
April 29, 2015

# Cybersecurity: Is Your Company Prepared?

Sabine Mcintosh
Managing Director
Global Head of TTS Digital Security and Account Services
sabine.mcintosh@citi.com
+44 (20) 7508-7392

Elizabeth Petrie
Director Strategic Analysis
Information Protection Directorate
elizabeth.petrie@citi.com
+1 (202) 776-1518

# Cyber Attacks—Common Tactics and Impacts on Business

Cyber Attack is an attempt by online criminals to access or damage a computer network/system often stealing data or money, and using both technical and non-technical methods.

CLIENT ADVISORY BOARD

## Common Attack Methods

Human Effect

### Social Engineering

Relying on human interaction to trick people into breaking security procedures and sharing useful information for exploit efforts

Technology

### Malware

Software tools that enable an unauthorized user to gain control of a computer system and gather sensitive information

Human + Technology

### Cyber Masquerading

Taking over executive account to conduct cyber espionage or complete financial transaction

### Phishing

Emails or online posts that masquerade as a trustworthy party in an attempt to trick the target into divulging information or downloading malware

## Impact on Business

**$113 Billion**
Estimated global cost of consumer cybercrime in 2013, or $298 per person[1]

| US | China | Europe | Others |
|---|---|---|---|
| $38BN | $37BN | $13BN | $25BN |

Countries with the greatest number of victims (as % of internet users): Russia (85%), China (77%), South Africa (73%)

**$3 Trillion**
Estimated Cyber Attack Fallout Cost to Global Economy by 2020[2]

1. Symantec: "The 2013 Norton Cybercrime Report"; October 2013.
2. McKinsey report: "Risk and responsibility in a hyperconnected world: Implications for enterprises"; January 2014.



citi

# Cyber Threat Trends Against Financial Centers and Assets

Cyber attackers are increasingly targeting financial centers to steal money and sensitive data. The biggest threat is the combined type of attacks using various tactics.

CLIENT ADVISORY BOARD

| Trends in Cyber Crime | Common Manifestation against Financial Centers |
|---|---|
| **Multi-vector attacks** | Attacks against treasurers are delivered in multiple phases, Using Email, Social Media, unsecure Mobile/Personal devices to log into corporate assets. |
| **Targeted victims** | Caller pretends to be bank's fraud team or Microsoft Help. Victim reveals sensitive information or even allows screen sharing on their machine leading to exploitation and fraud. |
| **Sophisticated tools** | New malware programmers are using sophisticated methods that evade Anti-Virus solutions. Banking malware now features file stealing capabilities. |
| **Indirect attacks** | Attacker targets third-party vendors in order to access sensitive financial center data/systems and steal data/money. |
| **New players: Organized Crime** | Blackmail and Extortion schemes, Data stealing, and even Drug and Human Smuggling is being aided by cyber crime services. |
| **Persistence and long-term outlook** | Advanced tools are added to infected machines to steal valuable intellectual property. |



