June 20, 2017

Cyber Fraud in the Digital Age

Mark McNulty
Global Head of FI Payments and Clearing

Rajesh Shenoy
Global Head of Digital Security

Justin Deck
Senior Cyber Intelligence Advisor

Nathan Chapell
Cyber Strategic Intelligence Analyst
<table>
<thead>
<tr>
<th>What to Remember If You Forget Everything Else</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>The frequency, speed, and effectiveness</strong> of sophisticated cyber attacks continues to increase.</td>
</tr>
<tr>
<td>• “<strong>Bad Actors</strong>” include cyber criminals, nation states, cyber terrorists, and hacktivists…but you also can’t lose sight of the insider threats. While the Advanced Persistent Threat is largely nation-state, some criminal actors also display similar attributes.</td>
</tr>
<tr>
<td>• <strong>Being “intelligence-led”</strong> is the key to long-term success:</td>
</tr>
<tr>
<td>- Know your enemy</td>
</tr>
<tr>
<td>- Know yourself</td>
</tr>
<tr>
<td>• <strong>Cyber security layered defensive strategies</strong> must have a strong prevention component…but no organization can be 100% successful with only a prevention strategy - your ability to detect and respond are equally critical.</td>
</tr>
<tr>
<td>• <strong>People, Process, and Technology</strong> capabilities are needed to combat threats.</td>
</tr>
<tr>
<td>• <strong>Security should evolve</strong> and adapt to emerging cyber risks.</td>
</tr>
<tr>
<td>• Working in <strong>partnership to share information is key</strong> to maintaining end to end security</td>
</tr>
</tbody>
</table>
Cyber Attacks - Impact on Businesses

Estimated global cost of cybercrime, as of Jan 2017\(^1\)

- 2015: $400B
- 2016: $600B

Estimated cost to the U.S. from the theft of intellectual property, as of Feb 2017\(^2\)

- Jan 2016: $17.4M
- Jan 2017: $8.4M
- 2021: $6T

Average annual cost of cybercrime to companies (per organization), as of Oct 2016\(^3\)

1. U.S. $17.4M
2. Japan $8.4M
3. Germany $7.8M
4. U.K. $7.2M

1. Forbes; “(Cyber crime) increasing to almost four times the estimated cost of data breaches in 2015”; January 2016.
The Changing Information Security Threat Landscape

The volume and sophistication of threats are constantly increasing. Organizations must be right all the time, while malicious actors only need to be lucky once.

Key Trends: Multi-vector attacks, Sophisticated Tools, Impersonation, Targeted Victims, Persistence / Long-term Outlook, Business Email Compromise
Cyber Threat Actors

INSIDER
- Motivations vary including fraud, revenge, desire for destruction
- Access is often authorized, making detection hard

NATION-STATE
- Sophisticated actors
- Targeting trade secrets, sensitive information
- Supporting national interests

HACKTIVISM
- Advancement of a social or political agenda
- Attacks often disruptive

CYBER CRIME
- Financially motivated
- Frequent use of social engineering

TERRORISM
- Politically or ideologically motivated
- Goal is to instill fear
- Attacks often destructive
Business Email Compromise

More than **40,000** enterprise victims worldwide

**45%** increase in activity in latter half of 2016

**Two-thirds** of attacks spoofed the victim’s corporate domain

**Actors** routinely leverage authoritarian pressure and a sense of urgency to entice victims into taking action

---

1. FBI, “Business E-mail Compromise E-mail Account Compromise The 5 Billion Dollar Scam”, May 2017.
Business Email Compromise

CEO impersonation is popular in BEC attacks, however, cybercriminals are increasingly targeting victims deeper within organizations. Actors are shifting from CEO-to-CFO scams to CEO-to-different employee groups:

- Accounts Payable for wire transfers or check payments
- Human Resources for personally-identifiable information and wage and tax data
- Engineering for intellectual property theft

1. Hacker discovers CEO is Traveling
2. Hacker emails employee to transfer money. States will be unreachable and act quickly.
3. Employee can't contact CEO
4. Hacker pretending to be legal counsel follows up pressing to act now
5. Transfers funds

2. FBI, “Business E-mail Compromise E-mail Account Compromise The 5 Billion Dollar Scam”, May 2017.
3. FS-ISAC, “Fraud Alert – Business E-mail Compromise Continues to Swindle and Defraud U.S. Businesses “, June 2015
Bridging the Gap Between Crime and Espionage

Carbanak

A sophisticated and specialized cybercriminal group responsible for more than $1B in global losses since 2013.

Advanced Espionage-like Tactics

- Watched system administrators for months
- Altered memory to evade detection

Cyber Attack Lifecycle

- Advanced cyber criminal group: several months
- Typical cyber criminal group: days or weeks

Typical Cybercriminal Group

Emerging Cyber Criminal Monetization Schemes

Deposit & Withdraw

Fraudsters deposit money into account where mule withdraws funds from the bank, not an ATM (due to withdrawal limits).

