Lightning War

OUTFLANKED BY CYBER-THREATS, CAN FINANCIAL FIRMS MANEUVER FAST ENOUGH?

By Sherree DeCovny

As a core part of the critical economic infrastructure, financial firms offer a prime target for adversaries who want to steal data and funds or even to disrupt the industry. Financial firms effectively have fallen behind in a cyber arms race, and the magnitude of risk has vastly increased, with organized crime and state-sponsored attacks becoming more active and powerful. But financial professionals may have a surprising ability to adapt. "I have noticed many of the formulas used to measure risk in cybersecurity are based on the same formulas that I learned when I studied for my finance degree," says Jess Parnell, director of information security at Centripetal Networks. "The minor adaptation of these formulas for the financial industry just makes common sense."

KEY POINTS

The magnitude of cyber-threats to financial firms has reached the point of placing critical economic infrastructure at risk, with the potential to cause large-scale disruption of markets and other systems.

Cybersecurity for financial firms requires a hybrid skillset that goes beyond IT or financial acumen; moreover, the scope of the threat requires cooperation among financial institutions and government agencies.

Financial professionals may have a surprising advantage, as models for evaluating cyber-risk are derived from some of the same concepts as modern finance.

THE GATHERING STORM

Organized crime is seeking to monetize the theft of account credentials and to take over accounts, sometimes leveraging payment or messaging infrastructures. In one recent high-profile case, hackers got into SWIFT's systems and stole $81 million from the Bangladeshi central bank's account at the Federal Reserve Bank of New York.

Strategic rivals such as Russia, China, North Korea, Iran, and others hack to obtain specific data, duplicate business models, and disrupt the functioning of the markets. A case in point is the 2012–2013 distributed denial-of-service attacks against the US financial sector. The attacks were allegedly the work of a nation-state–sponsored group. In March 2016, the US Department of Justice indicted seven Iranians who, according to a statement from the US Attorney's Office, "were employed by two Iran-based computer companies, ITSecTeam ('ITSEC') and Mersad Company ('MERSAD'), which were sponsored by Iran's Islamic Revolutionary Guard Corps."

"Investment companies are dealing with a number of different challenges, which are often different from the banks and payment processors," says John Carlson, chief of staff at the Financial Services Information Sharing and Analysis Center (FS-ISAC). "Adversaries are going after different elements of the sector for different reasons."

The amount of money being spent to protect the financial services industry is growing markedly. In 2020, organizations across all industries are expected to spend $101.6 billion on cybersecurity software, services, and hardware, according to International Data Corporation (IDC). This is a 27% increase from the $73.7 billion that organizations were projected to spend on cybersecurity in 2016. IDC also projected that 2016 would see the banking industry spend more than any other on cybersecurity; JP Morgan alone announced plans in August 2015 to double its budget to $500 million.

"The whole IT organization is under a tremendous amount of pressure to protect the assets," says Aubrey Chernick, CEO of the National Center for Crisis and Continuity Coordination (NC4), headquartered in El Segundo, California. "No bank wants to have reputational damage by having an article appear about their cyber-disclosures, and yet it's almost impossible not to have something like that occur."

Several cybersecurity frameworks for the financial services industry contain broad recommendations on what firms should be doing to analyze and respond to threats—so many that it is leading to framework fatigue. Just to name a few: The National Institute of Standards and Technology has the NIST Framework; the Federal Financial Institutions Examination Council provides the Cybersecurity Assessment Tool from its website; and the World Federation of Exchanges has the Global Exchange Cyber Security Working Group.

In October 2016, the G7 nations released their eight fundamental elements of cybersecurity for the financial sector. In the same month, the Federal Reserve, Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency announced their own joint proposed rules. The latter apply to any financial company that takes deposits and has at least $50 billion in assets, including regional banks, credit card businesses, large insurers, and clearinghouses.

DEFENSIVE COUNTERMEASURES

To this end, financial firms are building IT fortresses to protect themselves against cyber-threats. Many vendors provide hardware, firewalls, software packages, consulting, and other professional services in what has become a multi-billion-dollar industry.

Because attacks come in so many different forms, firms typically have a security policy in place, enacted by a layered defense approach. This strategy involves security tactics and procedures such as password security practices,

technical security controls, real-time threat intelligence analysis, and employee cyber-awareness training. Still, it is important to look beyond what goes on *within* an enterprise to what goes on *between* enterprises.

"Sharing cyber-threat information with other companies can be problematic," says Chernick. "They don't want to share it in many cases because of legal concerns, and they certainly don't want the competition to find out that they had an attack."

To address the legal and confidentiality issues, the US government passed the Cybersecurity Information Sharing Act, and the Department of Homeland Security (DHS) developed its Automated Indicator Sharing initiative. In addition, Information Sharing and Analysis Centers (ISACs) allow organizations to share sensitive information anonymously through a trusted intermediary. FS-ISAC, the entity for the financial services industry, has thousands of members, including banks and asset managers of all sizes.

FS-ISAC facilitates information sharing around vulnerabilities, incidences, threats, and campaigns from several types of adversaries, including organized crime, nation-states, and hacktivists. It also runs exercises that provide opportunities to look more deeply at interdependencies between institutions and other sectors, especially the retail, legal, electricity, and communications sectors. These exercises enable more-effective coordination with law enforcement—particularly the FBI and the US Secret Service—to deal with attacks that emanate from nation-states.

As part of its Securities Industry Risk Group, the organization has a Broker-Dealer Council, an Asset Manager Council, and an Alternative Investors Council for hedge funds, venture capitalists, and private equity firms. These councils are trusted communities of practitioners that have their own conversations about specific threats, issues, and regulatory-compliance challenges.