citi

# Question

## What is the role of Treasury in cyber security?

a) Prevention

b) Detection

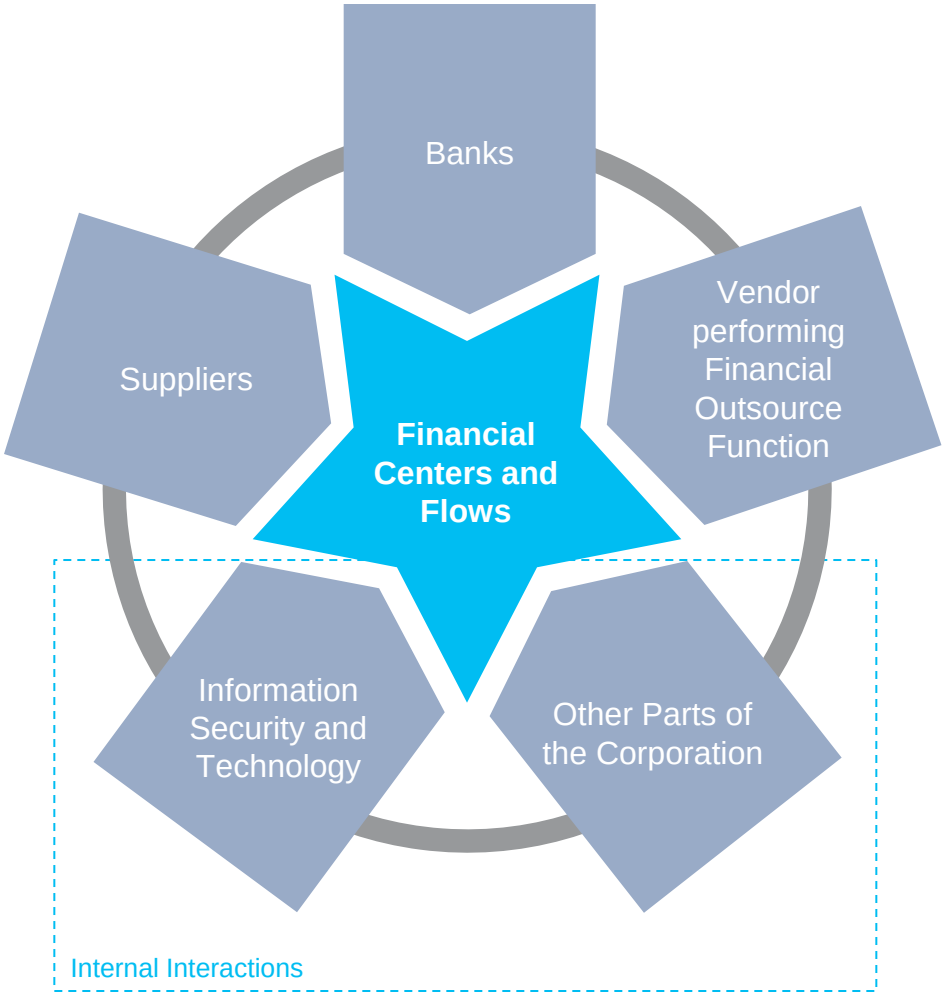
c) Education

d) Mitigation

e) All of the above

# Why is Digital Security Important to Treasurers?

Treasury is at the nexus of a company's financial flows.




## Key Risk Areas

- Human Factors
  - Insider Fraud
  - Access to sensitive data
  - Changing bank details
- Technology/Process Factors
  - Data privacy and sensitive data restrictions
  - Connectivity interacting with banking system
  - Exploitation of security weaknesses in other areas

# Question

In what areas are you concerned about cyber security threats and risks?

a) Electronic Banking

b) Financial Supply Chain

c) None

# Security Best Practices—Within the Financial Center

How to improve internal fraud prevention and react in the face of cyber attacks?

CLIENT ADVISORY BOARD

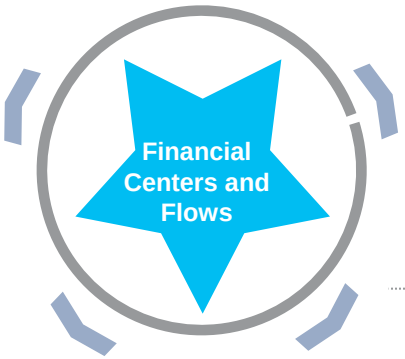
## Prevention

### Monitor Your Internal Controls

- Implement electronic payments for recurring check disbursements
- Use additional levels of control for new payee authentication
- Minimize spare check stock and maintain tight control over inventory
- Conduct surprise audits
- Review exception items and account activity daily

### Manage Your Transaction Controls

- Enable controls around access to systems and data
- Use locked beneficiary templates (preformats) for payments to prevent beneficiary takeover
- Separate deposit and disbursement accounts allowing depository accounts to block all check presentment




### Use Risk Mitigating Human Resource Best Practices

- Promote staff training on cyber threats and fraud awareness
- Periodically rotate staff in financially sensitive assignments
- Separate financial responsibilities amongst staff
- Require staff with financial responsibilities to take mandatory time off
- Ensure hiring procedures include reference checks, background screening

