Cyber-Situational Awareness in the Financial Sector
Introduction

The e-financial movement has become a panacea for crime and economic attack. Most of the crimes that exploit vulnerabilities inherent to the Internet are not new—fraud, theft, impersonation, denial of service, and related extortion demands have plagued the financial services industry for years. However, the widespread use of e-finance technologies exposes users to crimes of greater dimensions in terms of depth and scope. Open network technologies create a fertile environment for crimes of great magnitude and complexity to be committed very quickly. To protect themselves, organizations need to understand both the risks and benefits offered by these technologies.

The Financial Services Threat Environment

The highly diverse range of cyber-attacks currently being directed at elements of the financial sector, herein identified as Financial Sector Threats\(^1\), have been identified as the most omnipresent form of criminal activity propagated across our electronic infrastructure according to authorities including the World Bank, the United States Secret Service (USSS), and the Federal Bureau of Investigation (FBI). Respective of this reality, it has become paramount to the protection of both the economic and national security interests of the United States that our nation’s leaders rapidly achieve a higher level of cybersecurity situational awareness and effectively prioritize strategic mitigation of confirmed vulnerabilities known to reside across the financial sector today.

Over the past decade, cyber-attacks have realized explosive advancement in their complexity, diversity and overall volume therein evolving into powerful weapons in the realm of economic markets having gained the capability to destroy critical databases, interrupt underlying services, and impart catastrophic financial damage to a vast array of different constituencies—all in an incredibly short timeframe. According to a 2010 report issued by the Federal Deposit Insurance Corporation (FDIC)\(^2\), over $700 million in losses were sustained by financial institutions in the first quarter of 2010 alone.

FinCEN Suspicious Activity Reports: Fraud on the Rise

In the overview of 2009 Suspicious Activity Reports (SARs) filed with the Financial Crimes Enforcement Network\(^3\) (FinCEN), an arm of the U.S. Treasury Department, experts found that of the 56,000 instances of fraudulent wire or funds transfers occurring since 1997, more than half have occurred in the past two years. Countless other reports published in recent years across the financial and IT security sectors reinforce the seemingly unstoppable encroachment of dedicated cyber-attacks leveraged against highly

---


\(^2\) See: FDIC at www.fdic.gov

\(^3\) See: FinCEN at www.fincen.gov
mission-critical, interconnected financial systems. As evidenced Check & ACH fraud are rising at very high rates, and people that have money-moving rights are being targeted. This is causing both small and mid-size companies to experience material financial losses. To address this issue, financial services organizations must assess the integrity of their ACH and check life cycles.


**IT Security Trends from the FDIC Technology Incident Report**

In the 2007 FDIC Technology Incident Report noted the following troubling IT security trends in the financial sector:

- “The number of computer intrusion SAR filings are growing at a fast pace. The estimated mean (average) loss per SAR almost tripled the estimated mean loss per SAR identified one year ago”.
- “Unknown unauthorized access was the most frequently identified type of computer intrusion: meaning the Financial Institutions (FI) could not or did not identify how the intrusion occurred--followed by ID theft/account takeover.”
- “Online bill payment applications were most frequently targeted by cyber thieves; however, unauthorized access to ACH and wire transfer applications caused the most losses to FIs in the computer intrusion category.”
- “An increase in websites hosting malicious code was noted by FDIC and anti-virus software vendors.”
• “Spear phishing (when end users with high computer access levels are targeted via social engineering) was also cited in several sampled computer intrusion SARs.”

There are a rapidly increasing quantity and multiplicity of profound cyber threats known to currently stalk nearly all electronic aspects of the banking and finance sectors; yet, data about specific instances and overarching cyber attack trends playing out throughout these industries remains remarkably scarce. Industry surveys conducted by independent third parties such as industry analysts or media firms surface some baseline cross-sector findings, but organizations are armed with little in the way of actionable intelligence regarding the cyber-attacks faced by their peers. This failure in fostering Financial Sector Threat incident information sharing is partially caused by a lack of standard methods for reporting or tracking these attacks and also resultant of a dearth of adequate regulations requiring financial sector entities to detail both attempted and successful attacks to appropriate authorities.

The FSSCC’s Most Pressing Cyber Threats

The Financial Services Sector Coordinating Council (FSSCC) for Critical Infrastructure Protection and Homeland Security has assigned what it views to be the most pressing cyber threats on the landscape today into five specific areas:

• Application Security
• Identity Theft
• Mobile Devices
• Supply Chain
• Undersea Cables

