WHITE PAPER

Strong Security for a Brighter Future in Retail

Executive Summary

Retailers have long understood that the customer is king. From a security standpoint, that leaves stores responsible for protecting not just their own data, but their customers' crown jewels as well. It's a demanding proposition, made more complex by omnichannel initiatives, the rise of mobile payments and the need to gain better customer analysis from big data scattered across cloud and on-premises systems.

Since 2013, national news stories have regularly featured the details of major retail cyber breaches. Government scrutiny of the retail industry's cybersecurity protection measures and breach notification requirements has increased as well. Corporate boards, executives, and security directors all know that threat actors constantly attack retailers. Yet many retailers large and small remain underprepared to identify, contain and mitigate cyber threats.

After a sluggish start in early 2016, consumer spending is bouncing back, driving retailers to change and innovate in some exciting areas. Technology is at the forefront and remains central to enhancing the customer experience, improving customer relationships and optimizing retail operations. Savvy retailers are weaving IT security into the fabric of their businesses, instead of using information security solutions and services simply as a series of data locks and surveillance sitting on top of critical systems. From the merging of physical and digital systems to serve omnishoppers, to the migration to single-view retail management systems and cloud-based apps, to the use of big data and mobile payment options, security is central to the future of retail.

What You Will Learn

- How to enhance retail innovations with security
- The importance of risk assessment
- How to bridge the gap between security awareness and action
- Why communication and training are vital

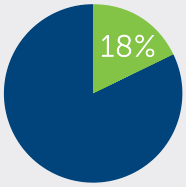
Who Should Read This White Paper

» CISOs/CSOs
» CIOs
» Directors of Security/IT
» Security Architects

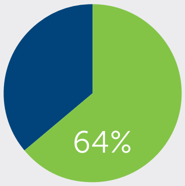
Take Steps to Secure Your Customers and Your Innovation

How does your business connect to the Internet to make money and run operations? It may sound like a simple question, but vulnerabilities can arise whenever you conduct online transactions with customers and suppliers, introduce new in-store devices, adopt new cloud-based environments or allow for employee logins. Any of your current business processes or new innovations can become a pathway for hackers to exploit, particularly in times of rapid expansion, international growth, or mergers and acquisitions.

Faced with a massive attack surface and a barrage of unknown threats, your level of strategic and operational preparedness can set you apart, make you more resilient to cyber threats and ensure that you retain customer trust. The following steps can help you stay secure without constraining the ability to innovate and grow.



Percent of IT security professionals who believe their company's cybersecurity program is in a "mature" stage.[1]



Consumers who would likely end their relationship with an organization after their personal information had been exposed.[2]

[1] Ponemon Institute, *2015 Global Study on IT Security Spending & Investments*, June 2015

[2] Walker, Zak, Rippleshot, "The Impact of Data Breaches and Customer Loyalty," December 17, 2015

Step 1: Assess Your Risk, Test and Repeat

The journey to resilience starts with determining what you're protecting and who holds the keys. For retailers, the answer is obvious — customer data, credit card account information, credentials and other personally identifiable information are highly sought after on the black market. What's more, your employees, partners and other third parties often have access to this valuable customer data.

The Europay, MasterCard and Visa (EMV) mandate will help prevent credit card fraud, but it's not a panacea. Many retailers are struggling to maintain inventory levels, pricing systems and order fulfillment between channels while using different systems for their stores and online businesses. Hackers scan for vulnerabilities wherever someone connects to the Internet — whether it's massive enterprise systems, the POS, in-store mobile devices, a supplier's network or an employee's tablet.

Start by assessing what data you are storing, where it resides and who can access it. For sensitive financial information, grant access only to the most limited set of people who need it, and place stringent policies and controls around its use. Administrator credentials are a hacker's keys to the kingdom — the more people who have them, the more avenues for attack.

Testing is a crucial and ongoing component of an effective security program. Engage qualified security experts that will emulate hackers using real techniques and evasion methods to validate your security effectiveness across networks, endpoints and mobile technology. Regular penetration testing should include phishing techniques to identify weaknesses in the human side of your security program.

