Symantec White Paper

Cyber Security for Financial Services:

Strategies that Empower your Business, Drive Innovation and Build Customer Trust

Confidence in a connected world.

Symantec™

Empowering Innovation: Transforming Information Security for Business Agility

The financial services industry has a long history of providing exceptional value and deep confidence in a world of risk. Today, the intense competitiveness of financial services demands a constant search for cost-effective ways to improve performance and deliver new, innovative products and services to meet customer demands while retaining loyalty and trust. However, as financial services organizations forge new initiatives to drive business growth they are navigating a landscape marked by numerous challenges.

- New regulations that have imposed stringent financial and consumer protections are increasing regulatory compliance risks.
- Fragmentation at the line-of-business level and siloed business operations are hampering collaboration and innovation.
- Generational changes in the customer base and changing consumer behavior is driving demand for new services and product delivery models.
- Digital competitors that have already made their mark in serving customers who value convenience and innovation over personalized service are encroaching on market share and accelerating the need to "go digital."
- The recent financial crisis and slow recovery has slowed the pace of IT investments.
- Escalating and increasingly sophisticated cyber attacks are impacting financial services firms and eroding consumer trust.

Facing a need to change with the times, financial institutions are adopting new business strategies. As financial services leaders undertake initiatives to modernize their products and services, an even more vigilant approach to managing financial, reputational and legal/regulatory risks will be required.

Technology as the Foundation for Innovation

As banks and other financial institutions take advantage of mobile, cloud, social and other technical trends to reignite growth and rebuild customer trust, several competing forces come into play: the need to innovate quickly, decrease IT complexity and deliver an unparalled customer experience – all while providing the airtight security and digital privacy that customers expect.

Against a backdrop of constant change, cloud, mobile and emerging technologies provide a foundation for innovation in products and services that support increased productivity and broader operational capabilities. However, cyber criminals are also using the same technologies to launch increasingly damaging attacks, such as:

- Cloud-based botnets that takeover processing power.
- Exploitation of Near Field Communications, which banks are using for new services.
- Distributed Denial of Service (DD0oS) attacks launched via the cloud, thereby increasing their intensity and impact.
- Hacks on multifactor authentication technologies, fostering disruption and fear among customers.

As financial firms chart new paths, the high cost of failure comes into play, such as regulatory penalties, class-action lawsuits, lost revenue, brand damage and diminished shareholder faith. Held to a higher standard because of the nature of the industry and the vast amount of sensitive data that is involved, they must ensure that their services not only offer an unparalleled customer experience, but are also secure.

Information security empowers innovation

The ability to operate in the digital world depends on the ability to maintain a trusted environment. Against this backdrop, IT Security plays a strategic role. By forging strong security and risk management programs, IT Security empowers financial firms to innovate, compete with confidence and build market share.

Financial Services in the Crosshairs for Cyber Attacks

Financial services organizations operate large, mission-critical networks that process seemingly endless volumes of sensitive information. It's no wonder that financial services organizations are in the crosshairs for cyber attacks. The industry has the biggest data centers, the most transactions—and the highest IT security and regulatory compliance risk exposure. According to the 2014 Global Economic Crime Survey published by PricewaterhouseCoopers, cybercrime is one of the most common types of economic crime reported by financial services respondents—38 percent in 2011 versus 39 percent in 2014. One only has to look at a sampling of data breaches to know that confidential customer data and proprietary intelligence is increasingly subject to theft:

- JPMorgan Chase (83 million accounts)
- Heartland Payments Systems (134 million accounts)
- Global Payments, Inc. (1-1.5 million accounts)
- Citigroup (360,000 accounts)

Compounding the situation is the fact that the velocity, volume and variety of attacks make security a constantly moving target. More and more, financial services organizations are operating under a constant state of attack, leaving IT and security teams challenged in their ability to collect, disseminate and interpret malicious events. As they strive to manage an almost unmanageable volume and complexity of threats, it will become imperative that financial services organizations proactively seek help from outside agencies for actionable intelligence.

