Leveraging technology to prevent fraud and cybercrime

Bob Stark

Vice President, Strategy

kyriba™
Proactive | Treasury | Management

Fraud is a driving concern

- **62%** of organizations have experienced attempted or actual payments fraud[1]
- **34%** of organizations have been subjected to a cyberattack in the last 18 months[2]
- **20%** of corporates report fraud committed by employees[3]
- **92%** of Treasurers think they are 'performing well' in their battle against fraud[4]
- Average = **18 months** before fraud detected[5]

Sources: (1, 2, 3) AFP, 2015; (4) ACT, 2016; (5) ACFE, 2014

kyriba
Proactive | Treasury | Management

CFOs and Treasurers need to ask…

kyriba
Proactive | Treasury | Management

Fraud Prevention

Spear Phishing

- Cybercriminals are specifically targeting…you
- Attacks are quick and lethal; one mistake or exception from policy is all that it takes
- Typically hack your system or convince you to do something

kyriba
Proactive | Treasury | Management

Fraud Prevention – Spear Phishing

Application Security – Protecting access to your system

- UserID/Password should not grant access to the system
- Attacks prey on weak login/authentication – the easiest entry point to hack a software solution and access data
- Require combination of password controls:
  - Password timeouts, resets, history, alphanumeric requirements
  - Virtual Keypad
  - Multi-factor authentication (hard or soft token)
  - IP Filtering
  - Single Sign-On w/ internal IT environment

Fraud Prevention – Spear Phishing

Getting you to do their dirty work

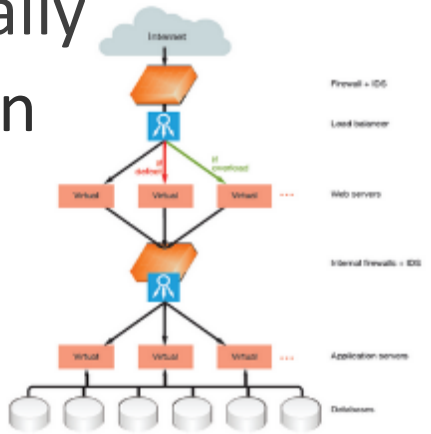
- Business email compromises (BEC) the most popular
- Changing payment instructions is another favorite
- Attacks prey on lack of formal change management process

kyriba
Proactive | Treasury | Management

Fraud Prevention – Data Compromise

Data Security

- IT thinks treasury data is safer hosted externally
- Cloud technology offers more safeguards than internal hosting
  - Encryption of data - in transit and at rest
  - Hosting within audited certified data centers that feature 24/7 security, biometric access
  - Separation of duties & other policy driven protections to restrict access to hosting infrastructure and client data
  - Firewalls to protect externally and between tiers



kyriba
Proactive | Treasury | Management

Fraud Prevention – Data Compromise

Assessing Data Security - Audit Reporting

- Most vendors offer a SOC1 Type II report
- IT often requests a SOC2 Type II report
- Must evaluate details of audit; there is no pass/fail

Report	
SOC1 (SSAE16)	SOC1 is the report; SSAE16 is the standard SSAE16 is AICPA's 'minimum standard'
SOC2	AICPA's recommended report for cloud service providers due to standardized Trust Service Principles
Penetration Testing	Most vendors outsource to specialists (Intel, Qualys, etc.)

Fraud Prevention – Connectivity

Is my bank connectivity safe?

- Recent hacking of payments software has shaken the industry
- Concerns arise about controls surrounding the access points
- Two easy solutions:
  1) Communication to/from banks must be encrypted; no human readable files!
  2) Ensure safeguards of hosted connectivity and service bureaus meet your organization's information security

kyriba
Proactive | Treasury | Management

Fraud Prevention – Bank Accounts

Control of Bank Accounts

- As organizations expand/decentralize, easy to lose control of accounts and signatories
- Need to establish:
  1) Central repository – visibility into accounts, tracking of authorized signers, and one source for documentation
  2) Structured workflows – mandate approval processes to ensure no ‘under the radar’ bank accounts or signatories
  3) Reconciliation procedures – with the bank(s)