Even if you're meeting Payment Card Industry Data Security Standard (PCI DSS) compliance mandates each year, it's more important to measure the effectiveness of your security program against real-world attacks. Compliance frameworks like PCI DSS can provide a helpful and rigorous security baseline, but never assume that meeting a compliance mandate (or even passing a compliance inspection) will protect you from an attack.

Regular penetration testing reveals how hackers might penetrate your defenses. It provides rich and actionable insight you can use to calculate actual risk, create an incident response strategy and allocate cybersecurity resources accordingly. Whether your retail business is small and local or global and complex, assessment and testing will assist with the compliance process and help you prioritize and implement security more effectively.

Step 2: Bridge the Gap Between Awareness and Action

With retail breaches dominating headlines, you're probably aware there's a problem. But how do you go from understanding your risk to combatting chronic cyber attacks — especially ones that are pervasive, persistent, and staged across time and infrastructure? Retailers need four key capabilities to effectively manage a cycle of ongoing threats: the ability to **prevent**, **detect**, **predict** and **respond**.

Prevent What You Can

Information security professionals now know that eliminating the possibility of a breach is an unrealistic goal. Prevention technologies like firewalls are an essential first layer of defense that can recognize and stop known threats. However, highly adaptive threat actors continue to adjust their tactics and toolkits. Even layered security technology can no longer provide a complete defense. An effective security program accounts for eventual compromise and takes steps to rapidly identify, contain and eradicate threats inside the network.

Detect What You Can't Prevent

Some of the most damaging retail data breaches went unnoticed for a significant duration of time, enabling cybercriminals to steal reams of customer data. Modern retailers need strong security technology, processes, programs and staff to help detect threats quickly. Ask your security team these critical questions: "Do we know if hackers are inside our defenses today? How do we know and how did they get in?"

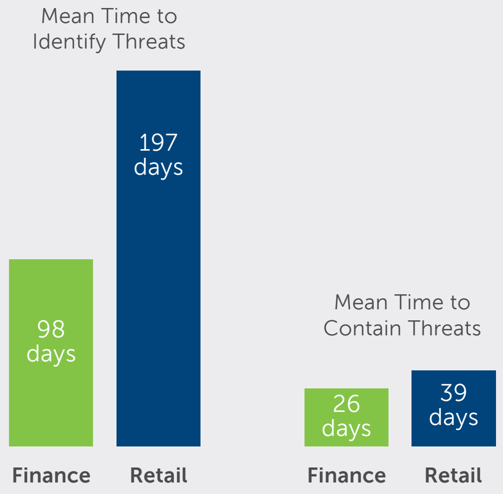
Adequate security tools are required in order to pinpoint threat activity on the network, and across endpoints, POS terminals, mobile devices and cloud-based applications. You are already trying to gain more visibility into your customer data across channels for greater insight into their path to purchase.[3] In the same way, enterprise security visibility is essential to your cybersecurity strategy because it helps you respond to unusual activity more quickly, reducing down time and related costs.

Predict What Will Happen Next

To make retail sales predictions, business leaders apply internal and environmental intelligence to test their assumptions. The same applies to cybersecurity risk. Your security team needs to apply threat intelligence to determine the intent and capabilities of current, real-world hackers who may be targeting your organization. This means keeping tabs on global cyber threat intelligence, threat activity related to your industry and the threat statistics and activity on your own network.

Analyzing real-time threat intelligence gives you predictive capabilities. It enables your security team to strengthen defenses in the most critical areas, detect more intrusions and contain threats earlier in the attack timeline. Gathered from your own security environment and often supplemented with broader, deeper intelligence from a third party, threat intelligence helps you zero in on the threats that need immediate attention.