Cyber threats – fighting a battle on many fronts

The underground financial fraud community has become increasingly organized, facilitating an expanded reach. Trojans targeting financial institutions have become one of the most prevalent threats on the internet today. As reported in the 2014 Symantec State of Financial Trojans report, the number of financial Trojans dropped by 53 percent in 2014. However, the number of infections of Zeus and its variants grew by ten times from 2012 to 2014. Financial Trojans compromised 4.1 million users' computers. Analysis of the configuration files for these Trojans reveals that customers of 1,467 institutions are being targeted. Nearly 95 percent of these organizations belong to the financial sector, spanning a broad range of institutions.

As new mobile technologies expand the attack surface, attacks will continue to grow rapidly. Android banking Trojans, such as the Android.iBanking Trojan, specialize in stealing banking information by intercepting SMS messages and continue to make the rounds.

Email remains a significant attack vector for cybercriminals, but there is a clear movement toward social media platforms. In 2014, Symantec observed that 70 percent of social media scams were manually shared. These scams spread rapidly and are lucrative for cybercriminals because people are more likely to click on something posted by a friend.

Finally, the Depository Trust Clearing Corporation (DTCC) has named Distributed Denial of Service attacks as one of the three types of attacks that pose a "systemic risk" to the financial system. Often used as a smokescreen for more targeted attacks, DDoS attacks against financial institutions show no signs of abating. Rather, they are growing in intensity and frequency. As reported in the Symantec 2015 Internet Security Threat Report, DDoS traffic saw peaks in April and July of 2014, and there was a 183 percent increase in domain name server (DNS) amplification attacks between January and August 2014.

Web App attacks continue to be a popular method for attackers, with organized crime being the most frequently seen threat actor. According to the 2015 Verizon Data Breach Investigation Report, 95 percent of these incidents involve harvesting credential stolen from customer devices, then logging into web applications with them. Within the financial services industry, end-user devices were a factor in 82 percent of incidents and nearly a tenth of them involve some human element, such as phishing or social.

Unwitting insiders place organizations at risk

Hackers, organized crime groups and nation-states are clearly forces to be reckoned with, but it's the unwitting insiders who are the most-cited culprits of cybercrime. Many times they unknowingly compromise data or jeopardize information security by circumventing security practices in favor of productivity or through the loss of mobile devices. Equally concerning, employees lacking a security mindset can easily fall victim to targeted phishing schemes.

Hidden risk in the business ecosystem

Not to be overlooked is the risk that third-parties bring to the table. In today's interconnected business ecosystem, the security posture of partners, vendors and other critical third parties can have a tremendous impact on the risk posture of today's financial services firm.

Impact of a Cyber Security Breach

Information security is more and more becoming a board-level issue. Almost half (48 percent) of respondents to PwC's 2014 Global Economic Crime Survey said the perception of cybercrime risk to their organization had increased the past year, up from 39 percent in 2011. However, that being said, only 41 percent of financial services respondents believe it is likely that they will experience cybercrime in the next 24 months. Recognizing that today's cyber attacks have become a serious enterprise risk-management issue, it is imperative that business leaders are sufficiently informed on the state of information security within their organization to be able to assess those risks and their potential impact to the business.

Quantify the cost

Historically, organizations have used the established cost-per-record amount to quantify the costs of a data breach. Calculated by dividing a sum of all lost estimates by total records lost, this formula estimates a cost of $201 per record in 2014, compared to $188 in 2013. These expenses covered detection, escalation, notification and after-the-fact response, such as offering data monitoring services to affected customers.

While this approach has the advantage of being easy to calculate, remember and apply, it fails to account for the differences between smaller and large-scale breaches. Larger organizations, for example, have higher losses per breach because they have more records and thus higher overall costs. As insurers become increasingly uncomfortable estimating potential losses using a standard cost-per-record model, organizations are encouraged to apply new breach-cost models that both fit the industry data and account for uncertainty as the record volume increases.

Long-term domino effects

Beyond the immediate financial impact, the consequences of a data breach can extend from brand and reputation damage to loss of revenue, degraded consumer confidence, lower share prices and greater regulatory scrutiny.

Insure against cyber risk

A cyberattack can result in a business experiencing serious financial losses and enduring extensive litigation. Having adequate insurance that at least partially covers cyber security incidents could be a major factor in recovering successfully from a cyber-related incident. As such, it should be considered an important component of any organizational cyber risk management strategy.