## Post-attack Management and Recovery

- Issue alerts and reminders for staff to know exactly what to do in the event of an actual or potential compromise
- Notify your security officer and your usual bank contact to investigate any suspicious activity
- Act quickly to recover lost funds (Bank can work with you to investigate and attempt recovery of funds)



citi

# Question

## Who is responsible for security in your organization?

a) Information Security

b) Internal Audit

c) Operations Control

c) Everyone

e) None of the above

# Fraud Risk Management

The Fraud Risk Managers Toolkit will be a packaged set of materials that can be used to expand awareness and best practices within the client organization to tackle fraud risks encapsulating both **Social Engineering and Digital Security.**

CLIENT ADVISORY BOARD

## Toolkit Components

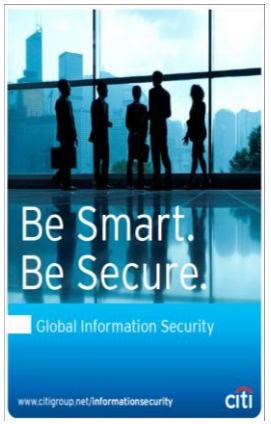
**General**
- Fraud Basics (What is Fraud?) (brochure)
- How to raise Awareness in your organization (slipsheet)
- Fraud Prevention (microsite)
- Posters and placemat

**Fraud Risk Bulletins**
- A series of regular emails to Fraud Risk Managers
- 1. Identify Crisis, 2. Prepare, Prevent, Protect. 3. Lock it up 4. See it. Report it.

**Formal Training materials**
- Classroom session - presentations
- Training Video
- Case Study Scenarios (videos and animation)

**Core Payments materials**
- Cash Management: Cash in Transit, Teller Implant and Mobile Teller Services (slip sheet)
- Manual vs. Electronic Payments(presentation)
- CitiDirect BE Best Practices, video (Video/Slipsheet)

| | |
|---|---|
| **Social Engineering** | Human and physical and psychological elements |
| **Digital Security** | Cyber attacks Payment Flow management |







citi

# Appendix

# Treasurer Fraud Attempt—Impersonation

This is a the general case of how cyber-attacks may target and compromise a senior executive's account to conduct fraud.

CLIENT ADVISORY BOARD

- Treasurer updates Social Networking Site account that he will be speaking at the annual International Association of CFOs and Corporate Treasurers in China

- The Social Networking Site Account is opened by Hacker using online brute force attack to guess the Treasurer's login ID and password

- Hacker makes connections with all associates (e.g. key supplier) holding a Treasurer title linked to that account

- Hacker sends a Social Networking Site message to all associates asking them to click on the link to the upcoming conference that the Treasurer is speaking at

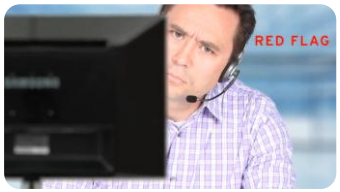
- All associates are infected unknowingly by malware when they click on the link

- Because of the malware infection, the Hacker compromises the credentials for the associate's e-mail account and sends directions to the Treasurer's Account Payable colleague to change vendor bank details and transfer funds

# Treasurer Fraud Attempt—Beneficiary Change

The follow-up scenario demonstrates the tactic of the Hacker to fabricate a change of beneficiary to steal money.

CLIENT ADVISORY BOARD




- Account Payable staff (Mike) notices an email requesting change of bank account details from his supplier (Hacker), and is surprised that the tone is more formal than usual
- Mike replies requiring signature verification call-back
- Supplier replies that he is currently traveling and not available via usual contact number and to work with his trusted colleague Yahon

- Soon after Yahon calls Treasurer (in-bound call) to complete the transaction
- Yahon becomes anxious, aggressive, and responds that Supplier had provided dual authorization by email and instructed him to contact Treasurer
- Mike quickly takes Yahon through the security process given the urgency, and upon his answering of a few questions correctly, confirmed the change of bank details

- Two weeks later, Sam (actual supplier) calls the Treasurer noticing a large overdue payment
- Mike remembers the invoice due to its unusual size as he needed management approval and it was received on the same day as the request to change bank details
- Sam says that they did not change their bank account
- Mike escalates for investigation and finds that payment was effected 4 weeks earlier, soon after the holidays

- Mike explains to Sam that soon after Hacker's email and Yahon's call, an invoice from "ABC Technology" was received right away and paid to the new bank account held with Lucky bank
- Sam confirms that they have never banked with Lucky Bank, and did not request a bank account change
- Mike realizes that he acted on a fraudulent request to change account details

# Treasurer Fraud Attempt—Screen Sharing

This is a social engineering illustration where the fraudster impersonates a Citi helpdesk staff, requesting a client to share screen and conducting fraud.