Convert

Fraudsters send mule a QR code and directions to nearest Bitcoin ATM where the mule converts the cash into Bitcoins.

Movement

Fraudsters use the QR code to complete transaction and receive funds electronically as Bitcoins.

Cyber Security Fusion Center

**Mission** Citi’s Cyber Security Fusion Center (CSFC) is an intelligence-led organization that unifies Citi’s efforts to **prevent**, **detect**, **respond** to, and **recover** from cyber-attacks. Through a culture of collaboration, the CSFC fuses intelligence from a variety of sources to help prevent attacks, reduce risk, and support executive decision-making.

**Strategic Objectives**

- Help prevent and detect cyber-attacks against Citi, its customers, and critical partners
- Reduce Citi’s vulnerability and risk to cyber-attacks
- Minimize damage and attacks through an effective and efficient response effort
- Driving a learning organization to action
Outlook: What to Think About

Outsourcing & Third-Party Relationships

Escalation is Key

The Threat Environment Evolves Quickly

Actors are Patient & Targeting is Long Term

The Importance of Preparation

Information Sharing is Critical
Security Ecosystem – Opportunities and Challenges

1. PREVENT
   - Segregation of Duties
   - Vendor Management
   - Technology Controls
   - Robust Update Program

2. DETECT
   - Staff Training
   - Audits
   - Reconciliations
   - Network Monitoring
   - Vulnerability Assessments

3. RESPOND
   - Manage Responses
   - Effectively Escalate
   - Manage Security Incidents
   - Investigations
   - Testing

4. MITIGATE
   - Intelligence-led Approach
   - Cyber Exercises
   - Threat Intelligence
   - Information Security Enhancements
Challenges and Cooperation in Correspondent Banking

Industry collaboration is key to preventing fraud in correspondent banking.

**Challenges**

**Detection** of fraud through pattern recognition tools has unique challenges in correspondent banking:

- Correspondent banks sometimes lack relationship with ultimate sender and beneficiary
- Patterns of “normal” activity are typically diverse, and difficult to detect potential fraud activity
- Incomplete visibility of payment flows due to multiple correspondents involved

**Response** may be more complex, given nature of flows involved:

- Lack of industry defined standards to confirm validity of transactions
- Potential significant turnaround times for confirmation from various parties
- Potential significant impact of “false positive” on large value cross border payments that may be critical

**Industry Collaboration**

Industry collaboration is needed to address these challenges

**Detection**

- Financial Market Utility-based fraud detection tools can play a role by spanning across the entire flow

**Response**

- Standards and tools adopted across the industry can facilitate response to transactions flagged as suspicious

**Industry Initiatives**

*Industry initiatives* are already being launched:

- SWIFT as part of its “Customer Security Program”
- The Clearing House is launching a working group
**Customer Security Programme**

Launched in 2016 the SWIFT Customer Security Programme supports customers in reinforcing the security of their SWIFT-related infrastructure. SWIFT customers remain responsible for the security of their own environment.

- Secure your local environment
- Prepare for Swift Alliance Access 7.2
- Implement Customer Security Controls Framework
- **Complete self attestation by end 2017**

---

**Your Community**

- Inform SWIFT if you suspect that you have been compromised
- Provide contact details of your company’s CISO for incident escalation
- **Sign up to our Security Notification Service**

---

**Your Counterparts**

- ‘Clean-up’ your RMA relationships
- **Put in place fraud detection measures**
- Engage with us on market practice
Customer Security Controls Framework

1. Restrict Internet access
2. Segregate critical systems from general IT environment
3. Reduce attack surface and vulnerabilities
4. Physically secure the environment
5. Prevent compromise of credentials
6. Manage identities and segregate privileges
7. Detect anomalous activity to system or transaction records
8. Plan for incident response and
   - Applicable to all customers and to the whole end-to-end transaction chain beyond the SWIFT local infrastructure
   - Mapped against recognised international standards – NIST, PCI-DSS and ISO 27002
   - 16 controls are mandatory, 11 are advisory
   - Self attestation submitted by end 2017
Daily Validation Reports - available now

Activity Reports
View aggregate daily activity, maximum value of single transactions and comparison to daily averages
View your outbound activity >>
<table>
<thead>
<tr>
<th>Message type</th>
<th>Messages sent</th>
<th>Amount (cumulative)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MT103</td>
<td>2,000</td>
<td>273,523,982.30</td>
</tr>
<tr>
<td>MT203</td>
<td>1,215</td>
<td>50,047,000,000.00</td>
</tr>
<tr>
<td>MT203C</td>
<td>133</td>
<td>5,572,124.00</td>
</tr>
</tbody>
</table>