Information Security a Business Risk Management Issue

The ability to respond appropriately to a cyberattack can mean the difference between a business's success and failure. Driven by resilient and relentless hackers, cyber criminals and nation states, today's attacks are increasingly sophisticated and complex. In order to get ahead and stay ahead, security practices must go beyond keeping pace with the constantly evolving threat landscape. Doing so will demand constant attention and ongoing investments to prevent, protect, detect and respond to security risks.

It is vital that financial services organizations invest in personnel, processes and technology to understand and monitor the various threat actors who may be motivated to disrupt core business functions. Further, information security is more than a challenge for the IT department. Given the evolving nature of cyber threats and the importance of cyber resilience to the business continuity of financial services organizations, information security merits board-level attention. The broader C-suite must therefore be involved for the organization to become more secure.

Building Confidence in Information Security

Today, business is conducted online. Gone are the days when one can build a perimeter and trust it to be secure. With each new partner, customer and business alliance, the network is extended, becoming more and more porous. Establishing an IT governance program that integrates the people, processes and technology is vital to delivering the foundation of security needed to drive business innovation while mitigating risk, reducing operational costs and easing the burden of regulation.

Protect critical data assets

Many financial services firms have focused on implementing preventative controls such as firewalls, perimeter security, vulnerability testing and intrusion prevention. However, in a fast-changing threat environment, even highly sophisticated organizations may suffer from blind spots, leaving themselves vulnerable to:

- ***Incomplete discovery*** of confidential data in data stores and on endpoints and attached devices.
- ***Inadequate processes*** such as health checks, policies and solution setup issues.
- ***Inadequate integration*** of data protection into ongoing change management, database and IT asset management processes.
- ***Patchy coverage*** of data stores, especially of endpoints that may be temporarily attached to networks and devices that temporarily attach to endpoints.

Gaps in security coverage are hard to justify when valuable, sensitive and regulated data is at risk. However, we have come to a point where financial organizations have to recognize the fact that they are going to be compromised sooner or later. Minimizing the risks of future cyber-attacks requires a fundamental change in the way we approach security—from "building bigger walls" in an attempt to block out all malware, to a more realistic approach that focuses on making your organization cyber-resilient. Beyond the basics, a Data Loss Prevention solution is recommended to discover, monitor, protect and manage confidential data wherever it is stored or used, augmented by encryption solutions to protect data on mobile endpoints, or to trigger Safe Harbor exemptions in cases of suspicious data movement.

Prepare for targeted attacks

The financial services industry is literally "where the money is," so it is the prime focus of targeted attacks. Even organizations with strong IT security solutions may be vulnerable to zero-day or phishing attacks that evade signature-based security. Advanced attackers continue to favor zero-day vulnerabilities to silently sneak onto victims' computers, and 2014 had an all-time high of 24 discovered zero-days.

The annual Symantec Internet Security Threat Report documents phishing attacks in 1 out of every 965 emails and one in 1,126 websites were found to be infected with malware. In 2014, attackers continued to breach networks with highly targeted spear-phishing attacks, which increased 8 percent overall. They used less effort than the year before, deploying 14 percent less email toward 20 percent fewer targets. Five out of every six large companies were targeted with spear phishing attacks in 2014, a 40 percent increase over the previous year.

Attackers also perfected watering hole attacks, making each attack more selective by infecting legitimate websites, monitoring site visitors and targeting only the companies they wanted to attack.

As financial institutions prepare to defend themselves against adversaries, the areas of greatest need include:

- ***Advance warning*** of impending attacks, reducing requirements for slow, reactive firefighting or expensive mitigation.
- ***Context of potential attacks*** to operationalize, automate and prioritize processes to identify attackers' mission, funding and target.
- ***Establishing a security mindset*** among employees to close vulnerabilities from gaps in personnel knowledge or awareness.

Solutions include:

- ***Threat awareness*** data feeds to automate and correlate network and endpoint security logs with feeds of:
  - » Information about immediate threats and risks.
  - » IP, reputation, URL and domain information.
  - » Data about vulnerabilities and risks as they are discovered.
- ***Managed response*** from experienced teams providing cybersecurity as a service.
- ***Hardened infrastructure*** to lock down systems—for example ATMs—and limit what even users with full installation privileges may run on them.

