Symantec White Paper

Cyber Security for Retail Services:

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

Confidence in a connected world.

Retail's Changing Landscape

Retailers are facing a new, digital era as the forces of social media, omni-channel shopping and a wave of emerging payment technologies are transforming the industry. With few exceptions, retailers are facing:

- ***Explosion of choice*** – consumers can effortlessly and on a moment's notice select alternative products, product/service bundles, channels, stores and price points.
- ***Consumer disappointment*** – limited in-store experiences are driving an increase in "showrooming" behavior, wherein consumers "shop in-store, buy online".
- ***Rising digital influence threatening store loyalty*** – consumers feel better connected to coupons, promotions and competitive offers than they do to store associates.
- ***Channel conflict*** – pure digital competitors developing "brick-and-mortar-style" augmented-reality apps, social shopping and same day delivery are accelerating the need to "go digital".
- ***Mobility*** – consumers expect mobile store navigation, product information, recommendations and coupons – and prefer brands and stores that offer them.

Forge new initiatives, security practices

Against this rapidly evolving digital retail landscape, retailers find themselves to be poorly defended targets of escalating and increasingly sophisticated cyber attacks. In the past, the retail industry has narrowly framed IT security as "checkbox compliance" with Payment Card Industry (PCI) data-protection requirements and delegated responsibility to stores. Now, changing consumer attitude to security breaches demands new focus on security. Requirements to comply with PCI, SOX, HIPAA and state privacy regulations make data protection critical.

Retailers can no longer afford to ignore security issues; however, they are hindered by employee turnover, distributed operations, limited staffing and insufficient IT resources. Facing a need to change with the times, retailers are slowly embracing technology and adopting new approaches to both business and security. As they undertake initiatives to modernize their products and services, an even more vigilant approach to protecting customer data and guarding against data breaches will be required.

Retailers Are – And Always Have Been – Attractive Targets

Cybercrime is big business and retailers are attractive targets. Traditional retail metrics that focus IT attention on initiatives to maximize store performance over security have left retailers with gaps in defenses. Combine inadequate security with large repositories of customer data and retailers are ripe for attack. One only has to look at a sampling of data breaches to know that customer data is increasingly subject to theft:

Retailer	Damage	Means of Access
Neiman Marcus	350,000 payment cards	Malware implanted through outside attack
Michaels Arts and Crafts	2.6 million payment cards – 7% of all cards used at Michaels	Eight-month intrusion through PoS systems at some stores
Sally Beauty Supply	Company acknowledges 25,000+ payment cards exposed; outside estimates run to 282,000	Methods closely resemble those used in the Target breach
P.F. Chang's China Bistro	Customer data exposed at 33 restaurants	Targeted attack on PoS system

Attacked from within

According to the PricewaterhouseCoopers 2015 Global State of Information Security Survey, the number of detected incidents in 2014 increased 19 percent over 2013. The criminal element is clearly a force to be reckoned with, but there is an increase in respondents who point the finger at unwitting and malicious employees. According to the report current employees (34 percent) and former employees (30 percent) account for the most incidents.

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 third parties can have a tremendous impact on a retailer's risk posture. The PwC study reports a 27 percent jump in incidents attributed to third-party service providers, contractors, suppliers and business partners, which often have trusted access to the company's network and data.

Now it's getting even worse – a wakeup call for retailers

While the industry has suffered data breaches before, 2014 marked a turning point for retailers. Threats became more persistent and dynamic. By all indicators, these threats will only increase, possibly due to the financial services industry improving its defenses against cybercrime. The scale and sophistication of the attacks also increased. In 2014 attacks exposed more records than ever before, and used highly sophisticated vectors to penetrate defenses. The consequences are also increasing. Before 2014, the blame typically fell on IT, but now Boards, customers and the media are demanding accountability in the C-Suite.

Compounding the situation is the fact that October 2015 brings an end to the magnetic stripe "swipe-and-sign" credit card. With the introduction of EMV, a new chip-and-pin payment system that is less vulnerable to compromise, hacking attacks will be more difficult to pull off. With a source of easily monetized payment card information disappearing, fraudsters are stepping up their game. The flurry of attacks may be a "last gasp" of easy card-cloning fraud before a shift to web-based (card-not-present) attacks.

Gaps in IT Retail Security

Retail IT Security has often been reactive and underfunded; however, gaps in security are now becoming a critical issue. From a technology perspective, retailers have historically taken a checkbox approach to PCI compliance. Compliance-driven security has resulted in incomplete data protection and poorly integrated point solutions spread over a wide geographic area. Further, endpoint security is often neglected on Point-of-Sale systems due to challenges in implementation, maintenance and training. With limited staffing and conflicting priorities, retailers are challenged in combating security threats. In principle, responsibility for IT security cannot be delegated, but many retailers still delegate key security activities to auditor, contractors and stores. Finally, many retailers lack a governance process and focus instead on regulatory compliance at the expense of a framework that governs information.

