White Paper

Cyber Security for Financial Services: Vulnerabilities, Threats, and Defenses

The Financial Sector Security Landscape in 2021

Since the earliest days of civilian computing, the financial services industry has led the adoption of new information technologies to serve its customers. Today, the search for a competitive edge drives financial firms to explore technologies to drive out cost, improve performance, and deliver new products and services, all while retaining customer trust.

As they innovate, financial firms face new challenges—some brought on by the advancing technologies themselves:

Proliferation of Internet-connected devices, work-from-home initiatives, and new digital banking services are increasing the "attack surface" of financial firms and raising the cost and complexity of defense.

Cloud computing allows cyber criminals to build global botnets that steal processor power, launch phishing and distributed denial of service attacks, and cover their tracks.

Cryptocurrencies open avenues for instantaneous, anonymous payment of extortion demands in targeted ransomware attacks that encrypt or threaten to disclose sensitive information.

Near-field communications, authentication protocols, and wireless networks can be hacked or spoofed, exposing both financial firms and their customers to impersonation and theft.

Social media put the personal information and relationships of financial employees and customers online, ready for exploitation in phishing, spoofing, and extortion attempts.

New financial technology (fintech) firms are inserting unproven, opaque payment technologies into millions of consumers' mobile devices, connected to legacy bank systems through application programming interfaces (APIs).

And far from fading away, many of the "old" challenges to the industry keep getting more complicated:

Regulations like the California Privacy Rights Act and the EU General Data Protection Regulation raise the costs of compliance, and the impact of any breach.

Improved efficiency of services—accelerated by digitization—makes it easier for customers to split their business among multiple firms, or leave for a competitor.

Generational changes in the customer base and changing consumer behaviors drive demand for nontraditional services and delivery models.

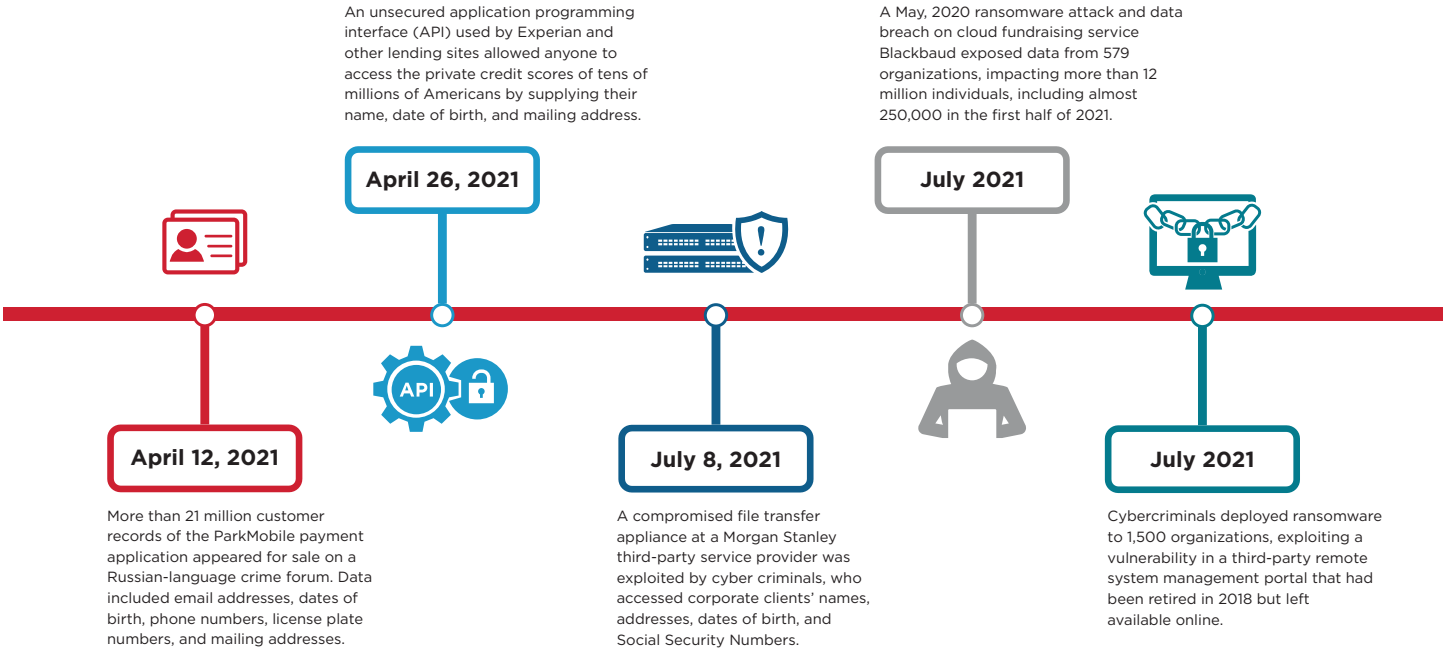
Fragmentation of financial business operations and IT systems raises the cost of innovation at established financial services firms, exposing them to upstart competitors.

