LOCKHEED MARTIN

Combating the Biggest Cyber Threats to the Financial Services Industry

A White Paper Presented by:
Lockheed Martin Corporation

Combating the Biggest Cyber Threats to the Financial Services Industry

Financial institutions have long been a favorite target of criminals. However, today's "bank robbers" are looking for more than just cash and need never set foot inside a brick-and-mortar establishment to get what they are looking for. Technology has changed the game and added more threats for the financial services (FS) industry.

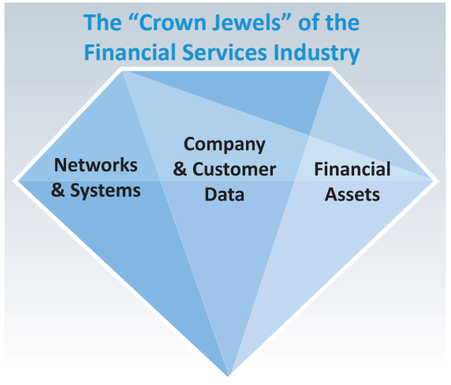
Even as FS organizations grapple with shrinking profit margins, growing consumer expectations, and a challenging regulatory environment, many are realizing the lethal impact posed by cyber threats.

A recent study by the Depository Trust & Clearing Corporation (DTCC) revealed almost half of FS firms (46 percent) named cybersecurity as their top concern—nearly double their response from the prior year.[1] The dramatic shift comes as no surprise given how quickly cyberattacks and breaches have become more constant and sophisticated, making them more difficult for most companies to detect. In fact, the FBI notified 3,000 U.S. companies across a number of industries, including FS, that they had been victims of cyber intrusions in 2013.[2]

Unfortunately, that number represents only a fraction of the true number of cyber intrusions into the private sector by common criminals, organized crime rings, and foreign governments and their proxies.

The Far Reaching Impact of a Breach

Cyberattacks have far-reaching economic consequences beyond the financial, reputational, and legal ramifications for an individual firm. A security breach at a few financial institutions can pose a substantial danger to market confidence and the nation's financial stability. The implications are so great that the U.S. Director of National Intelligence has ranked cybercrime as the top national security threat, "higher than that of terrorism, espionage, and weapons of mass destruction."[3]



Regulators around the globe are also awakening to the systemic danger posed by cybercrimes against the FS industry. Public companies in the U.S. must now disclose in their Security Exchange Commission (SEC) filings on any cyber incidents that have had material impact—a dramatic change that prevents organizations from keeping cyberattacks out of the public eye.[4]

The Biggest Threats Faced by the Financial Services Sector

Today, with all of a FS firm's sensitive information being stored electronically, more systems and databases in use, and the Internet—and subsequently mobile computing—exponentially growing data transmissions, it's never been easier for sensitive information to fall into the wrong hands.

Beyond protecting data, such as customer records, clearing and trading information, or confidential documents, FS organizations have the hefty challenge of safeguarding their systems and networks as well as the financial assets they hold. That means the FS industry faces a larger number of threats than most other industries. Here are nine of the biggest challenges:

