Protecting the Financial Services Organization: How to Defend Against Cyber Criminals in an Increasingly Digital World

Traditional security methods are proving futile against today’s highly organized gangs of cyber criminals. This is especially the case for financial services firms, where too much is at stake to take chances. Needed: a security solution with centralized controls that responds swiftly to real-time threat data—so that your data is protected wherever your people are.

INSIDE

Your Cybersecurity Checklists

Cyber Crime Is on the Rise

The Race Is On

Traditional Defenses Don't Work

Stop Cyber Crime with Juniper Networks
Executive Overview

Financial services have become a digital business. To some extent this is true of all industries, but the speed and extent of the transformation of the financial sector has been breathtaking. Technologies like blockchain are opening up the space to new competitors. Automation and artificial intelligence (AI) are disrupting a previously stable workforce. Customers are more demanding, and their loyalty is tenuous. And serious cyber threats are coming from all directions.

Once the domain of individual freelance criminals, organized crime gangs now control the financial services cyber crime market. A decade ago, approximately 80% of black-market cyber criminals were independent loners, with the remaining 20% consisting of organized crime factions.¹ That statistic has been turned upside down. These highly organized gangs of experienced fraudsters operate in the same manner as traditional organized crime families and are proving to be even more elusive to prosecution. Their attacks are highly sophisticated, constantly evolving, increasingly evasive, and carefully orchestrated by experienced fraudsters who have access to infinite resources.
Simultaneously, rapid technology innovations and digitization have completely transformed financial services. Although boosting business efficiency and effectiveness, these technical advancements also open many vulnerable back doors to cyber exploits. Blockchain, with its ability to store information on distributed ledgers without a central clearinghouse, is upending markets. Artificial intelligence now drives the way leading firms provide everything from customer service to investment advice. Robotic process automation (RPA) is creating armies of digital workers, or “bots,” that are emptying out the busy trading rooms of the largest brokerages.

In short, the cyber crime market and the financial services business environment have both changed radically in recent years. Traditional security methods are proving futile. It is imperative that the strategies and technology used to safeguard company networks, data, and overall brand and reputation keep pace with would-be attackers to ensure the timely detection and remediation of attacks.

Although no bank, insurance firm, or brokerage house company can protect itself 100% from cyber exploits, we provide checklists of key security best practices that significantly reduce your risk of becoming the next victim.
Your Cybersecurity Checklists

The No. 1 attack vector for financial services firms in 2017 is still phishing, with 43% of such businesses reporting this kind of attack. According to PwC's Global State of Information Security Survey 2017, other serious considerations for financial services include the complexity of emerging technology (37%), threats from foreign attackers (35%), and lack of clear guidance from regulators (33%).²

Recognizing who your true adversaries are will help you formulate a new strategy for securing your networks and data—in short, your business. You need to change both your perspective and your security strategy going forward.

For starters, begin thinking like a cyber criminal. Get into the mindset of an organized fraudster intent on breaking into a financial services firm like yours. And come up with a holistic cyber defense that is fast, intelligent, automated, and adaptive to meet the specific cyber threats facing your particular industry.

On the following pages, we present trends in financial services cyber security to be aware of, as well as four checklists to follow to make sure your security defenses meet all these criteria.

Phishing is the No. 1 attack vector for financial services firms in 2017:

43% report attacks

Other serious security considerations for financial services:

- Complexity of emerging technology (37%)
- Threats from foreign attackers (35%)
- Lack of clear guidance from regulators (33%)
Cyber Crime Is on the Rise

Organized criminals have elevated cyber crime into a flourishing underground economy where the barrier for entry is low and the payouts are large.

A full 75% of the top 20 U.S. commercial banks (by revenue) are already infected with malware, while 95% of the top 20 U.S. commercial banks (by revenue) were given a network security grade of “C” or lower by PwC in its 2016 study of security in the financial services industry. Then there’s the fact that one in every five financial institutions uses an email service provider with severe security vulnerabilities.

The top 20 U.S. commercial banks (by revenue):

75% are infected with malware.

95% were given a network security grade of “C” or lower by PwC in its 2016 study of security in the financial services industry.
Highly orchestrated gangs of experienced fraudsters operate in the same manner as traditional organized crime networks—and are proving to be even more elusive to prosecution by law enforcement. Everything from money laundering to untraceable payment methods to spoofed domains are weapons in their formidable arsenals. They use “straw” businesses to launder their profits, which are often paid in untraceable bitcoins to secret overseas accounts.