> To defend themselves against cybercriminal assault and protect their reputations with consumers, retailers must fill technology, staffing and process gaps to bring their IT security posture up to par with that of other industries.

Point-of-Sale Security Contributes to Risk

Cybercriminals have an insatiable thirst for credit card data. Given that large retailers may process thousands of transactions daily through their POS and there is a thriving market for stolen credit card data, it stands to reason that POS terminals are in the crosshairs of cybercriminals.

Thriving marketplace for stolen cards

Credit card information continues to maintain its value on the underground market. Today, prices for stolen credit card information range between $0.50 and $20. The price can depend on a number of factors, such as the brand of the card, the amount of metadata provided, volume discounts and how recently the card data was stolen.

POS Security Issues

Despite improvements in card security technologies and PCI-DSS requirements, there are still gaps in the security of POS systems:

- ***Accessibility*** – breaches have occurred by gaining direct access to POS systems as well as through the corporate network.
- ***Lack of point-to-point encryption (P2PE)*** – credit card numbers are not encrypted in the POS system and can still be found in plain text within the memory of the POS system.
- ***Software vulnerabilities*** – many POS systems are running older operating systems, such as Windows XP or Windows XP Embedded, which are more susceptible to attack.
- ***Susceptibility to malicious code*** – As many POS systems are running a version of Windows, they are capable of running any malware that runs on Windows.

Innovations in Payments

Advances in technology, combined with the need to step up security, are altering the way payments are made. The industry is shifting from traditional magnetic stripe technology to payment innovations that include EMV, P2P encryption for mobile payments, Near-field Communications (NFC) and mobile wallet.

Major card networks have set an October 2015 deadline for implementation of EMV technologies. According to the Aite Group, by the end of 2015 an estimated 71 percent of US credit cards and 41 percent of debit cards will be EMV-enabled. It's anticipated that mobile payment will dramatically redefine the payments industry as more people use mobile apps that take advantage of the phone's near-field communications to interact with the POS terminal.

New Technologies: Fuel Innovation, Introduce Risk

As retailers take advantage of mobile, cloud, social and other technical trends to connect with customers and drive market share of the digital wallet, 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 retailers are using for new services and payment methods.
- Distributed Denial of Service (DDoS) attacks launched via the cloud, thereby increasing their intensity and impact.
- Hacks on multifactor authentication technologies, fostering disruption and fear among customers.

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 retailers to innovate, compete in the digital world with confidence and build market share.

Burden of Compliance (PCI-DSS) Adds to IT Security Challenges

Compliance with the Payment Card Industry Data Security Standard (PCI-DSS) continues to improve. However, with four out of five companies still failing at the interim assessment, it's clear that PCI compliance still has a long way to go. Complicating matters, the PCI-DSS itself continues to evolve. In January 2014, version 3.0 of the PCI-DSS became effective, putting in place new requirements for the design, implementation and maintenance of secure systems and networks and the management of vulnerabilities. Organizations may face both technical and nontechnical challenges when addressing PCI-DSS v.3.0 compliance requirements. Among the most significant potential pitfalls are:

- Scale and complexity of requirements.
- Uncertainty about scope and impact.
- Failure to involve the business side of the organization and lack of insight into existing business processes.
- Failure to prepare for PCI-DSS compliance activities.
- Storage of prohibited sensitive data types.

Challenging Situation, Substantial Stakes

Not surprisingly, the mega, high-profile data breaches have made information security a board-level issue. However, despite the ongoing publicity of retail breaches, companies continue to be slow to elevate security to a Board-level discussion. Only 39 percent of respondents to PwC's 2015 Global State of Information Security Survey say their Board participates in the overall security strategy. 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

Large retailers suffering data breaches can expect to find themselves facing expenses in the double- and triple-digit millions. The average cost of cybercrime attacks per organization in the United States is estimated at $12.69M. These expenses include detection, escalation, notification and after-the-fact response such as legal, consulting, card replacement and credit monitoring fees. Slow reaction and delays in notification, however, can drive expenses even higher.

Long-term domino effects

Beyond the immediate financial impact, the real business consequences of a data breach to a retail organization may be the hit to customer loyalty and trust as well as brand and reputation damage. Retailers may face lower profits, increased reputation-control costs, consumer-monitoring services fees, class-action lawsuits, lower share prices and greater regulatory scrutiny. Not to be overlooked are the costs associated with executive turnover.

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. Cyber insurance policy premiums are "not one size fits all." Premiums are factored on a company's services, data risks and exposures, computer and network security, privacy policies and procedures and annual gross revenue. Implementing strong risk-management strategies will reduce the likelihood that your business experiences a data breach, and may even reduce your cyber insurance premiums.