CLIENT ADVISORY BOARD

- Peter (secondary authorizer) receives a call from Mr Green (fraudster) who wants to speak with Emma (first authorizer)
- Peter re-directs the call to Emma
- Green explains to Emma that he is from Citi Helpdesk calling regarding a CitiDirect BE Java software update
- Emma asked Green to send her an email to confirm he is from Citi, providing Green her email and phone number
- Shortly after, Green sends an email that "appears" to be from citidirect.com

- Green calls Emma again once the email had been received, asking her to open the CitiDirect BE application
- Green then provides an alternative internet address which redirected Emma to a remote sharing website appearing to show CitiDirect BE login
- Green asks Emma to return to the first (genuine) CitiDirect BE login page via Challenge Response
- Green then spends 5 minutes with Emma 'testing', but does not ask her to authorize a transaction

- Green asked Emma to leave the CitiDirect BE session open for 10 minutes and re-direct the call to a transaction maker
- Emma redirected Green to Bob, who was then asked to follow the exact same screen sharing process
- Green asked Bob to leave the session open and re-direct his call to Peter, which he did
- Peter explained to Green that he did not have a CitiDirect BE application on his 'thin client' computer; therefore, Peter was asked to use Emma's laptop to log into CitiDirect BE

- Green explains that the 'updates' have been completed and made a request to Emma and Peter not to use CitiDirect BE until Jan 5 to avoid disrupting the 'server migration'
- On Dec 31, Bob noticed that $800,000 had been debited from their accounts
- Both Bob and Peter simultaneously try to contact Citi and Green to understand why there was a debit on the account
- Citibank responded that there has been no scheduled 'software updates' and that the circumstances were suspicious

# Continuous Innovation to Keep Ahead of the Threat

Citi is leveraging its global Innovation Labs to explore and develop new security solutions.

CLIENT ADVISORY BOARD

## Biometrics

- Voice Biometrics: Evaluate technologies to enable user access via simple verification of their natural speech
- Behavioral Biometrics: Deploy passive log-in tool using client behavior (i.e. typing) that cannot be emulated by external agents

## Device Security

- Malware Detection: Enable passive detection tools to identify viruses
- Information Breach: Advise clients when their private credentials are being publicly distributed by cyber criminals

citi

## Out of Band Security

- Out of Band Authentication: Provide One-Time-Password via SMS, Phone Call or device application, using a channel or device separate from the primary banking channel
- Digital Signature and Transaction Approval: Secure transactions via mobile device separate from desktop banking channel


## Transaction Security

- Payment Risk Manager: Use data analytics tools to identify unusual payment transactions for clients to review prior to execution by Citi
- Risk-based Authentication: Enable simpler security for low risk transactions and complex security for higher risk transactions

The key challenge is to balance user experience, security, and worldwide availability for Citi clients. The above smart experiments may or may not be rolled out



citi

*IRS Circular 230 Disclosure: Citigroup Inc. and its affiliates do not provide tax or legal advise. Any discussion of tax matters in these materials (i) is not intended or written to be used, and cannot be used or relied upon, by you for the purpose of avoiding any tax penalties and (ii) may have been written in connection with the "promotion or marketing" of any transaction contemplated hereby ("Transaction"). Accordingly, you should seek advice based on your particular circumstances from an independent tax advisor.*

Any terms set forth herein are intended for discussion purposes only and are subject to the final terms as set forth in separate definitive written agreements. This presentation is not a commitment or firm offer and does not obligate us to enter into such a commitment, nor are we acting as a fiduciary to you. By accepting this presentation, subject to applicable law or regulation, you agree to keep confidential the information contained herein and the existence of and proposed terms for any Transaction.

We are required to obtain, verify and record certain information that identifies each entity that enters into a formal business relationship with us. We will ask for your complete name, street address, and taxpayer ID number. We may also request corporate formation documents, or other forms of identification, to verify information provided.