1. **Advanced Persistent Threats (APT).** APTs use undetected, continuous computer hacking processes to gain access to a high-value organization's network. Phishing emails or other tricks to fool employees into downloading malware are a common practice. When the unauthorized person gains access, they often go undetected for a long period of time—quietly stealing data, committing fraud, destroying an institution's economic stability or undermining its reputation.
2. **Insider and Internal Threats.** Any employee, contractor, supplier, or business partner who has authorized yet uncontrolled access to systems and/or sensitive information all have the opportunity to do irrevocable harm to a company. This threat has grown more substantial by the increased use of personal devices in the workplace, personal email, and cloud-based and USB storage devices. Intentionally or unintentionally, insiders can undermine systems, open them to malicious intrusion, and engage in fraud, theft, or market manipulation.
3. **Denial of Service Attacks.** These threats are defined as "any attack intended to compromise the availability of networks and systems" and are of concern to financial corporations operating consumer-facing websites or trading systems. Such attacks flood a network with phony connection requests, making it unavailable to process legitimate user requests.
4. **Account Takeovers.** Cyber criminals have quickly discovered how to exploit financial and market systems that interface with the Internet, such as the Automated Clearing House (ACH) systems, card payments, and market trades. Exploiting system users, rather than the systems themselves, earn criminals access to existing bank or credit card accounts or financial systems, and allow them to carry out unauthorized transactions. A recent report on cybersecurity in the banking sector identified that almost half (46 percent) of institutions reported account takeovers as the most frequent cyber intrusion activity they experience.[5]
5. **Securities and Market Trading Breaches.** Financial institutions in the securities and brokerage business, as well as their customers, are frequently targeted by cyber criminals. According to the FBI, market manipulation and unauthorized stock trading are common risks faced by traders and the exchanges they are sold on.[6]
6. **Third-Party-Payment Processor Breaches.** Sophisticated cyber criminals are also targeting the computer networks of large payment processors, resulting in the loss of millions of dollars and the compromise of personal information of millions of individuals.
7. **Supply Chain Infiltration.** In recent years, trusted suppliers of technical, computer and security equipment, software and hardware have been targeted by cyber criminals seeking to gain physical and technical access to financial institutions. Cyber criminals are continuously devising new ways to infiltrate financial institutions, from posing as vendor employees to delivering infected equipment. Some recent attacks involved hardware installed in bank branch systems to enable transactions to be manipulated via mobile networks.[7]
8. **Mobile Banking Breaches.** Meeting customer demands for greater mobile banking capability, has opened financial institutions up to another cyber threat. Cyber criminals have quickly figured out how to exploit the vulnerabilities in mobile technology by using malicious websites, text messages, or mobile applications to gain access to a user's credentials and account information.

9. **Payment Card Skimming.** A skimmer fitted to the outside or inside of an ATM or gas station pumps enables a criminal to collect card numbers and personal identification number (PIN) codes. The stolen data is usually sold or used to make fake cards to withdraw money from the compromised accounts. As companies continue to roll out—and consumers embrace—new electronic, wireless payment systems, criminals are quickly adapting. Hackers have already designed Bluetooth-enabled wireless skimmers to instantly download data when in range of the wireless network.

How to Ready Your Organization

Despite taking significant steps to strengthen their cybersecurity, banks and other FS organizations will continue to be challenged by the speed of technological change and the increasingly sophisticated nature of cyber threats. Institutions are aware that the threat landscape is constantly evolving, but many will find it difficult to stay current amid competitive pressure to integrate new technologies into their product and service offerings.

Additionally, present-day cybersecurity risk management practices within the FS industry are primarily driven by compliance requirements and managed as an IT function. This approach unfortunately focuses on security controls and vulnerabilities, creating highly reactive (rather than proactive) operational environments. When vulnerabilities and incidents are found, they're handled at a micro level rather than using the intelligence to develop larger-scale threat scenarios and patterns.

Larger FS organizations who want to stay ahead of cyber criminals and reduce risk have adopted security operations centers (SOCs). These are dedicated facilities that defend the entire enterprise and respond to all forms of security threats. These traditional centers served well in response to traditional attacks, but today's threat landscape requires organizations to take a predictive approach to security so threats may be addressed before they cause harm rather than merely reacting to them.

The next level of cybersecurity involves evolving a traditional SOC into a security intelligence center (SIC). People and technology are still crucial elements; however, both are evolved and tailored to support an Intelligence Driven Defense®. This is driven by organizational collaboration, intelligence and event analysis, and early threat detection.

Building a Security Intelligence Center

People, technology and capabilities are at the heart of a dedicated SIC that defends an organization's enterprise systems and provides an efficient, effective response to active threats and potential incidents. Here are the five steps an organization must take to build a world-class SIC:

Step 1. Know Your Organization

SICs are typically found in large enterprises but, given the threat to organizations of all sizes, even small firms are urged to put more formal security measures in place. Determining your organization's threat profile (value of your organization's assets or functions) will help you determine the need for and scale of a SIC. Additionally, organizational support of a SIC is critical. Although dedicated to security, the SIC's mission can be effective only if security is a part of the organization's culture.

