Retail Information Security Challenges:
Protecting Customers While Enabling New Technology and Improving the Bottom Line
Retail Information Security Challenges:
Protecting Customers While Enabling New Technology and Improving the Bottom Line

By Peggy Bresnick Kendler

As the economy slowly recovers from the financial crisis of the past few years, retailers face the daunting challenges of re-engaging cautious buyers while simultaneously improving customer service, keeping costs in line, and differentiating themselves from their competitors. The retail segment — which covers a gamut of businesses ranging from clothing and electronics sellers, convenience stores, mall and airport kiosks to restaurants and fast food chains, gas stations, campus gift shops, grocery and furniture stores, pet shops and more — is also under pressure to empower employees to be as educated and informed as customers, who are more savvy and demanding than ever before. Customers now expect purchases and exchanges to be available through any means, anytime and anywhere.

As a result, the retail landscape is changing faster and more dramatically than ever before. Online shopping is exploding, as retailers of all types and sizes expand product offerings, add new services and embrace tools like social media and video. It is becoming harder to distinguish pure play online retailers from traditional brick-and-mortar retailers, which continue to add new features and functionality along with incentives like free shipping.

Retail Security in a Mobile World
Shoppers are increasingly relying on portable media, smart phones, and mobile point-of-sale devices to purchase goods and services, too. During the past year, the percentage of consumers who used their mobile phone to make online purchases doubled, increasing from 9 percent in 2010 to 18 percent in 2011, according to a recent report, “Opportunity Calling: The Future of Mobile Communications, Take Two,” by Oracle Communications. While m-commerce may still be in its infancy, the number of subscribers accessing retail content via mobile phones increased 95 percent in 2011, according to a September 2011 comScore report. This remarkable growth occurred even though more than 68 percent of respondents indicated doubt surrounding their mobile phone’s information security.

Although it offers new opportunities to reach and engage with consumers, the rapid growth of devices and access points — combined with increased enforcement of industry regulations — has created enormous complexity and risk in the retail environment, and has made it more critical than ever for retailers to scrutinize how and where sensitive data is sent within and outside of their stores and offices.

Identifying the Problems
In general, organizations are more aware of the dangers of attacks and are better arming themselves today than even a year ago. A March 2011 report from the Ponemon Institute, which looked at the cost of data breach incidents for U.S.-based organizations, found that companies are more proactively protecting themselves from malicious threats. In fact, average detection and escalation costs rose by 72 percent over 2009 levels, suggesting that companies of all types are investing more resources in both detection and prevention.

As in other industries, retailers have become increasingly concerned with security. They face an ever-growing threat of losses, not just through traditional means like employee theft and professional shoplifters, but also through increasing attacks against point-of-sale systems, mobile devices and

ABOUT THE AUTHOR
Peggy Bresnick Kendler has been a professional writer for the past 30 years. She has worked on a wide variety of special projects on behalf of some of the most familiar companies in the financial technology field.
computers by criminals who aim to steal customer data and customer information.

Security breaches at large companies make big news. However, cyber criminals are now targeting smaller businesses just as often. Small retailers have become easy targets because they can be unaware of security requirements and have a misperception that hackers only target larger organizations. And the smaller companies may lack the sophisticated security systems that larger enterprises have implemented. In fact, in 2010, the U.S. Secret Service and Verizon, Inc.’s forensic analysis unit responded to 761 data breaches — and nearly two thirds (63 percent) involved companies with 100 employees or fewer. This represents a huge jump from 2009 levels, when 27 percent of data breaches involved smaller companies. Interestingly, 95 percent of credit card data breaches that Visa uncovers involve its smallest business customers.

Smaller retailers must be especially mindful of containing costs and tracking inventory, and because they don’t have the big budgets and resources of a larger enterprise, they may have to rely on a single person to handle technology capabilities and IT issues. Larger companies, in turn, must deal with the complexity of hundreds or even thousands of locations, an increased number of employees and legacy internal applications and systems, and the challenge of coordinating IT and security staff around the globe.

While retailers have many different business models and challenges, they all have some things in common: important data to protect and compliance mandates to meet. Technology has become a powerful enabler of competitive differentiation for retailers. For instance, retailers that integrate their brick and mortar store systems with online and other sales channels ensure that customers can buy their products anytime, anywhere. And technology can help retailers guard against threats, protecting sensitive data and proactively fighting fraud, before it happens.

Among retailers surveyed in 2011 by RSR Research, 56 percent identified educating and empowering in-store employees using technology as a valuable opportunity for improving the in-store experience, up from 49 percent in 2010.

**Retail Security Drivers**

Several factors drive retail security challenges. First, customers have become more accustomed to and comfortable with sharing their personal information online and through customer loyalty programs. At the same time, retailers face increased pressure to make data accessible to multiple internal users and external channels, which potentially opens the data floodgates to people with authorized access — and those who have nefarious intentions.