Banks and other financial institutions navigate this complex landscape by adopting mobile, cloud, social, and other technologies to stay competitive, and by delivering the airtight security and privacy their customers rightly expect. The costs of failure are high: penalties, lawsuits, lost revenue, brand damage, compromised credit, and broken trust. Held to a higher standard because of their fiduciary role and the vast amount of sensitive data they keep, financial firms must make sure the customer experience they deliver is not only engaging and efficient, but private and safe.

Financial Services in the Crosshairs

Financial services are a $20+ trillion global market, and industry networks process an unfathomable volume of sensitive information. It's no wonder that financial services organizations are the leading targets for cyber attacks, accounting for more than a quarter of such attacks in the US. And although they spend more on cyber security than firms in other industries, they are often victims as well. According to the PwC 2020 Global Economic Crime and Fraud Survey, cybercrime follows consumer fraud in the most common economic crimes reported by financial services firms. A sample of recent breaches above shows the range and scale of vulnerabilities and thefts.

Figure 1: Timeline of Recent Security Breaches



Compounding the difficulties of attack frequency, the variety of attack types and pathways make security a moving, mutating target. Financial services organizations operate under siege, with IT and security teams struggling to collect, alert, and interpret malicious events. Many financial services organizations are turning to outside organizations for security intelligence and other services—PwC reports that 36% of industry data breaches are now reported by outside monitoring services.

The Threat Landscape in 2021

This section outlines some of the trends affecting the financial-sector threat landscape during 2020 and 2021. Some will no doubt prove to be ripples from the dramatic changes in mobility and online activity occasioned by the COVID-19 pandemic, others continuations of long-term trends—only time will tell.

Social Engineering Takes the Lead

Social-engineering attacks have been gaining on Web Application attacks for years, and have finally emerged as the leading source of data breaches. Phishing ranks above business email compromises, pretexting, spam, and other social attacks, accounting by itself for more than 36% of all data breaches in 2020 according to Verizon, up nine points year-over-year. Most phishing emails try to steal credentials for hacking, fraud, or outright sale in online criminal markets.

Fewer and fewer phishing attacks are the old-style broken-English appeals from a bank you never heard of with a dodgy e-mail address. For C-level and other well-placed targets, cyber criminals take the time to mine company websites, industry press, news reports, and social-media accounts to understand and exploit financial executives' networks of business and personal relationships.

Ransomware on the Rise

Multiple industries were hit with ransomware attacks in 2021. Famously, Colonial Pipeline and JBS Foods paid the DarkSide and REvil gangs, respectively, millions of dollars for data decryption keys. Ransomware is the most dangerous, disruptive, and expensive form of cyber attack, in part because every successful extortion breeds future attempts. Even when the ransom is not paid, the costs of recovery are enormous—more than $600M in the case of Ireland's health service, even though the Conti ransomware gang released the decryption key without collecting ransom.

The Human Touch: Miscellaneous Error

We focus here on cyber crimes, but PwC ranks miscellaneous errors by company insiders in the top four causes of data breaches across all industries. Misconfiguration of systems by administrators and developers is usually the culprit. But in financial services—as in other industries that rely on mass communications to keep customers informed—misdelivery of electronic and physical mail accounts for 55% of error breaches, and 13% of breaches overall.

No major breaches of financial firms were reported in 2021, but there may be cases that didn't make the news: financial firms have powerful incentives, and sometimes explicit policies, not to report breaches or ransom payments. What's more, their systems and culture of confidentiality makes it easier to underreport.

Supply-Chain Attacks

In March, 2020, a hacked update of SolarWinds network management software—likely state-sponsored—compromised thousands of corporate and government networks, illustrating a serious and often overlooked vulnerability. Cyber defenses of major financial firms are world class, on a par with military commands and intelligence services. But these firms rely on large networks of third-party providers for operational, IT, and security services—and the providers may not be as vigilant as their clients. What's more, it's fundamental to providers' business models that they serve multiple institutions—so a successful attack up the supply chain gives hackers lots of leverage.

Although the SolarWinds attack goals weren't financial, the 2021 attack through Kaseya Ltd.—another management software provider—was the single biggest global ransomware attack on record.