Cyber 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. Now more than ever, information security is more than a challenge for the IT department. With the evolving nature of cyber threats and the importance of cyber resilience to the business, information security merits board-level attention. The broader C-suite must therefore be involved for the organization to become more secure.

What Can Retailers Do?

Strategic processes are often lacking within retail IT security organizations. Because an effective security program will require top-down commitment, security executives must align themselves to the needs of the business and take proactive steps to ensure that executive leadership and the Board understand the importance of security to the organization.

Establish IT governance

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 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.

Invest in training

Because people are often the weakest link in the security chain, employee training is a fundamental component of every program. Retailers 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.

Neutralize third-party risk

As network perimeters have hardened, attackers are increasingly targeting the IT supply chain and partner network. Retailers should look to evaluate third-parties based on the risk they present to the business. Because self-certification processes are proving less reliable, retailers are encouraged to shift to active cyber-risk monitoring and mitigation with third parties in order to neutralize third-party risk.

Leverage the NIST framework

The NIST Cybersecurity Framework integrates cybersecurity practices that have been developed by the National Institute of Standards and Technology (NIST) and the International Standardization Organization (ISO). The Framework comprises a risk-based compilation of guidelines and provides organizations with an assessment mechanism designed to help them determine their current cybersecurity capabilities, set goals and establish a plan for improving and maintaining cybersecurity programs and practices. These practices include processes, procedures and technologies such as asset management, alignment with business strategy, risk assessment, access control, employee training, data security, event logging and analysis and incident response plans.

The Framework casts the discussion of cybersecurity in the vocabulary of risk management. As a result, it creates a common language for the discussion of cybersecurity importance and goals with executive leaders and Board members. The Framework may also set cybersecurity standards for future legal rulings. Organizations that adopt the Framework at the highest possible risk-tolerance level may be better positioned to comply with future cybersecurity and privacy regulations.

Commit to ongoing investment

Compared to industries such as financial services, manufacturing or media and entertainment, retail traditionally places a much lower priority on IT Security. Faced with a need to cut costs and make a profit against slim margins, most retailers opt for meeting the basic standards set forth by the payments card industry. A key finding from the PricewaterhouseCoopers 2015 Global State of Information Security survey shows that information security is a mere 3.7 percent of the IT budget. In order to get ahead of the threats retailers must step up and commit to ongoing investment.

Benefit through industry partnerships

By building partnerships, sharing attack information and collaborating with industry stakeholders, retailers can further enhance their own cyber resilience and help protect the industry as a whole. Two key organizations are the Retail Cyber Intelligence Sharing Center (R-CISC) and the Information Sharing and Analysis Center (ISAC). To facilitate information sharing among retailers, the National Retail Federation (NRF) launched a Retail Cyber Intelligence threat alert subsystem in consultation with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the U.S. Department of Homeland Security.

Build Trust through Information Security

Over the years, guided by recommendations from PCI auditors, many retailers have invested in a variety of tools. However, the practice of purchasing individual tools to solve narrow “checkbox” compliance problems has left retailers with a confusing patchwork of point solutions that are difficult to monitor and untrustworthy in a crisis. Further, insufficient staff adds to the problem. Even with advance notice of suspicious activity on the network, retailers with limited staff may be hard-pressed to adequately respond to intrusions. Retail has become a high-value, low-risk target for cyber criminals. Retailers need to mobilize quickly and take steps to address the IT and data security deficiencies and protect critical data assets.

Consolidate data protection

As hackers become more advanced and persistent in their efforts, retailers are left to play catch-up in their cyber security investments. Most retail organizations have focused on implementing basic security technologies such as firewalls and intrusion detection, antivirus for PCs on corporate networks and email gateway security. Despite these efforts, they 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.

Minimizing the risks of future cyber-attacks requires a fundamental change in the way retailers approach security. In addition to consolidating the patchwork of data protection solution already in place into an extensible suite of technologies, retailers should consider:

- *Endpoint protection* to prevent incursion through Point-of-Sale terminals.
- *Encryption* to protect data even when it resides on portable devices.

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.

Move beyond data protection to remediate other vulnerabilities

Digital technologies have become a pervasive part of the shopping experience and winning retailers will deliver integrated, seamless experiences to customers across channels and platforms. However, these digital technologies introduce new entry points for attack and retailers must move beyond fundamental blocking and tackling strategies in order to remediate vulnerabilities at headquarters and store networks such as:

- ***Mobile devices*** – legacy devices running customer software, new tablet and phone applications and customer shopping apps may all leak data or be vulnerable to misuse or attack.
- ***Inadequate authentication*** – in retail stores where staff turns over quickly, inadequate access controls on devices and networks may grant unauthorized users access to confidential data stores.