View your inbound activity >>
<table>
<thead>
<tr>
<th>Message type</th>
<th>Messages received</th>
<th>Amount received (cumulative)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MT103</td>
<td>1,034</td>
<td>369,756,161.71</td>
</tr>
<tr>
<td>MT203</td>
<td>50</td>
<td>2,614,469,335.00</td>
</tr>
<tr>
<td>MT203C</td>
<td>134</td>
<td>2,706,831.25</td>
</tr>
</tbody>
</table>

Risk Reports
Highlight large or uncharacteristic payments flow and identify new relationship combinations
View your outbound risk >>
<table>
<thead>
<tr>
<th>Message type</th>
<th>Currency</th>
<th>Amount (cumulative)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MT103</td>
<td>USD</td>
<td>49,562,367.15</td>
</tr>
<tr>
<td>MT203</td>
<td>EUR</td>
<td>48,993,200,171.46</td>
</tr>
<tr>
<td>MT203C</td>
<td>DKK</td>
<td>12,364,890.17</td>
</tr>
</tbody>
</table>

View your inbound risk >>
<table>
<thead>
<tr>
<th>Message type</th>
<th>Currency</th>
<th>Amount (cumulative)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MT103</td>
<td>USD</td>
<td>55,182,394.04</td>
</tr>
<tr>
<td>MT203</td>
<td>EUR</td>
<td>23,986,977,910.85</td>
</tr>
<tr>
<td>MT203C</td>
<td>DKK</td>
<td>5,204,671.22</td>
</tr>
</tbody>
</table>

Payment Controls – coming in 2018

SWIFT CSP | Your Counterparts – Prevent and Detect

Your Community
Customer Security Programme
Secure and Protect
Share and Prepare

Your Counterparts

Prevent and Detect

Daily Validation Reports - available now

Payment Controls Engine
Release / Abort

SWIFT Network
SWIFT CSP | Your Community – Share and Prepare

Register your CISO and sign-up to Security Notifications

Your Community

Customer Security Programme

Secure and Protect

Your Counterparts

Prevent and Detect

You

Share and Prepare

SWIFT Customer Security Programme

May 2017

Customer Security Programme

SWIFT’s customer security programme – a thousand birth - help customers enhance the security of their SWIFT networks and infrastructure against cyber threats.

www.swift.com

Access mySWIFT

Press

Ordering & Support

Hires

SWIFT Newsletters

Register for updates and stay informed on the latest SWIFT news.

Subscribe
Quick Tips

1. **Controlled Payments Environment:** Securing the infrastructure of any payments system is a critical control, for example at the **machine level** (controls such as anti-virus software, limiting USB port access) and the **network** it is connected to (controls such as proper firewalls, intrusion detection).

2. **Application Updates:** Software, including applications responsible for connectivity to SWIFT and other payments systems and channels, should always incorporate all required upgrades and patches, installed in a timely manner.

3. **Third Party Management:** Security controls should extend outside of your organization as well as to the broader ecosystem of vendors, partners, and other third parties.

4. **Multi-Factor Authentication:** Any system that can be used to initiate or amend a payment transaction should be subject to a **maker/checker process**, and a **multi-factor authentication process**. Multi-factor authentication is a practice of requiring two or more authentication steps in order to access a system. For example, requiring not only a user password but also an additional authentication mechanism in order to access a system (mechanisms like: one time password token, SafeWord card, biometrics).

5. **Timely Reconciliation:** Timely reconciliation processes can help quickly identify potential fraudulent payments, which can assist in the attempted recovery of funds issued.
Action Steps for Fraudulent Activity

1. Send an urgent MT199 with relevant payment details.

   ![Sample MT199 Message]

   1CITIUS33CXXX53036
   1CITIGB2LAXXX76152
   199 02
   :20:ABC123REF
   :21:XYZPAYMENTREF
   :79:ATTN INVESTIGATIONS TEAM
   WE SENT THE ABOVE PAYMENT UNDER OUR
   REFERENCE
   XYZPAYMENTREF VALUE DATED 08 AUG
   2016 PLEASE BE ADVISED THIS IS A
   FRAUDULENT PAYMENT WE ARE
   REQUESTING IMMEDIATE CANCELLATION
   OR RECALL

2. Immediately follow-up with a phone call or email to your Citi contact — relationship manager, CitiService contact, or account manager

   * Provide further details on fraudulent attack (i.e., unique payment, multiple transactions, attack within your infrastructure or on your client’s side, etc.)

3. Maintain contact with Citi to receive and provide frequent updates
Citi’s Fraud Awareness Toolkit

The Fraud Risk Managers Toolkit provides best practices to tackle fraud risks, encapsulating both Social Engineering and Digital Security.
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.

© 2017 Citibank, N.A. All rights reserved. Citi and Citi and Arc Design are trademarks and service marks of Citigroup Inc. or its affiliates and are used and registered throughout the world.