"Live Off the Land" Tactics

Security researchers are seeing increased use by hackers of legitimate software to access information undetected. Windows Management instrumentation and similar network administration and management tools evade signature-based antivirus and intrusion-prevention defenses, but are just as useful to manipulate servers and corrupt or exfiltrate data.

Web App Attacks at Industrial Scale

Web App attacks are simple, high-frequency automated attacks on Web application or mail servers, usually to mine credentials for sale or use in subsequent attacks—some also attempt to repurpose the apps as bots. They continue to be a popular attack method, with organized crime their most enthusiastic user. Financial firms report billions of these attacks per year, and thousands are successful. According to Verizon, phishing, miscellaneous errors, and Web App attacks together account for 81% of financial industry data breaches.

Watering Hole Attacks

Watering hole attacks are indirect, infecting websites known or suspected to be visited by employees of the real target—for example, the 2016 hack of Poland's Financial Supervision Authority website, targeting Polish banks. The compromised site redirected only visitors from preselected IP addresses to a customized exploit kit, which attempted to install malware on the selected targets.

Distributed Denial of Service Attacks

Distributed denial of service (DDoS) attacks are among the oldest, most common, and easiest to mitigate threats on the Internet. Because they target system availability, they rarely result in data exfiltration—Verizon counts only 4 breaches from 14,335 attacks during 2020. But they can be used as smokescreens to draw attention away from more targeted attacks. Most DDoS attacks are weak—trying to "overwhelm" websites with traffic in the range of 1Gb/s. DDoS protection services are both effective and inexpensive—a rare bright spot on the cyber security landscape.

Underworld Organizations

The underground financial fraud community has become increasingly well-organized, with markets on the dark web selling data, tools, and services. Organized gangs operate with impunity, ignored or protected—and sometimes sponsored—by jurisdictions out of the West's regulatory reach. And recently, underground groups like REvil have started offering "ransomware as a service"—selling advanced network takeover and encryption software to other gangs in exchange for a share of the ransom the gangs use it to extort.

Managing Information Security Risks

Financial services today are mobile, online, and in the cloud; the concept of a secure perimeter is a thing of the past. With each new partner, customer, and business alliance, that network extends further, and grows more porous. Establishing an IT governance program that integrates people, processes, and technology across this extended network is vital to mitigate risk, reduce operational costs, and ease the burden of regulation. The recommendations below will supplement what you're doing already to protect your networks, data, and people.

Protect Critical Data Assets

For years, financial services firms focused on preventive controls: firewalls, intrusion prevention, secure gateways, and vulnerability testing. But even rigorous programs may leave blind spots such as:

- Incomplete discovery of sensitive data in data stores, and on endpoints or attached devices.
- Inadequate processes such as health checks, policies, and solution setup issues.
- Inadequate integration of data protection into change management, database and IT asset management processes.

- Poor coverage of intermittently attached data stores, such as laptops temporarily attached to networks or USB drives temporarily attached to endpoints.

Bigger walls to block out malware won't address these cases. And as we've seen, many social-engineering and "live off the land" attacks don't involve malware at all. Finally, the varieties and vectors of attack change so fast, today's protection may be tomorrow's vulnerability. A more realistic approach is to make your organization cyber-resilient: well-defended, certainly, but also able to respond quickly and smoothly when those defenses fail. A Data Loss Prevention solution can discover, monitor, protect, and manage critical data wherever it is stored or used, protect it by encryption on mobile endpoints, or de-identify it to trigger Safe Harbor exemptions in cases of suspicious movement.

Prepare for Targeted Attacks

The financial services industry will always be the focus of targeted attacks. Even organizations with strong IT security solutions may be vulnerable to zero-day, phishing, and watering-hole attacks that evade signature-based security.

The pace of zero-day attacks has increased in 2021, reflecting increasing sophistication of cyber criminals, and increased availability of zero-day exploits in dark web markets. Highly targeted "spear" phishing attacks are also on the rise, narrowly focusing on a few well-placed targets with persuasive appeals. Attackers also refined highly selective watering-hole attacks, targeting only a narrow range of companies they want to attack.

Financial institutions should defend themselves against these attacks with advance warning, managed response, hardening of high-value targets, and employee awareness. Technical solutions include the following:

- Threat awareness data feeds that automate and correlate network and endpoint security logs with feeds from:
  - Information about immediate threats and risks.
  - IP, reputation, URL, and domain information.
  - Data about vulnerabilities and risks as they are discovered by security services.
- Managed response from experienced teams at companies that provide cyber security as a service.
- Hardened infrastructure to lock down systems like ATMs, and limit what even users with full privileges may run on them.

