Cyber Threats to Retail Financial Services and Payments

Ruth Wandhöfer
Global Head of Regulatory and Market Strategy
Chair European Payments Council Payment Security Group

May 2015
Increase in Digital Banking Enhances Need for Cyber Security

As business interactions move online, cyber threats are becoming more sophisticated and dangerous.

Tremendous Growth of Online Interactions with each Click or Tap Leaving a Trail of Data

Cyber Threat and Fraud are on the Rise with Significant Impacts on Business and the Economy

$3 Trillion
Estimated cyber attack fallout cost to global economy by 2020.¹

$200+ Billion
Estimated amount stolen from banks, financial institutions, companies and individuals, double the amount in 2010.²

Source: World Economic Forum, SWIFT.
2. The Guardian Report: "Online fraud costs global economy many times more than $100 billion"; October 2013.
The Changing Information Security Threat Landscape

The cyber threat landscape continues to evolve as better organized and more sophisticated attackers have emerged.

### Evolving Threats—An Illustration of the Information Security Challenge

<table>
<thead>
<tr>
<th></th>
<th>Past</th>
<th>Present</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Speed of Attack</strong></td>
<td>Non real-time theft of passwords and confidential information</td>
<td>Real time compromises of customer computers and communication channels</td>
</tr>
<tr>
<td><strong>Target of Attack</strong></td>
<td>Typically targets of opportunity</td>
<td>Frequently specifically chosen high value targets</td>
</tr>
<tr>
<td><strong>Value of Information</strong></td>
<td>Very variable—hard to monetize without exposing the malicious actor</td>
<td>Readily monetized in a sophisticated, secure, and anonymous</td>
</tr>
<tr>
<td><strong>Complexity of Business Model</strong></td>
<td>Workforce primarily based in same geography as business and on payroll</td>
<td>Workforce increasingly cross border and outsourced</td>
</tr>
<tr>
<td><strong>Sophistication of Techniques</strong></td>
<td>Moderately sophisticated adversaries seeking to exploit well known vulnerabilities</td>
<td>Highly sophisticated supply chain to create or detect vulnerabilities and exploit tools, then sold to &quot;worker bees&quot;</td>
</tr>
<tr>
<td><strong>Availability of Tools</strong></td>
<td>Custom tools created by knowledgeable individuals to perform a specific attack</td>
<td>Malicious tools are commodity items readily available on the black market</td>
</tr>
</tbody>
</table>
Nature and Frequency of Cyber Attacks

- The amount of knowledge required to launch very sophisticated attacks is decreasing over time making these threats more severe each day.
- Recent attacks show increased knowledge and understanding of the technology, infrastructure and systems of their victims.
- Bad Actors are going after customers, suppliers, and third-parties in addition to direct attacks.
- Intelligence, external and internal as well as shared knowledge across the industry and governments will be the most effective counter strategies.
Nature and Frequency of Cyber Attacks

Attack Sophistication vs. Intruder Technical Knowledge

- The amount of knowledge required to launch very sophisticated attacks is decreasing over time making these threats more severe each day.
- Recent attacks show increased knowledge and understanding of the technology, infrastructure and systems of their victims.
- Bad Actors are going after customers, suppliers, and third-parties in addition to direct attacks.
- Intelligence, external and internal as well as shared knowledge across the industry and governments will be the most effective counter strategies.

High
Low

<table>
<thead>
<tr>
<th>Year</th>
<th>Attack Sophistication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1980</td>
<td>Cross Site Scripting</td>
</tr>
<tr>
<td>1990</td>
<td>Password Guessing</td>
</tr>
<tr>
<td>2014</td>
<td>Self-replicating Code</td>
</tr>
<tr>
<td>2000</td>
<td>Password Cracking</td>
</tr>
<tr>
<td></td>
<td>Exploiting Known Vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>Disabling Audits</td>
</tr>
<tr>
<td></td>
<td>Back Doors</td>
</tr>
<tr>
<td></td>
<td>Hijacking</td>
</tr>
<tr>
<td></td>
<td>Sweepers</td>
</tr>
<tr>
<td></td>
<td>Sniffers</td>
</tr>
<tr>
<td></td>
<td>Packet Spoofing</td>
</tr>
<tr>
<td></td>
<td>GUI</td>
</tr>
<tr>
<td></td>
<td>Automated Probes/Scans</td>
</tr>
<tr>
<td></td>
<td>Denial of Service</td>
</tr>
<tr>
<td></td>
<td>www Attacks</td>
</tr>
<tr>
<td></td>
<td>“Stealth”/Advanced Scanning Techniques</td>
</tr>
</tbody>
</table>

