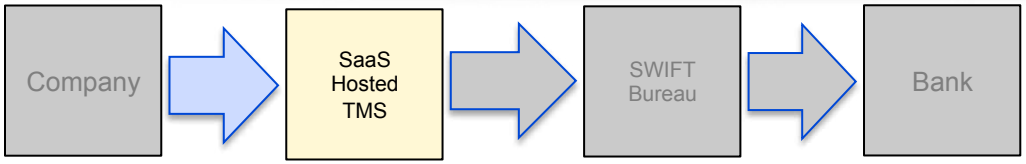


How to evaluate security of your TMS Vendor/Hosting facility

- Involve IT in evaluation because it's difficult for treasury to tell if technology meets standards.
- Understand vendor security process and controls as well as audit results.
- It's not enough to have audit reports since there is no pass/fail.
- There is also a big difference between Type I and Type II reports.

Audit Report/Test	Benefits
SOC1 (SSAE16)	SOC1 is the report; SSAE16 is the standard. SSAE16 is AICPA's "minimum standard."
SOC2	AICPA's recommended report for SaaS and cloud vendors
Penetration Testing	Most vendors outsource to specialists (McAfee, Qualys, etc.).

TMS Recommendations
Connectivity and access



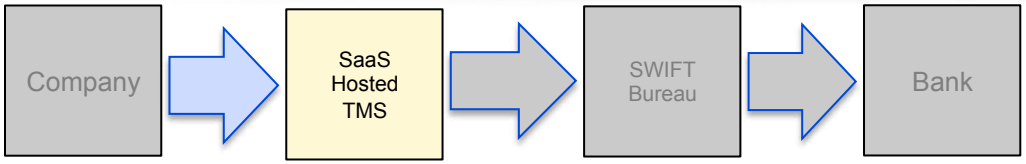
Weak access controls are the easiest entry point to hack a software solution and access data.

Best practice is a multi-layered approach.

- Password timeouts, resets, history, alphanumeric requirements
- Virtual keypads
- Two-factor authentication
- IP filtering
- VPN tunnel

Threats posed by phishing, copying keyboard strokes, and brute-force password attack are reduced.

TMS Recommendations
Application workflow controls



TMS provides for separation of duties and application of limit.

- Dual authorization for payments and flexible limits
- Standardization of approval workflow across all banks and all payment types
- Controls for validation of all system data (transaction and static data)

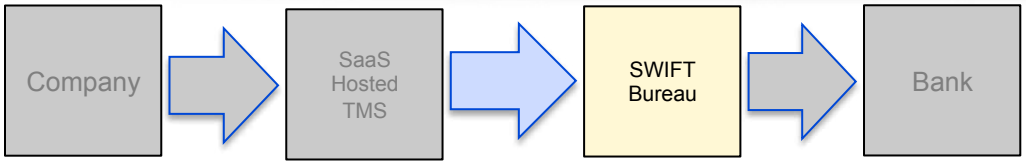
Secondary payment validation like 3SKey

Single sign on or similar user access control

eBAM

- Control point for universe of accounts and signatory control

SWIFT Bureau Recommendations



Communications encrypted

- IPSEC VPN, SSL, 3SKey

Data at Rest encrypted

Audited and SWIFT-certified

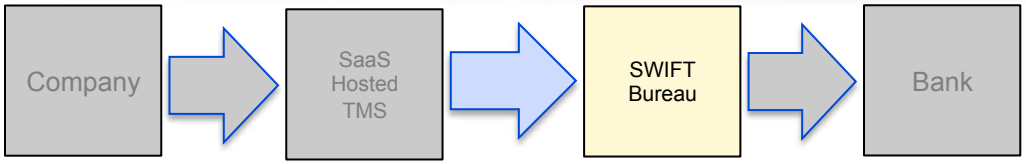
- At least annual audits for SSAE16 and ISO
- Multiple levels SOC1, preferred SOC2
- SWIFT certifications

Dedicated Information Security Team and documented standards

Network Penetration tests (ethical hack)