Financial services firms are rushing to place more and more critical workloads in the cloud—47% of all their IT services are now delivered via the cloud. They’re also venturing into open source and the Internet of Things (IoT). All this brings exciting innovations to both the front and back office, but also opens up tremendous vulnerabilities.

Security experts warn financial services firms that we now live in a continuous state of compromise. It isn’t a question of if you will be hit by cyber crime, but when.

**Vulnerability of financial services firms:**

*47% of IT services are delivered via the cloud.*

Cyber crime is expected to become a **$2.1 trillion problem** by 2019. This represents more than the gross domestic product (GDP) of Canada.

In 2016 alone, more than **4 billion records** were stolen by cyber criminals.
Intelligent

When asking yourself if your network is prepared for the onslaught of cyber criminals, the first criteria is intelligence—not just human but digital. Financial services security professionals must place themselves in the mindset of organized criminals and invest in intelligent security tools that proactively resist criminal countermeasures.

A Juniper-sponsored study by the Rand Corp. found that cyber criminals succeed at countermanding traditional security tactics such as sandboxing and anti-phishing frameworks. Financial services firms must look to more advanced security solutions to protect their networks.\(^7\)

Do we have the intelligence we need built into our network security measures?

- Our firewall policy enforcement is automated.
- We have deployed multifactor authentication.
- We use automated patch management and monitoring.
- We have isolated our sub-networks.
- We have adequate network access control.
- Our integrated security solution can detect threats inside the network as well as at end points.
- We feed real-time threat data into our network policy engines.
Adaptive

In 2017 we expect to see not only a record number of attacks but also record-breaking losses—including DDoS attacks that result in a 1-terabit data breach. Insurance giant AIG puts financial services firms at No. 1 risk of getting hit by a systemic cyber attack over all other industries in the coming 12 months. AIG experts also say to expect a “mass” DDoS attack that will bring down multiple financial institutions in 2017. Experts suggest that a key factor driving this explosion in number and size of attacks is the growing base of IoT devices used in financial services firms: intelligent devices like ATMs, card readers, and other devices that are connected and often vulnerable. Organized crime is capitalizing on these new ports of entry by investing in evolving attack scenarios, advanced persistent threat tactics, and dynamic malware exploits. Security technology must prove as agile and adaptive as the malicious attacks launched by organized crime.

Can we adapt?

- Our security solution is as agile and adaptive as the malicious attacks being launched by organized crime.
- Our security solution has policy engines that are fueled by real-time threat data.
- Our security solution has flexible and customizable controls that allow us to respond swiftly to new threat variants.
The Race Is On

Financial services firms find themselves in a virtual “arms race” with cyber criminals. Reaching into their deep pockets, which contain virtually unlimited resources, organized crime gangs can invest in the latest innovations and hire some of the world’s brightest computer minds to develop cyber threats of ever-increasing sophistication and scale.

Unsurprisingly, 86% of financial services firms plan to spend more on cybersecurity in 2017, according to a Duff & Phelps survey. Compared to 2016, when less than 60% of firms said they were spending more, this shows a sharpened awareness of the risks.10

But, just like legitimate internet businesses, organized cyber criminal gangs are creating new revenue streams by offering cyber crime services for hire. Ransomware-as-a-service, fraud-as-a-service, and extortion-as-a-service are now commonplace offerings on the “dark web.” By commercializing malware kits and offering as-a-service packages, criminals have also lowered the barrier to entry into this lucrative market for others.

Legitimate financial services businesses simply can’t keep up.
Fast

One study of worldwide financial institutions found that a single security incident could be so swiftly executed that it could cost as much as $1.2 million. Top concerns of financial institutions are phishing/social engineering attacks on customers (53%), local/branch offices (33%), digital/online banking services (31%), core transactional/back-office systems (23%), and point-of-sale systems (20%).

Most telling of all, two-thirds of the banks surveyed said they had fallen victim to some type of financial fraud in the last few years.

With their unlimited financial and human resources, organized crime gangs move at the speed of light. Their attack mechanisms and countertactics elude detection by the traditional security measures used by financial services firms. These attacks are being launched both outside and inside the network.

Do we have the speed we need to stay ahead of them?

- We have a rapid-response solution in place to immediately act on any perceived threat—whether from within or outside the network.

- Our centralized control system is capable of speeding deployment of patch management and streamlining policy enforcement across the network.