Key Adversaries

**Cyber Criminals**

- **Motivation:** Make Money
- **Methods:** Very mature underground economy supporting every facet of cyber criminal activity

**Cyber Terrorism**

- **Motivation:** Instill fear so targets comply with demands or ideology
- **Methods:** Using cyber to “enable” their programs (Recruit, Incite, Train, Plan and Finance). Underground forums allow these groups to easily acquire destructive capabilities

**Hactivists**

- **Motivation:** Seek publicity for their geopolitical agenda
- **Methods:** Disruption and Defacement

**State-Affiliated (Advanced Persistent Threat)**

- **Motivation:** Political and technological advantage to improve self interests
- **Methods:** Advanced operations to gain a foothold into a target’s infrastructure. Once a foothold is established, the adversary performs reconnaissance and methodically plans their attack. APT actors often leave back doors to re-establish access to the target in case their primary means is identified and mitigated.
Understanding Information Security Risk

Information Security Risk is determined based on strong assessment of the threats, known vulnerabilities and the assets involved.

External
- Nation State
- Cyber Terrorists
- Cyber Criminals
- Hacktivists

Internal
- Privileged Users
- End Users

Insecure Code and Applications
- Toxic Combinations/Over Entitlements
- Client Side Software Vulnerabilities
- Unauthorized Privileged User Access
- Unencrypted Data
- Improper Configuration Management
- Network and Operating System Software Vulnerabilities

Assets
- Intellectual Property
- Corporate Data
- Credentials
- Financial Transactions
Retail Payment Threats: Point of Sale Systems

Methods
According to Verizon, POS compromises were the leading cause of data breaches from 2011-2013. In 2015, their research found that most small organizations were targeted directly through brute forcing (or guessing) the passwords to access the systems; conversely, they found that larger organizations were compromised through a multi-staged attack, where malicious actors gained access to secondary systems and worked their way to POS systems. Common entry vectors include:

• POS Vendors
• Direct Retail System Compromises
• Third Party Compromise with B2B access

Threat Actors
The cybercriminals that steal payment card information often sell them on underground forums. The groups behind each malware family can often be identified through their methods and targets. For example, Backoff and Poseidon malware are often used against POS Vendors then spread to retailers through a remote desktop application.

Defense Considerations
Third Party vendor access management can help reduce the risk of compromise through this vector. The following, among others are best practices:

• Multi-factor authentication
• Lockout Policies
• Establish Normal Activity
• Training for third party vendors

Information Sharing
Partnerships that facilitate information sharing can be one of the best initial indicators of fraudulent activity, therefore allowing financial institutions, retailers and law enforcement to take action.
ASSESSMENT OF RECENT BREACHES

2014 Data Breaches - US perspective

Destructive Malware
- Sony
- Sony

Sensitive Information Theft (Intellectual Property, PII)
- Kaiser Permanente
- JP Morgan Chase
- USIS
- eesa
- Unicef
- Iowastateuniversity
- Medtronic
- University of Wisconsin
- Parksides
- Keypoint
- CHS

DDoS
- Hootsuite
- GitHub
- Neustar
- UltraDNS
- Namecheap
- CIRRUS
- PointDNS
- Timbuktu
- PCNP
- Tork
- Xbox
- Evernote

Payment Card Theft
- Sally Beauty Supply
- UPS
- CaK Systems
- Affinity Gaming
- AOL
- Bitly
- Boletol
- Deltek
- Futureppt
- Sandman
- Chick-fil-A

Customer Credential Theft
- Feedly
- Cloudflare
- SC Hong Kong
- PF Chang's
- Affinity Healthcare Solutions
- Affinity
- ADO
- Boletol
- Financelab
- MoshTix
- STOR

Known Targets
- Government
- Academic
- NGO
- Energy
- Retail

Citigroup

8
2014 Payment Card Breaches – US perspective

2014 saw a mix of attacks on brick-and-mortar establishments and online retailers, often exploiting the remote access tools IT professionals and vendors rely on to maintain payment card systems.