The increased complexity is driving the need for more expertise, for professional planning and execution, ongoing attention and metrics. Retailers

LOOKING FOR HELP

Many retailers opt to work with a security vendor with the expertise and proven solutions that address the most critical security challenges facing retail organizations.

An emerging leader is Dell SecureWorks, which provides a range of information security services to help retailers protect their IT assets, comply with regulations and reduce security costs. Dell SecureWorks works with IT departments, creating a partnership and an augmentation of the IT team to optimize each institution’s security efforts, create efficiencies and facilitate regulatory compliance. Using a flexible delivery model, Dell SecureWorks security services provide protection across the network, safeguarding the perimeter as well as critical internal assets, data, remote users, customers and partners. Its services are vendor agnostic and can assimilate easily into a merchant’s existing environment.

Dell SecureWorks offers a comprehensive suite of services, including:

- Managed information security services
- Firewall and log management
- Security information and event management (SIEM and SIM On-Demand)
- Security and risk consulting
- Compliance solutions, including PCI DSS

Because of its large customer base, Dell SecureWorks has a great deal of visibility into emerging issues as well, via its world-class threat intelligence services.

For more information on Dell SecureWorks, visit www.secureworks.com or call 877-905-6661.
must create consistent policies and processes for data governance, mobile and Web security, employee education and more. Many retailers struggle with setting up metrics to measure the success and improvements to the provisions they put in place.

And finally, Payment Card Industry Data Security Standard (PCI DSS) compliance is driving retailers to focus on their security capabilities. The PCI DSS is a set of detailed guidelines designed to ensure that all companies or merchants that accept, transmit or store any cardholder data maintain a secure environment. In order to be PCI compliant, retailers must use a firewall between their wireless network and their cardholder data environment, utilize the latest security and authentication, and actively use a network intrusion detection system, among other requirements.

While retailers can avoid some penalties and fines if they are compliant when a breach takes place, PCI-related fines can be as high as $500,000 for each incident if a company is breached and credit card information is compromised. In severe cases, non-compliance can mean that merchants can be prohibited from accepting credit cards.

Requirements continue to evolve, making PCI compliance and security especially challenging for retailers. Keeping up with the changing mandates can be difficult. Smaller and mid-size retailers may not have a large compliance team, and large retailers may struggle to implement mandates across multiple locations and regions while ensuring that they are making the most of new technology for customers and employees. It can also be problematic to understand what is needed to meet new requirements, and how the changes will impact the business.

**Retail Threats: The Concern**

Data breaches cause both financial and reputational damage. Costs can include fines and penalties from payment card companies and government regulators as well as increased card processing fees and actual fraud losses resulting from the theft of payment information, for which the retailer is responsible. A significant amount of retailers’ IT budgets and resources are devoted to investigating and responding to breaches.

Fraud not only affects consumer victims monetarily but also alters customer behavior and perceptions, which can negatively affect retailers. According to a 2010 Lexis/Nexis study, more than one in three consumers who were victims of fraud avoided certain merchants; one in four reported that they spend less money with certain merchants;

---

**DELL SECUREWORKS IN USE**

Dell SecureWorks security services can significantly improve security for retailers. A recent TechValidate poll of 25 retail users of Dell SecureWorks Security Services clients found that 87 percent of these businesses rated their overall security posture as “stronger” or “better” since engaging Dell SecureWorks as a security services vendor.

Examples of successful Dell SecureWorks customer engagements in the retail sector include:

- **A large enterprise retail company** seeking to improve the quality of protection, gain additional security expertise, improve regulatory compliance and increase threat response time implemented Dell SecureWorks to comply with the PCI Data Security Standard, Sarbanes-Oxley and other regulations. The retailer reports that it has saved 60 to 79 percent compared to performing the same security functions with in-house staff and tools and that its overall security posture is much stronger.

- **A large enterprise retailer** tapped Dell SecureWorks Security Services for 24x7 security coverage, to improve quality of protection, to provide additional security expertise and to improve operational efficiency. In addition, the firm wanted to improve its response to threats. As a result, the firm reports savings of 20 to 39 percent compared with the cost of performing the same security functions with in-house staff and tools.

- **A medium enterprise retailer** solved its security and operational efficiency challenges with Dell SecureWorks Security Services, while reducing overall costs. Dell SecureWorks provides the retailer with 20 to 59 percent savings over the cost of performing the same security functions in house, while boosting overall quality of protection, providing additional security expertise and helping the firm be more responsive to threats. In addition, Dell SecureWorks helped the retailer increase operational efficiency and gave visibility to the business on the importance of perimeter security.
Retail Threats: The Reality
At any given time, all retailers deal with security attacks in some way, shape or form. These threats fall into two main categories: financial threats and advanced persistent threats (APTs). In financial threats, cybercriminals seek monetary gain through the theft of card data, PINs and more. One example of a financial threat is the ZeuS Trojan, which can be spread via malicious links in email or links on social media sites. It has already infected an estimated 4 million computers worldwide.

With APTs, cybercriminals target a person or organization over a period of time to seek strategic advantage through espionage and theft of intellectual property. Criminals make use of a wide assortment of tools and mechanisms to accomplish their goal, which may be driven by financial or sociopolitical motives.