"These activities enhance the FS-ISAC members' resilience and their ability to understand how the environment is changing, which then drives the type of controls they need to put in place," says Carlson. "We can collaborate as a community and figure out how best to respond to different events as they unfold or as they escalate in importance."

The financial services industry conducted 13 cybersecurity simulation exercises among leaders in the public and private sectors in 2015. A finding from one exercise was that in certain scenarios, questions could be raised about the integrity of data because of a destructive malware attack against a financial institution or service provider. Leaders from the private sector decided that more needed to be done to maintain investor and depositor confidence in the face of cyber-risks.

In response, the entire industry collaborated on a set of standards to store, encrypt, and format brokerage and depository account balance information so that other institutions can access it in the event of an extreme scenario. This collaboration became known as the Sheltered Harbor initiative. FS-ISAC is the corporate entity that manages it, and participation is open to all financial institutions.

Another important initiative is the Financial Systemic Analysis & Resilience Center. It is designed for financial organizations that the US government designated as part of the critical infrastructure in a 2013 executive order from the Obama Administration. In 2016, the CEOs of those organizations decided to form an entity under FS-ISAC that focuses more intensely on information sharing, as well as deeper analysis and engagement with the government, particularly law enforcement agencies.

Recently, ransomware attacks in financial services and other sectors have increased. In such an attack, an adversary gains access to systems, encrypts critical data, and then demands a ransom (often in Bitcoin) to decrypt and return the data. In response, FS-ISAC partnered with other ISACs, the FBI, the Secret Service, and various technology vendors to convene 16 "Ransomware 101 Workshops" around the US. More than 3,000 businesspeople attended these events, the purpose of which was to raise awareness of ransomware threats and educate organizations about how to prevent and counter them.

FS-ISAC also conducts conference calls and publishes best practices papers written by cybersecurity experts. Members share information in multiple ways, including over a secure member portal, through specific email distribution lists, and via automated machine-to-machine indicator sharing. All sharing is governed by FS-ISAC's operating rules and sharing agreements and filtered through circles of trust and the Traffic Light Protocol (a color-coded labeling method for information sensitivity). Much of the sharing is done anonymously.

Of course, manually entering information in a portal will never be sufficient to keep up with all the threats. In 2014, FS-ISAC and the Depository Trust & Clearing Corporation teamed up to create Soltra (a company now owned by NC4), which enables cyber-threat intelligence to be shared in a structured, automated format.

Essentially, FS-ISAC collates the threat information, and NC4 provides a mechanism for anonymous information sharing, which is helpful to other companies and supports the various cybersecurity frameworks. Firms may receive more than 1,000 alerts a day—some come as a descriptive package providing information about the threat, while others are more structured.

Centripetal Networks is another company that works with FS-ISAC to operationalize threat intelligence for the financial sector and to educate staff. In his first term, President Obama wanted an on/off switch for the internet that could be deployed at the ISP level to shield the US from a foreign attack. Centripetal Networks' technology was developed to solve this issue through a DHS project, similar to the types of projects done by the Defense Advanced Research Projects Agency. The solution was not deployed because of privacy concerns, so it was repackaged and marketed to enterprises.

"At the ISP level, the device had to be extremely fast," explains Parnell. "We didn't want to introduce any latency into the network, but we wanted to be able to take down huge swaths of the internet if there was an attack on the US."

The solution checks every data packet at high speed, looking for any type of traffic that matches cyber-threat intelligence. There are two parts to the intellectual property: the high-speed algorithm and a purpose-built appliance. Centripetal Networks designs and manufactures most of the components used in the construction of the appliance (including the motherboard, architecture, and power supplies) in the US.

"We couldn't just buy an appliance from China and put this high-speed algorithm on there without realizing there might be a supply-chain impact," says Parnell. "The financial sector likes the box because we have full control over the manufacturing of the hardware, as well as the high-speed algorithm."

The high-speed boxes sit at the access points of the companies. They look for specific types of traffic, which are either blocked or logged and then later reviewed by an analyst. The boxes are deployed at both top-tier firms and smaller organizations. Although Centripetal Networks' strength has proven to be in working with the top 50 financial firms, it recently performed a successful proof of concept with a small bank to ensure the solution works on a smaller scale.

Centripetal Networks also recently performed a threat assessment at a large hedge fund. It installed a physical appliance in the firm's location to review traffic going through the network. Then it interpreted the data and provided weekly reports that included contextual information and suggestions for remediating infections.

According to a 2015 study by Frost & Sullivan, the global shortfall of trained cybersecurity professionals will reach 1.5 million in five years. Because a hybrid skillset is needed for this role, many types of experts are taking part in the decision-making, problem-solving, and response effort. Lawyers determine how much information can and should be shared with others, including government agencies. Corporate communications staff manage reputational risk and answer queries from customers about the effectiveness of the response to cyber-events.

Finance professionals can apply their knowledge and skills, too, especially if they have an enterprise IT management background. They can help to bridge the gap in understanding between the board of directors and the operating organization, as well as between the IT organization and the business. When a financial firm is hacked, it may be necessary to take a server offline—a move that could disrupt the business. That type of decision may have to be made by an interdisciplinary team.

"There is no perfectly secure network," says Parnell. "You need to be able to determine the acceptable level of risk that your organization will allow, balancing the cost of security and the impact your organization is willing to accept."

Sherree DeCovny is a freelance journalist specializing in finance and technology.