Critical mass of technical, operational and SWIFT expertise

SWIFT Bureau Recommendations



Other operational/technical best practices

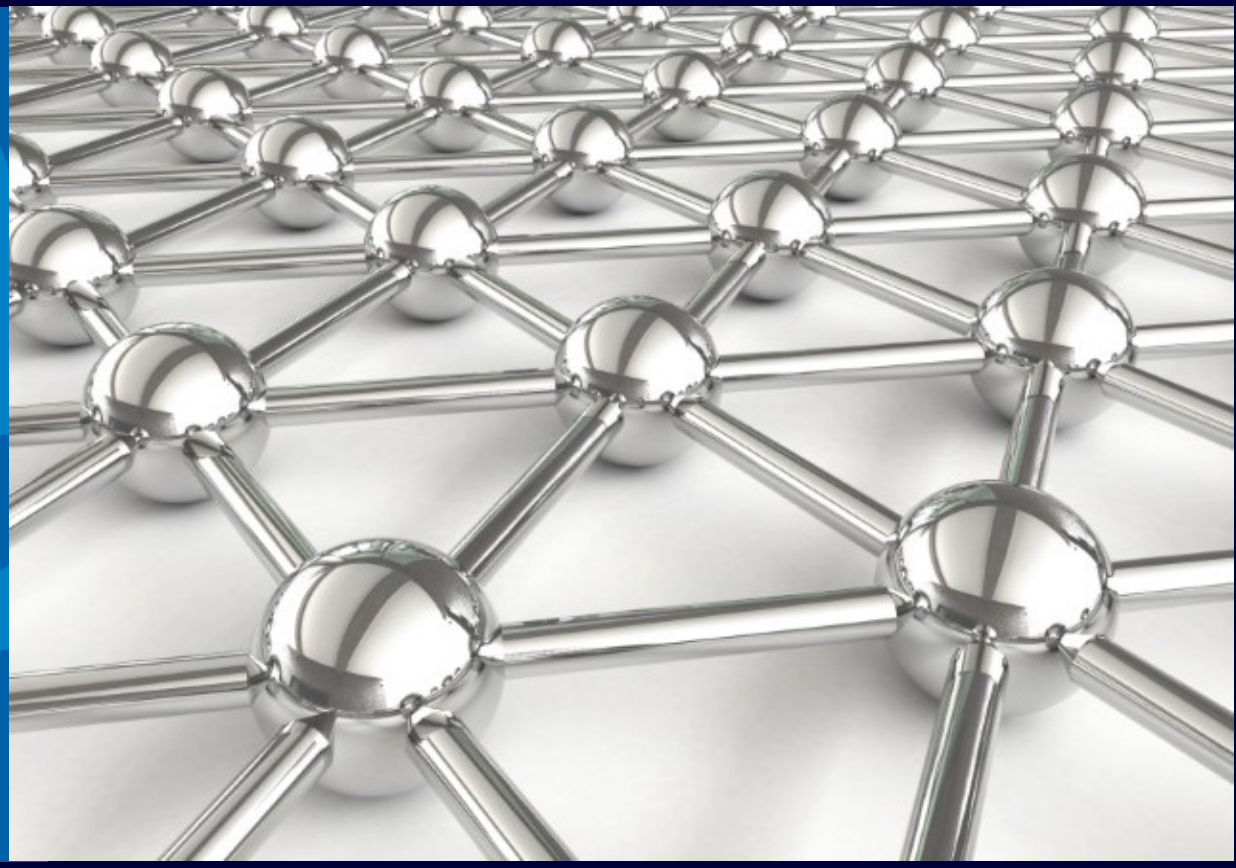
- Intrusion Detection systems
- Data Loss Prevention (DLP) policies and software to protect from data being sent out
- Active monitoring and alerts
- Client visibility to SWIFT traffic and monitoring

Understanding of liability and indemnification coverage

Bank communications security

Linda Haddad
Global Integration Product Manager

December 2014



Bank of America Merrill Lynch

Agenda

- The history of payment fraud
- Trends for bank data security
- 3SKey: Value proposition
- Details on 3SKey