Although most attacks against retailers target payment card data, any kind of attack can have a devastating effect on a retailer’s business. Cybercriminals no longer limit their attacks to large enterprises. They are relentless in their pursuit of retailers of all sizes and types. Smaller retailers make an appealing target because they tend to have fewer security provisions than larger firms.

While smaller retailers face a very real threat, they don’t always take the danger seriously. According to a January 2011 Zogby survey of 1,000 small retailers and small business owners sponsored by Visa Inc. and the National Cyber Security Alliance, nearly 50 percent of this group believe it’s not worth the cost and time to fully secure their businesses against fraudulent threats. And 85 percent of survey respondents said they believe they are less of a target than large companies. Furthermore, more than half (54 percent) of this group said they are better prepared to secure sensitive customer and corporate data than larger organizations. Even so, says the report, 84 percent of small retailers and small business owners responding to the survey said they have policies and procedures in place for securing their data and systems.

WHY RETAILERS MAKE APPEALING TARGETS
According to Risk Based Security’s 3rd Quarter 2011 Data Breach Intelligence report, nearly 50 percent of the reported data breaches in 2011 involved retail businesses, and those breaches accounted for nearly 25 percent of the total records exposed so far in 2011. Retail is a prime target for attacks for a number of reasons:

• Large transaction volume. With more than 20 billion transactions on an annual basis, retail transactions far surpass other industries. Electronic transactions worldwide are rising dramatically, as consumers continue to shift from cash and checks to plastic.

• Billions of payment cards in use globally. There are an estimated 1.5 billion payment cards in use just in the U.S.

• High employee turnover. U.S. retailers experience an average 30 percent annual turnover, higher than for any other industry. The revolving door can create security issues, making it more challenging to educate employees and enforce policies.

• Numerous physical and digital transaction points. Customers can now pay for goods and services in a number of ways, including mobile phone, mobile POS device, telephone, Web site and more.

• A very complex environment. Complexity is the enemy of security. Retailers are increasingly challenged with a growing architecture of applications, devices and locations. There are more potential entry points, elevating the risk of criminals finding a way to compromise data.
What Can Retailers Do?

Retailers are striving to make the most of resources and do more with fewer people and less equipment, and technology provides a way to reduce costs, drive sales, improve customer satisfaction and improve security. But cost-consciousness demands that retailers invest in solutions that employees and customers will actually use.

Small and medium businesses, in particular, often lack time and personnel to proactively focus on security. Management may be more concerned about compliance than with a longer-term strategy. Smaller organizations may also find that they lack employees with the needed skill sets to deal with maintaining adequate security.

Retailers across all industry segments must take steps to protect themselves — and their customers — from attacks. Retailers can take the following measures:

• **Implement a robust intrusion prevention solution (IPS):** To defend networks against SQL injection attacks, Web exploit kits and downloader Trojans, retailers should implement an intrusion prevention solution (IPS) with countermeasures that can detect and block current and emerging cyber attacks.

• **Implement a Web application firewall:** To help prevent Web applications from infiltration, retailers should employ a security expert to continuously maintain and monitor firewalls.

• **Monitor servers and security devices 24x7x365:** Retailers should monitor servers and security devices, such as firewalls, IDS/IPS, and host antivirus, at all times to identify and remediate security issues in real time.

• **Apply timely and actionable intelligence:** Retailers should always have current, actionable intelligence about the latest threats and the IP addresses associated with them so their security team can spot any infection inside their network attempting to communicate valuable data to hackers.

• **Perform regular vulnerability scans and penetration tests:** Vulnerability scans and network penetration tests can help retailers identify issues and improve their security posture, especially when defending against Web application attacks.

• **Implement Web content filtering:** To protect against Web-exploit kit and downloader Trojan attacks, retailers need to implement Web content filtering, as well as network and host-based antivirus solutions.

Protecting the Retail Industry from Threats

Today’s network attacks and information theft aren’t perpetrated by individuals for their own amusement. Cyberattacks are now typically carried out by sophisticated criminal organizations that are highly skilled and stealthy. The full range of threats continues to expand, become more diverse, and create increasing financial and reputational damage. But threats don’t always come from external sources; often, data leaks can originate from employees, through intentional theft, lost or stolen mobile devices, or accidental exposure.

Retailers can no longer consider information security an option. Those firms that do not adequately address security issues may face fines, serious damage to their brand and steep financial losses. Retailers that do not invest in their security provisions may find that the short-term savings are not worth the potential for huge losses should a breach occur.

Cyber-security typically isn’t a core competency for retailers. Savvy retailers frequently find that by partnering with an experienced service provider that offers optimized network security solutions, ongoing threat intelligence and comprehensive endpoint security they can protect themselves against current, emerging and persistent threats.

Retailers need to be constantly vigilant and aware of threats, and how they might impact their business — and have a superior way to address them. The threats are real, and the business impact can be monumental.