- Criminals have attacked both brick-and-mortar locations and e-Commerce sites - often using stolen or hacked remote administration credentials.
- Any place where payment cards and the internet meet is a potential target.
- Victim retailers rarely find the breach themselves, often found by banks.
- Franchises can present some specific issues regarding payment card theft.
- The financial impact of payment card breaches to institutions is rising year-over-year, with the US being one of the most expensive places to have a data breach.
A number of currently unregulated market players provide services to online merchants in order to facilitate e-commerce payment transactions outside the traditional cards world.

In order to ensure these players are regulated, the Payment Services Directive II, which is in the process of being adopted, introduces these new providers and services to the payment conduct of business rule regime. New key features of PSD 2 therefore include the introduction of third party payment providers (TPPs), which can provide three types of services:

1) Payment initiation
2) Payment instrument issuance
3) Account information services

While technical rules for communication between TPPs and account holding PSPs/banks are still to be developed by the EBA, it appears that the regulators’ intention is to continue to permit TPPs to ‘re-use’ online banking customers’ personalised security credentials in order to access their account, a process which facilitates the services of payment initiation and account information (as well as the provision of credit). For payment instrument issuance the TPP will contact the bank to understand whether funds are available on the customer account.

Account holding PSPs/banks will need to ensure additional security, given the threat of potential ‘fake’ TPPs that offer their services and obtain customer credentials in order to empty their account. In all circumstances the account holding TPP/bank remains first port of call for customer issues as well as liability back-stop in case of fraudulent, unauthorised transactions. Whilst TPPs will have to prove their ‘innocence’, this is unlikely to happen in case of a fraudulent intervention.
The rise of the cyber threat has wide immediate business implications and significant impacts over the long-term.

### Immediate Implications for the Business
- Loss of data
- Corruption or destruction of data
- Unauthorized access
- Account takeovers
- Compromised systems and applications
- Unavailability of services

### Impact on the Business
- Reputational loss
- Financial loss/fraud
- Regulatory compliance incidents and penalties
- Client loss
Role of Intelligence - Execution

Intelligence must be an integral part of the decision making process. Intelligence is having the right information, at the right time, and in the hands of the right people.

Intelligence is embedded in the day-to-day work, from the establishment of a customer relationship to the execution of any service. Capturing and understanding the knowledge of employees is the foundation of a successful Intelligence Program.

Output/Deliverables

- Inform operational planning and strategic decision-making
- Inventory of intelligence resources
- Identification of resource gaps, recommendations for remediation
- Centralized mechanism for ad hoc intelligence data
- Regular, frequent updates to senior management and key business stakeholders (e.g. dashboard-type, high-level briefing report)
- Intelligence-sharing and knowledge-sharing (lessons learned, etc.)

Intelligence Involves Forward-Looking Insights

Intelligence is built from a mosaic cutting across various views, which helps to identify emerging trends, make informed decisions and predict the next event.

Intelligence has a short half-life.
Digital Security is Our Business

Citi invests large amounts annually to help protect client assets. Working with our clients is critical to the integrity of end-to-end security.

Finding on Partnering End-to-end, Bringing Together Technology and Best Practices

- Security goes beyond technology and authentication mechanisms to various processes, including:
  - Maker/checker compliance for transaction authorization
  - Ensuring business devices are clean and password-protected
  - Leveraging data for alerts
  - Payment monitoring and behavior-based blocking tools

- Client collaboration is central to maintaining high security

Digital channels have brought better control, but as we leverage new channels, we need to be at the top of our game and keep ahead of the curve.
The Power of Our Network

CitiDirect BESM Online
Award winning digital corporate banking platform live in 96 markets that processes +$30 trillion annually

CitiDirect BESM Mobile
Industry leading mobile platform that processed $113 billion in Mobile Payments from on-the-road ICG clients in 2013 alone!
Working Together to Secure Digital Transactions

We are Only as Strong as the Weakest Link