Partner with Experts

An attack on one institution may be part of an attack on the industry. Partnerships share attack information across industry stakeholders, so that all financial firms can enhance their cyber resilience. Two organizations that promote sharing are the Financial Services Sector Coordinating Council (FSSCC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Training and Simulation

Employees are often the weakest link in a firm's security chain, so employee training is a fundamental defense. Financial services firms should cultivate a culture of security through employee awareness and training programs. A best practice is to educate employees in both business and personal IT security—the intersection of the two is large, and the benefits are mutual.

Financial firms can take training and simulation one step further by integrating their fraud, cyber, IT, physical security, and product development teams. Leveraging diverse talent to improve intelligence and responsiveness, financial firms can achieve more effective threat awareness and faster mitigation. Frequent tabletop exercises and an annual full-scenario run-through gives such teams the knowledge and experience they need to perform when called on during an attack.

Neutralize Third-Party Risk

Nearly all financial firms are now extended enterprises. As financial firms raise formidable defenses of their own networks and assets, attackers increasingly target their IT supply chains and partner networks. The SolarWinds and Kaseya breaches reveal the limits of implicit trust in, and self-certification by, third parties. Financial firms should demand that providers join them in active risk monitoring and mitigation, and periodically evaluate their effectiveness.

Enable Mobile Security

Digital and mobile banking surged during 2020, with so many customers in every age group using mobile apps that many financial firms are building their strategies around them. Accenture predicts that stand-alone banking applications will become submerged in more general "lifestyle apps," citing China's all-purpose mobile apps as a bellwether. But location-independent devices, whether run by financial institutions or third parties, open new security vulnerabilities, such as the following:

- Untested or insecure mobile applications that may leak data or serve as platforms for attack.
- Inadequate device and network authentication protocols, granting unauthorized users access to data.
- Inconsistent protection of information on employee, customer, and company-owned devices.

A full-fledged solution will manage mobile security from end to end, including:

- Application code that assures applications developed in-house are free from vulnerabilities.
- Strong authentication and certificate management across devices, applications, and users, including multi-level access control by identity and role, and expansion of customer access controls.
- Data protection solutions on shared devices, for example tablet computers used by staff and customers at branch offices.
- Two-factor authentication options available for high-value or high-sensitivity transactions or as a customer benefit.

Next-Generation Financial Security

Financial services firms to date have been reactive on security issues, defending against the types of attacks that have already occurred. Getting ahead of them will require raising information security capabilities to operational excellence—a challenge when budgets and skilled labor markets are stretched. Fortunately, frameworks are emerging that take information security back to first principles, and acknowledge the challenges introduced by mobile and cloud computing environments.

Zero Trust and Secure Access Service Edge

Zero Trust (ZT) is a security model popularized by Forrester Research, now being standardized by the National Institute of Standards and Technology (NIST), National Cyber Security Center of Excellence (NCCoE), and promoted by many security analysts and solution providers. ZT is based on the principle that in today's hybrid environments, prior authentication of individuals and devices is insufficient evidence to establish their current trustworthiness. It relies on continuous authentication of user and device identity, validation of device integrity, and restriction of permissions according to the user's role and context of the request.

Secure Access Service Edge (SASE), introduced by Gartner, is a simplified security solution for cloud and hybrid architectures. It emphasizes delivery of security as a service directly to the source of a network connection, the "service edge," to eliminate backhauling latency and costs.

ZT and SASE principles are directly relevant to the sprawling hybrid networks typical of modern financial firms, extending throughout their supply chains and to customers' mobile devices. Financial firms would do well to monitor the lively discussion of these principles in the industry press, and apply them when relevant.

Advanced Authentication

Advanced authentication offers much greater protection than traditional security and anti-fraud approaches. It is individualized for each user, and so resists the industrial-style automation of mass attacks. More than just identity management, advanced authentication monitors user attributes and behaviors to keep imposters from accessing infrastructure and data. Attributes include users' normal locations, devices, applications, and configurations. Behaviors include items such as users' typical access time of day, recent browsing history, and path through the site.

Advanced Automation

Automation of security response and mitigation has lagged behind monitoring and alerting, but is due for a change. Merging feeds, log data, and human intelligence into a sophisticated threat detection and discrimination mechanism sets the stage for automated response. For example, upon identifying a bad actor by IP, URL or any other security control, an automated solution can not only block the activity and send an alert, but isolate the affected system from the network, image it for forensics, rebuild it to a known good state, and bring it back online.