Step 2. Develop a Strategy

Executive support and a clear view of the mission and goals as well as a road map for achieving them are essential for the success of a SIC. Today's sophisticated threats are driving many organizations to enlist the help of security organizations to bring expertise and industry best practices to their SIC. A proprietary Cyber-Kill Chain® methodology is used to analyze intrusions and extract indicators, resulting in a tailored strategy and implementation that will achieve the most sensitive defensive goals.

Step 3. Build Your Team

An effective SIC depends as much on the people who staff it and their skills as on the technologies they are using. Operational and analytical functions are staffed with personnel who have knowledge of the network, systems and software used, and have cyber threat prevention, detection, and response experience.

Step 4. Assess Your Technology

Rapidly advancing technology and sizable risks face FS organizations. It is no longer enough to rely only on traditional defense, in-depth models and out-of-the-box solutions to secure information and networks. The next evolution in defense against cyber threats is an Intelligence Driven Defense®. The cutting-edge technology, vigilant people and innovative processes used in the Intelligence Driven Defense® approach detect, mitigate and effectively adapt to advanced cyber threats.

Step 5. Evolve Your Processes and Procedures

IT security is not a static target. All policies, practices and procedures launched by the SIC must continue to be refined. The goal is to improve the organization's security posture, and that goal should be continually evolving. A successful SIC reveals probes, attacks and incidents not previously visible—data that will be used to establish priorities for upgrading, patching and configuring systems and for adjusting security policies.

Cyber technology will continue to evolve to give FS organizations more opportunities to grow their businesses and improve their operations. But cyber threats will continue to grow as well. Given the sizable financial, reputational, legal and market ramifications cyber intrusions can inflict, the FS industry can no longer afford to defend itself with limited, reactive security approaches. Defense efforts focused on vendor-driven detections and out-of-the-box solutions are not enough to prevent a large-scale attack. The next evolution in cybersecurity is to deploy a security intelligence center to defend an organization from all threats, and an Intelligence Driven Defense® that employs cutting-edge technology, vigilant people and innovative processes.

2015-08

[1]Tom Reeve, "Cyber-security now the top concern for financial services," 15 May 15, 2015, SC Magazine. 29 July 2015
<http://www.scmagazineuk.com/cyber-security-now-the-top-concern-for-financial-services/article/414885/>

[2]Ellen Nakashima, "U.S. notified 3,000 companies in 2013 about cyberattacks," 24 March 2014, Washington Post, 29 July 2015
<https://www.washingtonpost.com/world/national-security/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_story.html>

[3]"Threats to the Financial Services Sector," 2014, PwC, 27 July 2015,
<https://www.pwc.com/en_GX/gx/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf>

[4]"Threats to the Financial Services Sector," 2014, PwC, 27 July 2015,
<https://www.pwc.com/en_GX/gx/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf>

[5]"Report on Cybersecurity in the Banking Sector," May 2014, New York State Department of Financial Services, 27 July 2015
< http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf>

[6]Gordon M. Snow, "Cybersecurity: Threats to the Financial Sector," 14 September 2011, Federal Bureau of Investigation, 29 July 2015
< https://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector>

[7]"Threats to the Financial Services Sector," 2014, PwC, 27 July 2015,
<https://www.pwc.com/en_GX/gx/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf>

[7]Ivy Schmerken, "Morgan Stanley Data Theft Exposes Insider Threat & Need for More Restrictions," 14 January 2015, Information Week, 10 June 2015 <http://www.wallstreetandtech.com/security/morgan-stanley-data-theft-exposes-insider-threat-and-need-for-more-restrictions/d/d-id/1318623>

Combating the Biggest Cyber Threats to the Financial Services Industry

For more information on cybersecurity solutions
Email: cyber.security@lmco.com
Phone: 855-LMCYBER
www.lockheedmartin.com/cyber

PIRA# CMK201508005