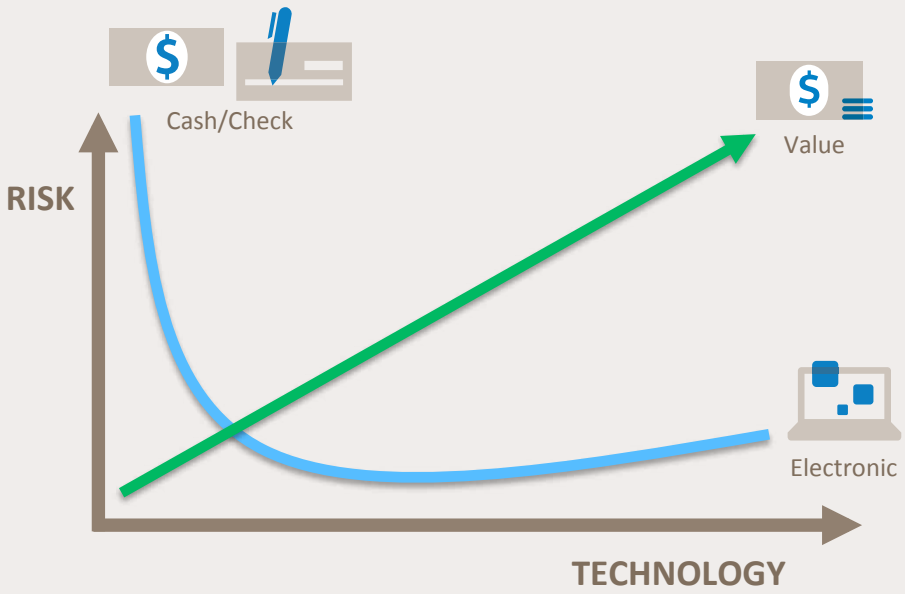



Bank of America
Merrill Lynch

The history of payment fraud

Bank of America Merrill Lynch

Staying ahead of the criminals.



"As the payments system has changed – from cash to checks to credit cards to digital – security continues to be the industry's first priority. What's encouraging is that the system gets more secure with more innovation and technical advancement."

– Brian Moynihan, CEO Bank of America Merrill Lynch

Trends for bank data security

Bank of America Merrill Lynch

- Secure passwords (https/FTP protocols)
- Secured transmission channel such as SWIFT FileAct
- Notifications about file receipt and processing issues
- Test files in test environment with test data only

- Standard PGP encryption
- Double encryption (securing both contents and transmission channel)
- Added control points by digitally signed files with client-private PGP keys or 3SKey tokens
- Restricted access by allowing the bank to push sensitive files directly to the client's server rather than requiring the client to access their mailbox and download files

- Monitored payment file activity transmission status
- Mobile and online payment approvals
- Separation of duties/ entitlements
- Managed 3SKey digital token assignments

SWIFT 3SKey value proposition

Bank of America Merrill Lynch

A multi-bank and multi-channel solution for corporates to securely authenticate and approve operations using digital signatures and strong authentication

Current Challenges

- Internal fraud is becoming more prevalent.
- Compliance and risk dictates stronger access and administrative controls.
- Proprietary bank solutions for authentication are difficult to manage.
- The Echange Télématique Entre Banques et Clients (ETEBAC) bank-agnostic key system in France has been retired and replaced with 3SKey.
- Client managed security/ admin controls for data transmission- based transactions

Industry Trend – Bank-Neutral/Industry Standards

- SWIFT SCORE provides standard connectivity solution across banks.
- Corporate membership doubled since 2009 to over 1K registered corporates.
- Single Access channel simplifies multi bank relationships.
- SWIFT acts as intermediary between the corporate client and the bank for all communication. Added cloud-based offering is through Alliance Lite2.
- ISO 20022 provides common harmonized format across banks.
- It is a fast-growing integration format for payments, information reporting and bank administration.
- Financial Institutions are working together to harmonize ISO 20022 standards for financial transactions.

Solution

- Companies want help to fight internal fraud.
- Companies want tools to manage employee access.
- 3SKey provides tools to manage administration of authorizations at the bank.
- 18 of SWIFT's top 25 banks offering corporate access have adopted 3SKey.[1]