Retailers are encouraged to implement a full-fledged solution to manage security across the extended network, including stores and mobile networks, covering:

- ***Application code*** to assure that applications running on point-of-sale terminals, inventory-control systems and checkout scanners are free from vulnerabilities.
- ***Strong authentication and certificate management*** across devices, applications and users, including multi-level access control by identity and role.
- ***Two-factor authentication*** options for high-value or high-sensitivity transactions, for example any action that changes access permissions.

Partner with experts for success

Securing a network of retail systems and stores dispersed across geographies can be a daunting task. Due to inadequate staffing even retailers that are PCI compliant and have the best tools to monitor for suspicious activity can be challenged in recognizing and acting on security issues before they become full-blown attacks. By partnering with a Managed Security Services provider to augment staff, retailers can achieve state-of-the-art 24/7 monitoring and managed response from experienced teams, all while controlling costs. A Managed Security Service provider, adhering to a proven, multi-tiered approach to data security can help mitigate business, financial and reputation damage from a data breach.

Defend Against Targeted Attacks

To combat data breaches, many retailers have taken steps to beef up policies and procedures as well as implement new IT security solutions and infrastructures for payment systems. However, 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 2015 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.

The Retail industry is systematically being targeted, possibly because it is recognized as both a softer target than the Financial Services industry and as a richer source of consumer information. It is also much easier to monetize customers' payment-card information than insurance or banking records, especially with the rise of underground information markets. As retailers prepare to defend themselves against adversaries, they can most benefit from:

- ***Advance warning*** of impending attacks to reduce requirements for slow, reactive firefighting or expensive after-the-fact mitigation.
- ***Context of potential attacks*** to operationalize, automate and prioritize processes to identify attackers' mission, funding and target.
- ***Establishing a security mindset*** among employees – particularly at stores where employee training and "churn" are significant challenges.

Solutions include:

- ***Threat awareness*** data feeds to automate and correlate network and endpoint security logs.
- ***Managed response*** from experienced teams providing cybersecurity as a service.
- ***Hardened infrastructure*** to lock down systems—for example Point-of-Sale terminals – and limit what even insiders with full privileges may run on them.

Mature Capabilities to Operational Excellence

Getting ahead of the threats will require maturing information security capabilities to operational excellence. Any decentralized organization with a high "churn rate" of inexperienced staff needs to consider automating processes that grant access to systems and data, or respond to unauthorized access or suspicious behaviors. Retail firms can mature capabilities to operational excellence by employing advanced behavioral authentication, Big Data analytics and security response automation.

Advanced behavioral authentication

More than just identity management, advanced authentication methodologies monitor users' – in this case headquarters and store employees' – 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 authentication offers much greater protection than traditional security and anti-fraud approaches. Automated behavioral authentication can clear authorized users and flag suspicious behavior, reducing security event false alarms and misses. A key advantage is that it is individualized for each user, and as a result resists the industrial-style automation that characterizes mass attacks. Further, self-learning capabilities adapt to users' behaviors without time-consuming and error-prone configuration or training.

Big Data analytics

Retail firms collect – but rarely use – 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, data breach analysis will increasingly leverage the use of Big Data. Deep analytics consolidate all security information into a single, powerful predictive model. Big data analytics can characterize and ring-fence "typical" behavior over a broad data landscape and alert the security team to "atypical" events. Unified security based on Big Data will transform IT Security, but requires a technology partner with a broad array of compatible solutions to accelerate development and deployment of this next-generation security solution.

Security response automation

Automation of security response and mitigation processes has lagged behind monitoring and alerting, but it can be appropriate in retail environments where dedicated security staff is few and responsibilities are diffuse. 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 block the activity and set up an alert if the attack is repeated. Automated security response is the next step in security automation, as security events become a routine part of IT operation. By offloading routine response and mitigation efforts, security teams can focus on less-frequent, more dangerous attacks.

Conclusion

Emerging digital technologies and services are redefining the retail industry. As retailers navigate the digital waters and embrace innovations in payment technology, they must contend with evolving and increasingly complex cyber threats. Information security is no longer an option and short-term savings of non-investment are not worth the potentially substantial losses that result from a data breach. Retailers must fill technology, staffing and process gaps to bring their IT security posture in line with that of other industries. Recognizing that cyber security is not a core competency, retailers are encouraged to partner with experienced service providers that offer optimized managed network security solutions and ongoing threat intelligence. By forging strong security and risk management programs, IT Security empowers retailers to innovate and compete with confidence while reducing risk and building customer trust and loyalty.

Symantec Offers Technology, Capabilities and Experience

Symantec solutions address the market, security and compliance challenges now facing the retail 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™

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo, Veritas, and the Veritas Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. 06/15. P/N 21352891.