The importance of partnerships

An attack on one institution may signal an attack on the industry at large. By building partnerships, sharing attack information and collaborating with industry stakeholders, financial firms can further enhance their cyber resilience. Shared human intelligence about the activities of adversaries, focused on the industries they are targeting, benefits the industry as a whole. Two key organizations are the Financial Services Sector Coordinating Council (FSSCC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Training and simulation

Because people are often the weakest link in the security chain, employee training is a fundamental component of every program. Financial services firms should look to cultivate a culture of security through employee awareness and training programs. A best practice is to educate employees both in terms of business IT security and personal IT security – the crossover between the two is too large to ignore personal security behavior.

Financial firms can take training and simulation one step further by building cyber "fusion centers" that integrate the fraud, cyber, IT, physical security and product development teams. By leveraging diverse talent to boost intelligence and speed response, financial firms can reduce costs while achieving more efficient and faster threat awareness and mitigation. Conducting frequent small-scale table top exercises and an annual full scenario run-through gives teams the knowledge and experience needed to perform when called upon to respond to an attack. Looking ahead, financial services firms will borrow from the military wargaming exercises in order to adopt better approaches to preparation and simulation testing.

Neutralize third-party risk

Nearly all businesses can now be viewed as extended enterprises. As network perimeters have hardened, attackers are increasingly targeting the IT supply chain and partner network. As self-certification processes are proving less reliable, financial firms are encouraged to shift to active cyber-risk monitoring and mitigation with third parties in order to neutralize third-party risk.

Enable mobile security

Mobile is at the core of banking—in five years, three of every four customer interactions will be online or mobile. Financial firms know they must move to mobile platforms or risk losing an entire generation of consumers to new, digital-native startups. But location-independent devices open a new set of security vulnerabilities, such as:

- ***Untested or insecure applications*** on mobile devices that may leak data or be vulnerable to misuse or attack.
- ***Inadequate authentication*** on devices and networks, granting unauthorized users access to data stores.
- ***Inconsistent protection*** of information on employee devices, customer devices, and company-owned devices used in branches and elsewhere.

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

- ***Application code*** to assure that 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 for high-value or high-sensitivity transactions, or available as a customer benefit.

Mature Capabilities to Operational Excellence

The measures taken in most financial services firms have been largely reactive, designed to defend against the types of attacks that have already occurred. Getting ahead of the threats, however, will require maturing information security capabilities to operational excellence. It requires assuming that attackers are already inside the network. It requires defenders to actively hunt for potential intrusion in their environments using all available intelligence. And it also requires the analysis of large quantities of data in order to uncover previously hidden attack methods.

Advanced authentication

Advanced authentication offers much greater protection than traditional security and anti-fraud approaches. A key advantage is that it is individualized for each user, and as a result resists the industrial-style automation that characterizes mass attacks. More than just identity management, advanced authentication methodologies monitor users' 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 the users' typical access time of day, recent browsing history and path through the site.

Advanced automation

Automation of security response and mitigation processes has lagged behind monitoring and alerting, but is due for a change. Once feeds, log data and human intelligence are combined into a sophisticated threat detection and discrimination mechanism, the stage is set for automated response. For example, upon identifying a bad actor by IP, URL or any other security control, an automated solution could not only block the activity and send an alert, but also isolate the affected system from the network, image the system 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 much more. Modern data-mining and visualization techniques, accelerated by rules-based engines and machine-learning algorithms, have the potential to identify high-risk outliers with sensitivity unknown today. Traditionally a labor intensive process, cybercrime analysis will increasingly leverage the use of Big Data. The use of powerful, real-time analytics across multiple data sets – both structured and unstructured – will vastly improve the quality and speed of real-time cyber threat analysis while greatly reducing overall cost.

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 contend with evolving and increasing complex cyber threats.

IT Security plays a strategic role in providing the cover that 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 market, security and compliance challenges now facing the financial services Industry. We are dedicated to giving our customers the solutions they need to secure, automate, standardize, and streamline operations and transactions.

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Confidence in a connected world. Symantec™