[1] SWIFT for Corporates, Market Adoption Report – Q1 2014

Potential for 3SKey

Bank of America Merrill Lynch

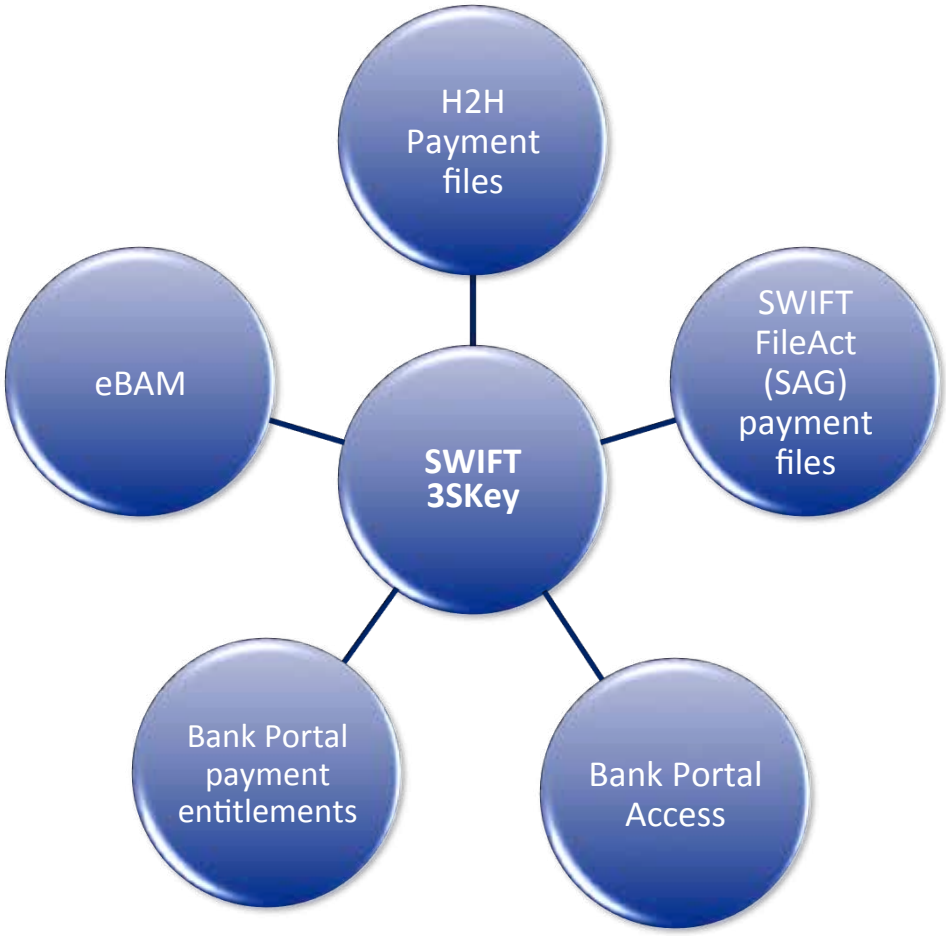
An electronic signature containing unique information specific to an individual that is attached to a message or file to authenticate its source and verify the integrity of its content

Source authentication: Two factors are used to create a digital ID for a user: something they know – **PIN,** and something they hold – **USB Token**. Digital ID authenticates at the individual level, allowing for administrative authorities at the individual user level within a company.

Secure content: The **USB Token** holds a digital certificate identifying the user and an encrypted security key which is used to encrypt the contents of any related message. Any manipulation of the contents of the data or file after signing will invalidate the Digital ID.

Legally-binding technology: 3SKey can support e-signature technology; its ability to authenticate at the individual user level could essentially act as that individual's "legal signature."

Entitlements: 3SKey applies authorities for content and transactions, i.e., limits.



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 as 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. Accordingly, any statements contained herein as to tax matters were neither written nor intended by us to be used and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed on such taxpayer.

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.

Summary

Look at all of the components, partners and communication channels.

- Determine all places where your data originates, is transported, and stored.
- Evaluate both current level of security and existing exposures.

Develop an action plan.

- Review each potential type of breakdown.
- Enhance protection where possible.
- Create response plan for inevitable breach.

Understand liability and insurance.

- Understand your vendors' and banks' liability coverage and your comfort.
- Use insurance riders and/or cyber insurance as an umbrella.
- Be sure monetary and securities are covered.

Bring in a specialist.

Thank you

Jeff Diorio
Principal
Jeff_Diorio@TreasuryStrategies.com

Treasury Strategies
Treasury Technology Practice

Our expertise in treasury best practices, knowledge of technology solutions and unbiased viewpoint provide our clients with an experienced team to guide them through the technology maze.

Clients

- Corporations
- Not-for-Profit Organizations
- Public Sector Organizations
- Technology Vendors

Solutions for Treasury Departments

- Pre-implementation Best Practices Review
- Process Review & Re-engineering
- Gap Analysis with Current Technology
- Corporate SWIFT Connectivity
- Technology Selection
- Technology Implementation & Optimization
- Strategic Roadmap

Solutions for Technology Vendors

- Implementation Resource Partnering
- Functionality Enhancement
- Business Strategy

About Treasury Strategies, Inc.

Who We Are

Treasury Strategies, Inc. is the leading treasury consulting firm working with corporations and financial services providers. Our experience and thought leadership in treasury management, working capital management, liquidity and payments, combined with our comprehensive view of the market, rewards you with a unique perspective, unparalleled insights and actionable solutions.

What We Do

Corporations

We help you maximize worldwide treasury performance and navigate regulatory and payment system changes through a focus on best practices, technology, liquidity and controls.

Treasury Technology

We provide guidance through every step of the technology process – which includes creating a roadmap, selection, implementation and optimization. Our expert approach will uncover opportunities to optimize the value of your treasury through fully integrated technology solutions.

Financial Services

Our experience, analytic approach and benchmarks provide unique consulting solutions to help you strengthen and grow your business.

Locations

Chicago • London • New York

Accreditations

SWIFT Ready Consultancy SWIFT for corporates - 2009

Connect with Us

www.TreasuryStrategies.com/content/networking-communities

@TreasuryStrat