- We have protections woven into the fabric of the network—and not only at the end points—enabling the fastest response rate to a detected attack, regardless of its location on the network.
Traditional Cybersecurity Doesn’t Work Anymore

Financial services security professionals are struggling to keep up with cyber criminals. The state-of-the-art environments they are deploying—and charged with protecting—are designed to streamline business processes and accelerate revenues. But they also leave their organizations exposed to dangerous cyber adversaries.

The impact has been devastating. Although financial insurance companies continue to invest in cybersecurity, they don’t have the same resources as their foes. According to Gartner, spending on cybersecurity increased by 7.9% in 2016, topping $81 billion as organizations scrambled to stay ahead of cyber criminals.14

Approximately one in 10 financial services firms says investing in artificial intelligence is a top priority, according to one study. They are deploying AI-enhanced robotic process automation (RPA), natural language processing, and blockchain across their business-critical operations. AI is also being used to address rising security concerns.

Yet 2016 turned out to be a record year for cyber crime. We saw the largest data breaches to date, an explosion of DDoS attacks, and an off-the-charts number of ransomware variants. Legitimate financial services simply can’t keep up with the criminals.

Traditional security methods no longer apply. Companies need a unified network security platform to gain the upper hand.
Automated

Financial institutions are at the forefront of automation, replacing many traditional jobs with “bots” that possess artificial intelligence capabilities. But they also need to automate their network to stay on top of the security threats.

Although organized criminals have the leisure that comes with deep financial backing, many financial services businesses possess only limited budgets and are forced to do more with less. This makes automation essential.

Just as when using automation in the front office increases efficiency and reduces errors, automated security updates to the network have proven less prone to countermeasures by organized criminals. Such updates also increase operational efficiency.

Have we completed necessary essential automation?

☐ We have invested in automated solutions.

☐ We have improved operational efficiency.

☐ We can do more with less personnel.

☐ We orchestrate streamlined delivery of enterprise applications with customized security.

☐ Our automated responses to attacks speed up our ability to detect and respond to cyber exploits.
Stop Cyber Crime with Juniper Networks

As the cyber crime market and business environment have dramatically changed in recent years, and so must the strategies and technology used to safeguard the company networks, data, and brand reputation of financial services firms.

Juniper’s innovative security approach detects and remediates threats faster, safeguarding your financial services business from today’s cyber crime. Protect your virtual and physical environment with end-to-end, automated, and intelligent defense using Juniper’s Software-Defined Secure Network (SDSN).

To achieve cybersecurity that truly defeats cyber crime, go to Juniper Networks’ security solutions page.
Quick Reference: Your Cybersecurity Checklists

### Intelligent

Do we have the intelligence we need built into our network security measures?

- Our firewall policy enforcement is automated.
- We have deployed multifactor authentication.
- We use automated patch management and monitoring.
- We have isolated our sub-networks.
- We have adequate network access control.
- Our integrated security solution can detect threats inside the network as well as at end points.
- We feed real-time threat data into our network policy engines.

### Adaptive

Can we be as agile as the malicious attacks launched by organized crime?

- Our security solution is as agile and adaptive as the malicious attacks being launched by organized crime.
- Our security solution has policy engines that are fueled by real-time threat data.
- Our security solution has flexible and customizable controls that allow us to respond swiftly to new threat variants.

### Fast

Do we have the speed we need to stay ahead of organized crime gangs?

- We have a rapid-response solution in place to immediately act on any perceived threat—whether from within or outside the network.
- Our centralized control system is capable of speeding deployment of patch management and streamlining policy enforcement across the network.
- We have protections woven into the fabric of the network—and not only at the end points—enabling the fastest response rate to a detected attack, regardless of its location on the network.

### Automated

Have we completed necessary essential automation?

- We have invested in automated solutions.
- We have improved operational efficiency.
- We can do more with less personnel.
- We orchestrate streamlined delivery of enterprise applications with customized security.
- Our automated responses to attacks speed up our ability to detect and respond to cyber exploits.
You aspire to cloud-like functionality. Juniper helps you get there by simplifying your journey, providing a secure environment where you can build without limits. It’s cloud excellence for all organizations within the financial services industry.

Juniper Networks challenges the status quo with products, solutions, and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable, and secure networks that provide agility, performance, and value. Additional information can be found at Juniper Networks, or connect with Juniper on Twitter and Facebook.

For more information, go to www.juniper.net/security.

Citations: