Cybersecurity & Fraud Prevention in Today’s Digital Marketplace

December 2016
The Anatomy of a Cyber Attack & Best Practices in Information Security

December 2016

Justin Deck
Citi’s Strategic Intelligence Analysis Group
What to Remember If You Forget Everything Else

• The frequency, speed, and effectiveness of sophisticated cyber attacks continues to increase.

• “Bad Actors” include cyber criminals, nation states, cyber terrorists, and hacktivists…but you also can’t lose sight of the insider threats.

• Being “intelligence-led” is the key to long-term success:
  - Know your enemy
  - Know yourself

• Cyber security layered defensive strategies 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.

• People, Process, and Technology capabilities are needed to combat threats.

• Security should evolve and adapt to emerging cyber risks.

• Working in partnership to share information is key to maintaining end to end security
Cyber Attacks - Impact on Business

A **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.

$2 Trillion
Estimated global cost of cybercrime by 2019\(^1\)

$242 Billion
Combined cost to top three global economies\(^2\)

Total cost of cybercrime to companies\(^3\)

- **US**: $117M
- **All others**: $204BN
- **US**: $15.4M
- **UK**: $6.3M
- **Japan**: $6.8M
- **Germany**: $7.5M
- **China**: $71M
- **Germany**: $54M
- **Others**: $204BN

---

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 is increasing. Whereas criminals only need to succeed once, Institutions cannot afford one failure.

Key Trends
- ✓ Multi-vector attacks
- ✓ Targeted victims
- ✓ Sophisticated tools
- ✓ Persistence / long-term outlook
- ✓ Impersonation
- ✓ Business Email Compromise

Perpetrators were individuals.
Their actions were opportunistic and casual.
Their desire was to “prove that they can”.

Typically perpetrators were still individuals.
But their actions were premeditated and planned.
And their desire was for financial gain.

Perpetrators consist of organised syndicates, criminal enterprises and nation states.
Their actions are not only coordinated: they are also well funded.
Perpetrators are driven by opportunities for geopolitical and financial gain.
And they are acting with an increasing focus on disruption and destruction.
<table>
<thead>
<tr>
<th>Cyber Threat Actors</th>
<th>Nation-state</th>
<th>Cyber Crime</th>
<th>Terrorism</th>
<th>Hacktivism</th>
<th>Insider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sophisticated actors</td>
<td>Financially motivated</td>
<td>Politically or ideologically motivated</td>
<td>Advancement of a social or political agenda</td>
<td>Motivations vary including fraud, revenge, desire for destruction</td>
<td></td>
</tr>
<tr>
<td>Targeting trade secrets, sensitive information</td>
<td>Frequent use of social engineering</td>
<td>Goal is to instill fear</td>
<td>Attacks often disruptive</td>
<td>Access is often authorized, making detection hard</td>
<td></td>
</tr>
<tr>
<td>Supporting national interests</td>
<td></td>
<td>Attacks often destructive</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Anatomy of a Cyber Attack

- RECON
- Initial Compromise
- Establish Foothold
- Escalate Privileges
- Internal Recon
- Move Laterally
- Expand Presence
- Exfiltrate Data
- Maintain Presence
Citi is facing a must-win battle against sophisticated cyber adversaries. The mission of Citi Global Information Security is to prevent, detect, respond to, and recover from cyber attacks. Citi does this by implementing an intelligence-led strategy to protect the firm’s data, assets, people, and reputation.

Intelligence-Led Information Security
A business model and managerial philosophy where analysis and intelligence are pivotal to an objective, decision-making framework that facilitates information protection through effective implementation of strategies that target prolific and serious threat actors and their methods.
**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 prevent attacks, reduce risk, and support executive decision-making.

**Strategic Objectives**

- 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
Protect Citi, its Customers, and Critical Partners

A Team of Teams

The CSFC brings together experts from 11 teams across Citi’s Information Protection Directorate (IPD), Citi Security & Investigative Services (CSIS), Citi Technology Infrastructure (CTI), and Global Consumer Business (GCB) to form a “team of teams”. This approach enables effective collaboration, information sharing, and strategic intelligence analysis to support, enhance, and contribute to Citi’s security risk decision-making. Through a culture of collaboration, the CSFC fuses intelligence from a variety of sources to detect threats, reduce risk, and support executive decision-making.

Citi’s Intelligence-led Approach to Information Security

Intelligence-led means not just storing facts; it is taking those facts and using them to build a story. It is viewing the resolution of one isolated incident not as the end of a threat, but as the beginning.

Talent, Technology, Tradecraft

The CSFC’s greatest strength is its talent – Citi employees who are dedicated to protecting Citi and the financial sector from cyber threats. The CSFC continually seeks to include greater representation from Citi’s business lines to promote a “whole of enterprise” approach to information security. It also seeks to further refine its analytical methodologies, implement new technologies, and most important, grow professional development by cultivating human judgment to reduce the risk of successful cyber-attacks against Citi.
Fraud prevention requires controls and partnership.
Questions
Business Email Compromise
The 3.1 Billion Dollar Scam

Nic White
Global Fraud Prevention
Prior to the attack, the fraudster will spend 3-9 months identifying their target, completing intelligence gathering, identifying an attack date and creating a credible scenario.

“They have excellent tradecraft, and they do their homework. They use language specific to the company they are targeting, along with dollar amounts that lend legitimacy.”

“To make matters worse, the criminals often employ malware to infiltrate company networks, gaining access to legitimate e-mail threads about billing and invoices.”

The FBI - BEC An Emerging Global Threat, August 2015

Compromised Email

Spoofed Email

Look-a-like Email

XYZ@Citibank.com
XYZ@Citii.com
Although BEC scams continues to evolve, there are three primary variations currently being used.
Developing a Layered Defense

To ensure your business is sufficiently protected, it’s essential to create a layered defense utilizing security best practices recommended by the Industry & law enforcement.
Best Practices – Prevent

Preventive measures help strengthen your controls to reduce fraud exposure

**People**

**Educate your team**
- Deliver regular fraud training for all staff, including BEC awareness
- Encourage employees to be inquisitive and to follow their instincts
- Educate executives to be supportive of employees double checking requests

**Add a second pair of eyes**
- Introducing a second person to check a transaction helps identify anomalies and prevent errors

**Process**

**Limit access**
- Restrict the numbers of people who are authorized to send payments
- Remove system entitlements that employees don’t need

**Plan for high risk scenarios**
- Create a different process for anything marked *urgent, secret or confidential*. Or requests that state ‘*no further verification is needed*, ‘*I am travelling*’ or ‘*I am unavailable for a call back*’

**Think twice before posting**
- Be careful what is posted to social media and company websites, especially job descriptions, hierarchical information and out-of-office / travel details

**Technology**

**Strengthen your perimeter**
- Avoid using free web-based email accounts for business purposes
- Restrict access to social network sites and personal email accounts at employee work stations
- Consider registering domain names that are similar to actual domain and could be used for look-a-like emails

**Utilize CitiBusiness Online’s controls**
- Designate a system administrator to oversee the controls
- Implement dual approval and dollar limits for wire transfers
- Setup email / text notifications for significant activity
Best Practices – Detect

Detective measures help you recognize unusual activity and identify potential attacks

<table>
<thead>
<tr>
<th>People</th>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Look for common red flags</td>
<td>Make sure to check the request</td>
<td>Spot an intrusion</td>
</tr>
<tr>
<td>- Emails that contain unusual wording, a different tone or are sent at a strange time</td>
<td>- Perform call backs for any requests to send a payment to a new beneficiary</td>
<td>- Regularly update Anti-Malware and Anti-Virus protection</td>
</tr>
<tr>
<td>- Requests that arrive with a different email format, font or letterhead</td>
<td>- Do not perform call backs to new or temporary telephone numbers</td>
<td>- Install operating system (OS) updates and software patches as quickly as possible</td>
</tr>
<tr>
<td>- Check email addresses closely; verifying the full address and not just the shortened name</td>
<td>- Make sure you know the person you are calling, avoid calling new or unknown contacts</td>
<td>- Implement anti-phishing controls, such as flagging e-mails sent from similar domain names</td>
</tr>
<tr>
<td>- Consider the consistency with previous requests, for both suppliers as well as business executives</td>
<td>- Do not accept an inbound call in place of a call back</td>
<td>Up your guard</td>
</tr>
<tr>
<td>- Be cautious of requests that coincide with business travel dates, on a Friday afternoon or immediately before public holidays</td>
<td>Monitor your account</td>
<td>- Many victims of BEC have reported ransomware or scareware intrusions prior to attack. If you’ve already suffered a breach, prepare for further attacks</td>
</tr>
<tr>
<td></td>
<td>- Complete regular account reconciliation (at least once per day) to identify suspicious activity</td>
<td></td>
</tr>
</tbody>
</table>
Best Practices – Respond

Reactive and recovery measures help you mitigate the impact of an incident and minimize potential / future losses

People

Prepare for the worst
- Issue alerts and reminders for staff to know exactly what to do in the event of a potential compromise
- Don't be afraid to label an ‘incident’ as fraud. Most banks will not act on ‘potential’ fraud or issues
- Act quickly, every minute counts when it comes to recalling or recovering funds. The longer it takes to flag the incident, the lower the chance of recovering the funds

Process

Have a plan
- Create a process before you need it
- Define roles & responsibilities
- Understand who needs to be notified, what they need to know and by when
- Carefully review the transactions on your other banking accounts to ensure there are no further anomalies

Report it
- Inform Citi as early as possible
- Report the incident to law enforcement
- Alert any other banks you may hold an account with

Technology

Keep everything
- Retain any potential evidence, including PC’s, email traffic and call logs

Secure your perimeter
- Engage fraud/security experts to determine how the compromise occurred and assess your resilience to future attacks

Test yourself
- Consider testing your susceptibility to further malware by having your IT department send simulated phishing emails
Questions
These materials are for information purposes only and do not constitute legal or other advice. These materials are intended as an aid in improving cyber security and fraud awareness and are not a substitute for your own programme in this regard. We have no responsibility or liability for any consequences of any entity relying on any information in these materials.

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.

© 2016 Citigroup Inc. Citibank, N.A. Member FDIC. Equal Credit Opportunity Lender. Citi, Citi and Arc Design and other marks used herein are service marks of Citigroup Inc. or its affiliates, used and registered throughout the world.