---

4 See: FSSCC at https://www.fsscc.org/fsscc/
Table 1: FSSCC Cyber Threat Examples

<table>
<thead>
<tr>
<th>Application Security</th>
<th>Identity Theft</th>
<th>Mobile Devices</th>
<th>Supply Chain</th>
<th>Undersea Cables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access to sensitive applications</td>
<td>Customers’ personal or private information used for financial gain</td>
<td>Communications interruption during cyber attacks</td>
<td>Embedded backdoors across distributed infrastructure</td>
<td>Component failure</td>
</tr>
<tr>
<td>Toxic combinations, e.g., execution and approver</td>
<td>Unauthorized access to critical infrastructure</td>
<td>Access vulnerabilities exposed to smart devices</td>
<td>Reliance on third-party vendors across IT borders</td>
<td>Landing station chokepoint concentration risk</td>
</tr>
<tr>
<td>System shutdowns</td>
<td>Credentials abuse and compromised access</td>
<td>Data leakage</td>
<td>Quality controls at systems and network interaction points</td>
<td>Physical attack resiliency (introduced via poor design/connectivity risks)</td>
</tr>
<tr>
<td>Software standards and software assurance issues</td>
<td>Internet/ telecom network performance interruption</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The FDIC Cyber Fraud Chief’s Top Five Fraud Threats

In a July 23, 2010 interview ¹ Michael B. Benardo, chief of the Federal Deposit Insurance Corp.’s Cyber Fraud and Financial Crimes Section noted these top five fraud threats of concern to the FDIC:

1. **Malware and Botnets** — These software agents or robots that take over a user’s computer are often the root causes of commercial payments fraud, i.e. corporate account takeover. "Malware has gotten on the computers of commercial customers and financial institutions, thereby compromising their log-in credentials and causing the criminals to be able to commit fraud by moving money through wire transfers or ACH," Benardo says.

2. **Phishing** — The crime has evolved from badly-written, bogus emails to well-crafted assaults via e-mail, telephone and text message. "My worry is the next way that criminals will change phishing and be creative via social engineering," he says.

3. **Data Breaches** — Despite that most data breaches have occurred on the merchant and payments processor sides of the business, financial institutions are still deeply impacted by these losses. "They have to reissue cards and deal with the aftermath of credit card information getting out there, and how that can lead to the identity theft of their customers."
4. **Counterfeit Checks** -- The circulation of checks continues to drop, but counterfeit check fraud remains prevalent. Cashier checks and bank official checks are most often the targets, Benardo says. "[Criminals] understand Reg CC and know that those checks have faster funds availability, which allows them to get their money out of the scam faster."

5. **Mortgage Fraud** -- These crimes committed against financial institutions, as well as mortgage rescue scams that affect consumers and mortgage holders, continue to rock the financial market. "We're starting to see a lot of that," Benardo says.

Cross-border fraud was also on the rise. And as fraudsters continue to perfect their schemes, detection has become more difficult.

### Recommendations for Ensuring Financial Asset Safety and Soundness

According to the FDIC and FINCEN Computer Intrusions and wire transfer fraud have metastasized in this past year. Maintaining trust and confidence in the safety and soundness of e-financial assets has become ever more challenging. In the face of blended and staged attacks, managing technology risk is possible only through continuous monitoring of enterprise level risk metrics per the effectiveness of your security controls. Understanding your financial institution’s susceptibility to compromise is fundamental to successfully managing 21st century operational and systemic risk. The regulators who comprise the Federal Financial Examination Council (F.F.I.E.C.) are revising the Information Security Handbook for financial institutions this spring and will be issuing new guidance per managed service providers in May. These new guidelines will demand increased testing and continuous monitoring.

Security testing and measurement solutions from Core Security Technologies can assist in the preservation of electronic safety and soundness. Specifically, CORE INSIGHT Enterprise offers a best-of-breed risk assessment capability for discerning “technology risk” within financial institutions. CORE INSIGHT provides risk assessment capabilities that deliver enterprise-level metrics per the susceptibility of exfiltration of confidential customer information and the feasibility of rogue access to large-value funds transfer systems.

In addition to using security testing and measurement solutions like CORE INSIGHT, the financial sector can improve defense in depth via a number of proactive actions, including:


2. Educate the executive team and board so they understand the systemic issues that are being dealt with and what they need to do.

4. Increase the level of “integrity” to a higher level via the implementation of in-depth defense and continuous monitoring of security controls efficacy. Recommendations for ensuring integrity include:
   a. Move towards digital time-stamping of transactional data.
   b. Utilize two-factor authentication.
   c. Implement wireless security solutions.
   d. Conduct penetration tests of shared service provider systems and mandate remediation timetables via SLAs.
   e. Assess web applications for OWASP Top 10 vulnerabilities prior to deployment.

About CORE Insight Enterprise

CORE Insight Enterprise is the first security intelligence solution that enables organizations to continuously and proactively assess their business risks. CORE Insight empowers executives to make informed choices for improving security, optimizing budgets, and increasing operational efficiency. The Insight solution integrates seamlessly with existing IT environments, pinpointing imminent risks without disrupting business processes. By combining advanced simulation with real-world testing, CORE Insight provides actionable information otherwise overlooked amidst volumes of security data. Customers gain unprecedented intelligence regarding their organization’s real-time security posture, while connecting real risks to specific operational and business goals.

About Core Security

Core Security is the leading provider of predictive security intelligence solutions for enterprises and government organizations. We help more than 1,400 customers worldwide preempt critical security threats throughout their IT environments, and communicate the risk the threats pose to the business. Our patented, proven, award-winning enterprise solutions are backed by more than 15 years of applied expertise from CoreLabs, the company’s innovative security research center. For more information, visit www.coresecurity.com.