Comparison of Advanced Threat Detection and Response in Retail Industry vs. Finance Industry



Source: Ponemon Institute, Advanced Threats in Retail Companies: A Study in North American and EMEA, May 2015

Respond Rapidly And Effectively

More accurate cyber threat predictions lead to faster response and recovery with less effort. By recognizing a hacker's tactics early on, you can more easily develop a containment strategy and eradicate the threat. Even if a breach results in significant compromise, higher visibility and faster prediction provide you with the facts you need to quickly control the loss, determine disclosure requirements, communicate with customers and manage your reputation more effectively.

Your ability to respond to a threat quickly and effectively relies heavily on having a practiced your cybersecurity incident response plan (CIRP). Make sure your CIRP outlines how you will communicate and work with third parties, security providers and law enforcement.

Step 3: Keep Security Top of Mind with Your Employees and Partners

For the first time ever, cybersecurity concerns are top of mind for all retailers[4]. Up to now, many retailers may not have wanted to call attention to the risks posed by

[3] Ponemon Institute, *Advanced Threats in Retail Companies: A Study in North American and EMEA*, May 2015
[4] Business Wire, "100 Percent of Retailers Disclose Cyber Risks," a BDO USA Report, May 11, 2016, http://www.businesswire.com/news/home/20160511006412/en/100-Percent-Retailers-Disclose-Cyber-Risks-%E2%80%94

cybercriminals. One of the most powerful defenses against cyber attacks is an informed and vigilant workforce. A successful security program relies on employees, partners and suppliers having strong awareness of security policy and an understanding of their role in supporting security and privacy.

Top Risks for Retailers — 2016[4]

Risk	Rank	Percent Cited
General Economic Conditions	#1	100%
Privacy Concerns Related to Security Breach	#1 (tie)	100%
Competition and Consolidation in Retail Sector	#3	98%
Federal, State and/or Local Regulations	#4	96%
Natural Disasters, Terrorism and Geo-Political Events	#5	94%
Implementation and Maintenance of IT Systems	#6	93%

Instead of relegating security to the boardroom and IT, make communication about risk and prevention strategies a priority with your employees and partners. Hackers know that humans are a particular point of weakness in any organization's defenses. Because most workers are helpful and trusting, the hackers employ attack techniques to exploit these qualities, such as socially engineered emails that contain malware, phishing techniques that seek access to credentials, and even phone scams designed to elicit private customer lists.

Your security program should include employee training on security for everyone, from the boardroom to the mailroom. It should also clearly communicate security requirements to business partners and other affiliates. These components are just as vital as security technology in preventing attacks.

The senior leadership team, information security team, lines-of-business leaders, legal department, public relations department and employees all have distinct roles in protecting customer data and the enterprise, and minimizing damage if a breach occurs. Security awareness training helps ensure that your internal resources understand the policies and procedures for keeping sensitive data safe.

For retailers, there's an important external communication function as well. Should a breach occur, you must be prepared to communicate with the public, customers, regulators, shareholders and law enforcement. Legal requirements about the notification process differ by state and country. Plus, how a breach is disclosed, whether by a retailer proactively reporting it or a media outlet leaking the story, can significantly affect brand reputation and customer loyalty. You do not want to define your communication strategy in the aftermath of a breach. The more sound approach is to engage in a continuous process of assessment, prevention and response that includes an ongoing conversation with employees, partners and executives about the importance of security.

Conclusion

Even as the financial sector remains the most heavily targeted by cyber threats, retailers are the brands that consumers interact with every day and the names they remember. The value of your customer relationships is paramount, and protecting your customers' data and your own is crucial to keep customers coming back. Technology innovation is also vital. For threat actors, your existing technology is a target along with any new applications and systems that move customer data.

As you grow and innovate with technology, take the opportunity to improve your security posture. It's never too late to assess what data is at risk and how cybercriminals might access it. Continuous assessment and testing will keep you vigilant against threats and help allocate strong prevention technology where you need it most. What you cannot prevent, you can detect with the help of broad security visibility and expert security intelligence. This intelligence can also be used to predict the next attack target, creating a cycle of continuous prevention. Last but not least, make security a priority for all employees and the partners who share your data. Qualified security experts can guide you through any of these exercises for an improved and more secure retail experience for your customers.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com