Big Data Analytics/Security Intelligence

Financial firms collect enormous volumes of security information, including endpoint and network device logs, asset databases, user data, and more. Data-mining and visualization techniques, accelerated by rules-based engines and machine-learning algorithms, can identify high-risk device and behavior outliers with sensitivity unknown yesterday. Traditionally a labor intensive process, cyber crime analysis will increasingly use Big Data—powerful, real-time analytics across structured and unstructured data sets to improve the quality, speed, and economy of cyber threat analysis.

Conclusion

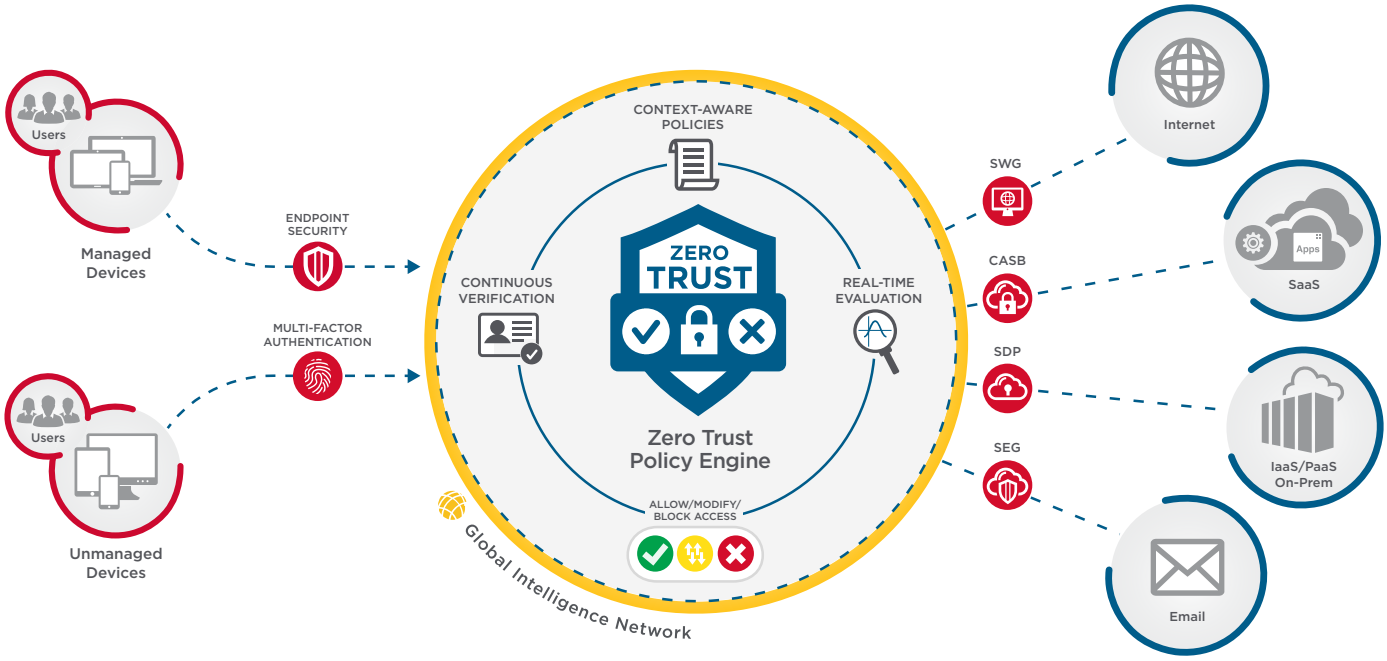
Confronted with stringent regulations and fragmented line-of-business operations and pressured by increased competition and changes in consumer expectations and behavior, financial services firms are adopting new strategies in order to innovate and modernize. Financial institutions are looking to take advantage of mobile, cloud, social, and other technical trends in order to reignite growth and build customer trust, but must also contend with evolving and increasing complex cyber threats.

IT Security plays a strategic role in providing the cover financial services firms need in order to conduct business efficiently and securely. By forging strong security and risk management programs, IT Security empowers financial firms to innovate and compete with confidence.

Symantec Offers Technology, Capabilities, and Experience

Symantec solutions address the security and compliance challenges the financial services Industry now faces. The company is dedicated to providing solutions to secure, automate, standardize, and streamline operations and transactions, and is a pioneer in security and data-protection solutions aligned to Zero Trust and Secure Access Service Edge concepts.

Figure 2: Zero Trust Policy Engine



Symantec
A Division of Broadcom

For more product information: broadcom.com

Sec-Fin-Services-WP100 October 1, 2021