kyriba
Proactive | Treasury | Management

Fraud Prevention – Payments

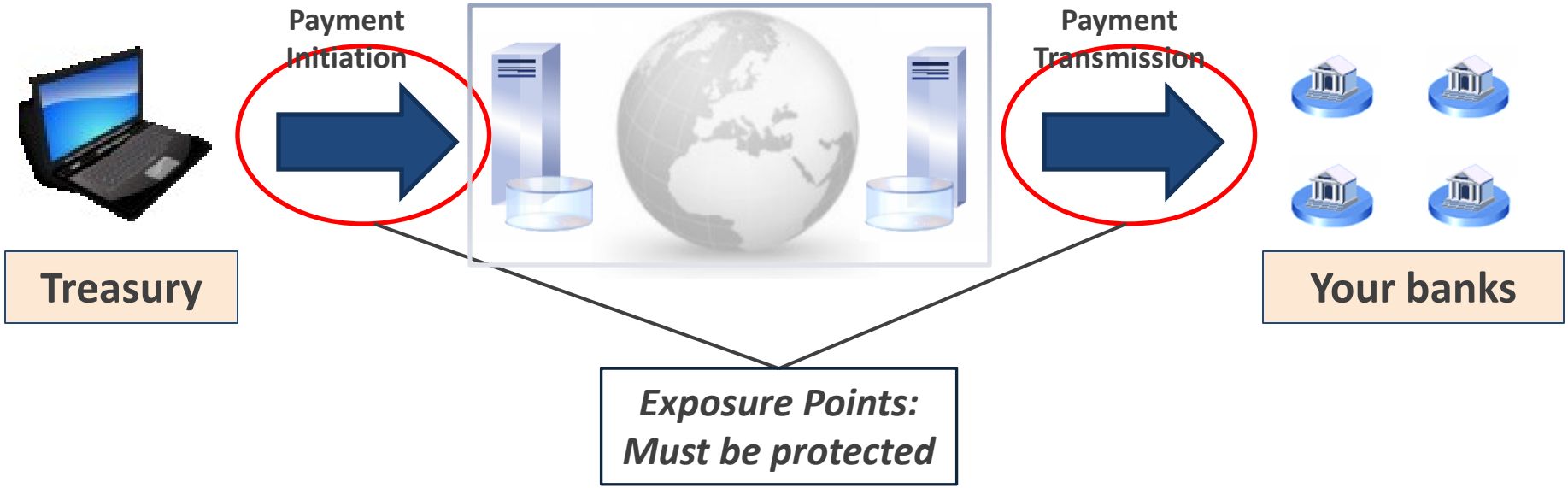
Treasury

Payment Initiation

Payment Transmission

Your banks

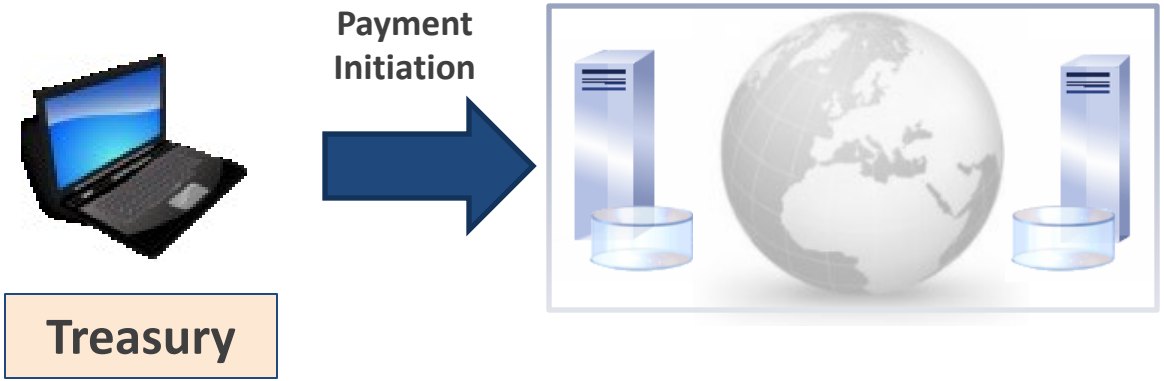
Fraud Prevention – Payments



- Each exposure point → opportunity for cybercrime
- Exceptions to standardized process → opportunity
- Good news: there are good ways to protect!

kyriba
Proactive | Treasury | Management

Fraud Prevention – Payments



- Separation of duties and application of limits are key; Ensure approvals align with dollar limits
- Standardization of approval workflow across all banks and all payment types is important
  - e.g. mandate review of attached documentation

Fraud Prevention – Payments

Payment Transmission

Your banks

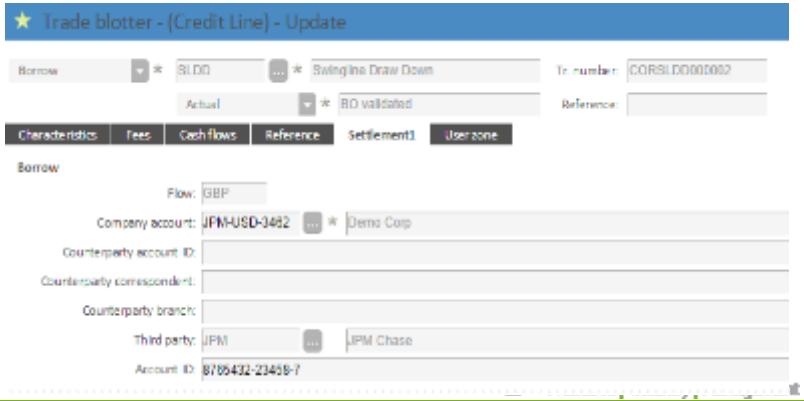
- Payment files to bank must be encrypted
- Acknowledgements/confirmations must be reviewed
- Where available, apply digital signatures (e.g. SWIFT 3SKey) to authenticate exported payment files
- Review payments vs. sanctions lists (e.g. OFAC)

kyriba
Proactive | Treasury | Management

Fraud Prevention – Trading

Trading – settlement instructions

- Standard settlement instructions (SSI) avoid redirection of funds to unauthorized accounts
  - Payment template should be automatically attached to trade and require approval to edit/remove
  - Even harder to audit disparate trading/payment workflows (e.g. initiate trade / walk paper down the hall / initiate payment)



Fraud Prevention – Trading

Trading – making the right trade

- More of an enforcement, than prevention
  - Trade has already occurred when it shows in treasury system
- Use of approvals and limits will help enforce the right behavior
  - Even if you shouldn't have done it, you still have to approve it after
- Also tracking multiple bids per trade is helpful to ensure right bid was selected
  - Also necessary for Dodd-Frank (for the exact same reason)

kyriba
Proactive | Treasury | Management

From prevention….to detection

kyriba
Proactive | Treasury | Management

Fraud Detection

Identifying Fraudulent Transactions

- Review of audit trails will identify specific actions

★ Audit trail - (Referential audit trail -Accounts)

Menu ▶ Filter: none

Entity type	Entity code	Entity number	Action	Description
AD - Define dual administration	Signatory Management-Signer	350354883	Modification	
AD - Define dual administration	Signatory Management-Signer	350354883	Modification	
AD - Define dual administration	Signatory Management-Authorities	350354884	Modification	
AD - Define dual administration	Signatory Management-Authorities	350354884	Modification	
AD - Define dual administration	Signatory Management-Authorities	350354884	Modification	
AD - Define dual administration	Set-up-Account	350354867	Modification	
AD - Define dual administration	Set-up-Account	350354867	Modification	
AD - Define dual administration	Set-up-Account	350354867	Modification	
AD - Define dual administration	Set-up-Third party	350354872	Modification	
AD - Define dual administration	Set-up-Third party	350354872	Modification	
AD - Define dual administration	Set-up-Third party	350354872	Modification	
AD - Define dual administration	Set-up-Company	350354873	Modification	
AD - Define dual administration	Set-up-Company	350354873	Modification	
AD - Define dual administration	Set-up-Company	350354873	Modification	
AD - Define dual administration	Signatory Management-Signer category	350354879	Modification	
AD - Define dual administration	Signatory Management-Signer category	350354879	Modification	
AD - Define dual administration	Set-up-Bank branch	708123898	Modification	
SU - Processtemplate	BANK_CONN	752736461	Modification	Bank Connections
SU - Processtemplate	BANK_CONN	752736461	Modification	Bank Connections
SU - Processtemplate	BANK_CONN	752736461	Modification	Bank Connections
SU - Processtemplate	BANK_CONN	752736461	Modification	Bank Connections
SU - Processtemplate	BANK_CONN	752736461	Modification	Bank Connections
SU - Processtemplate	BANK_CONN	752736461	Modification	Bank Connections
File alert	CSH_FLOW	770794118	Creation	Cash Flow Uplaods
File alert	BK_ST_ALRTQ	770794091	Creation	Bank Statement Upload

kyriba Proactive | Treasury | Management

Fraud Detection

Identifying Fraudulent Transactions

- Daily monitoring of balances and transactions will find suspicious/fraudulent transactions:
  - Daily bank reporting will proactively find suspicions transactions; especially via use of dashboards and automated reporting
  - Daily cash positioning forces review of transaction variances
  - Monthly accounting reconciliation offers same ability, but another checkpoint

kyriba
Proactive | Treasury | Management

Fraud Detection

Identifying Fraudulent Transactions

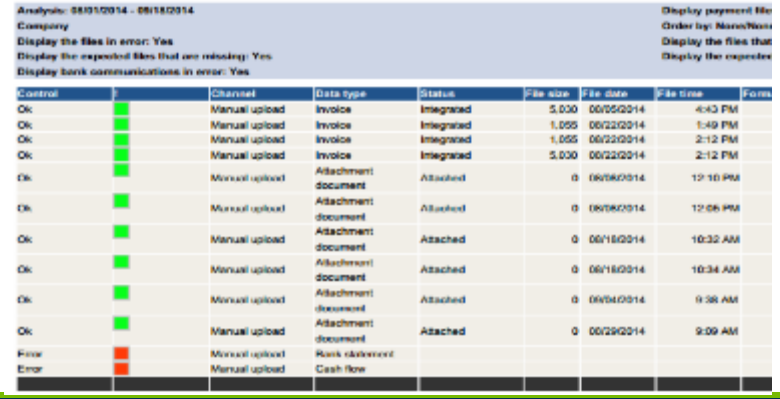
- Separating GL Posting from GL Reconciliation
  - Processes should be separated
  - Same person that created journal entries should not be reconciling those entries
  - Implementing both workflows in same system makes it easier to prove to auditors proper controls are in place

kyriba
Proactive | Treasury | Management

Fraud Detection

Central Monitoring

- Payments to be transmitted to bank
- Internal workflow changes (e.g. limits and approvals)
- Bank Accounts & Signatories
- Daily monitoring & reconciliation of all transactions

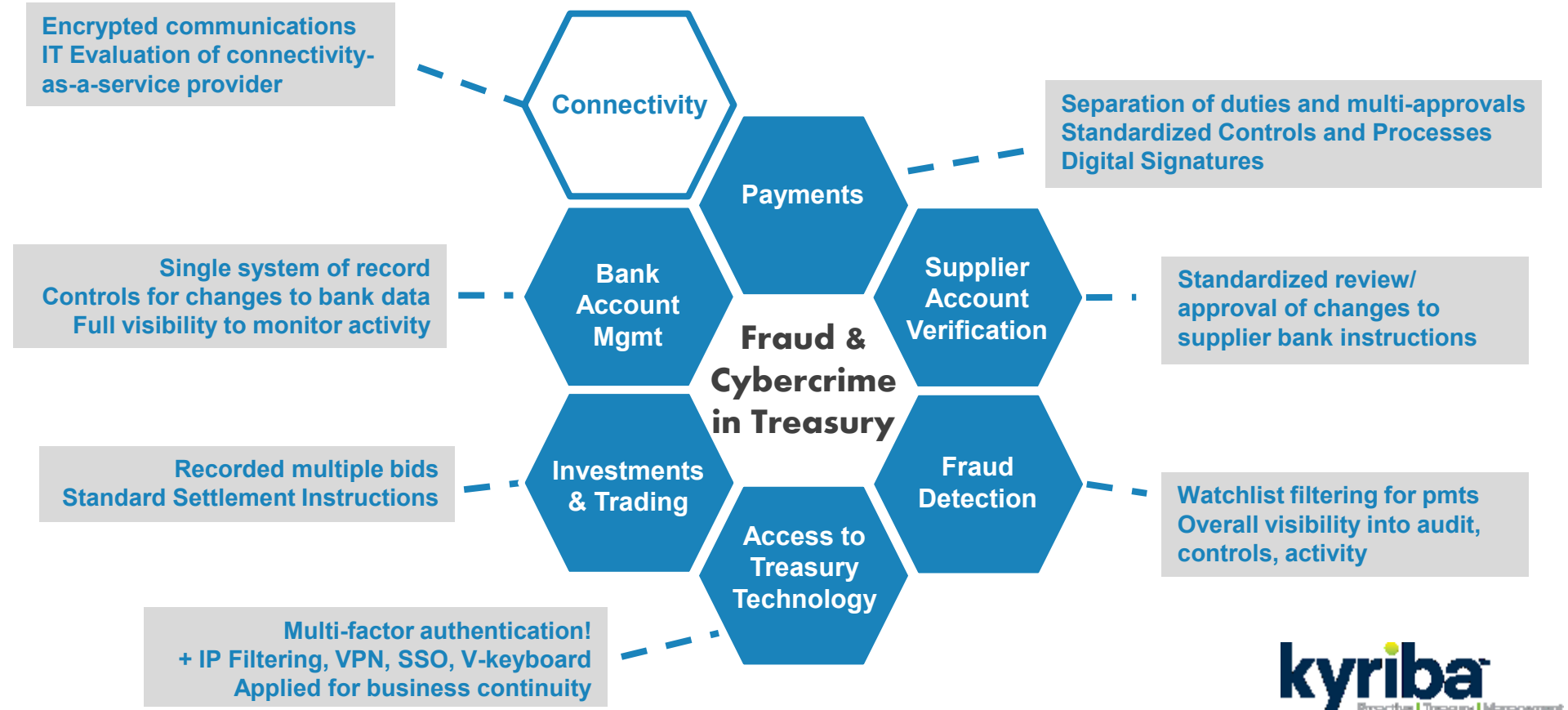


Control		Channel	Data type	Status	File size	File date	File time	Form
Ok		Manual upload	Invoice	Integrated	5,000	06/05/2014	4:43 PM	
Ok		Manual upload	Invoice	Integrated	1,055	06/22/2014	1:49 PM	
Ok		Manual upload	Invoice	Integrated	1,055	06/22/2014	2:12 PM	
Ok		Manual upload	Invoice	Integrated	5,000	06/22/2014	2:12 PM	
Ok		Manual upload	Attachment document	Attached	0	06/06/2014	12:10 PM	
Ok		Manual upload	Attachment document	Attached	0	06/06/2014	12:06 PM	
Ok		Manual upload	Attachment document	Attached	0	06/16/2014	10:32 AM	
Ok		Manual upload	Attachment document	Attached	0	06/16/2014	10:34 AM	
Ok		Manual upload	Attachment document	Attached	0	06/04/2014	9:38 AM	
Ok		Manual upload	Attachment document	Attached	0	06/29/2014	9:09 AM	
Error		Manual upload	Bank statement					
Error		Manual upload	Cash flow					

CFOs and Treasurers need to ask…

kyriba
Proactive | Treasury | Management

CFOs and Treasurers have answers



kyriba
Proactive | Treasury | Management

Questions?

Bob Stark
bob.stark@kyriba.com
@treasurybob

kyriba

kyriba
Proactive | Treasury | Management