Six Steps Toward Tighter PCI and Data Security

Pity those responsible for data security and loss prevention. When they do their jobs perfectly, nothing occurs – or rather, products are sold, transactions are processed, data is exchanged, etc., without problem or incident. The loss prevention executive’s best day is when no one notices what he or she does. They are noticed when things go wrong – for example, when thieves steal customers’ credit card data from the POS PIN pads in stores, as just occurred recently in 63 Barnes & Noble locations. Or when sensitive corporate or personal information is exposed because an employee hasn’t password-protected her BYOD smartphone. This Roadmap provides six steps designed to keep loss prevention executives out of the spotlight’s uncomfortable glare, including new PCI guidelines for handling the complexities of mobile payments, advances in video analytics and the data security advantages of EMV/chip-equipped payment cards.

SPONSORED BY

CyberSource®
Pity those responsible for data security and loss prevention. When they do their jobs perfectly, nothing occurs. Or rather, products are sold, transactions are processed, data is exchanged, etc., without problem or incident. The loss prevention executive’s best day is when no one notices what he or she does.

These executives, and the systems they’re responsible for, do get noticed when things go awry – for example, when thieves steal customers’ credit card data from the POS PIN pads in stores, as just occurred recently in 63 Barnes & Noble locations. Or when sensitive corporate or personal information is exposed because an employee hasn’t password-protected the smartphone she uses as part of a Bring Your Own Device (BYOD) deployment. Or when it’s discovered that a store’s WiFi network, now essential for supporting the flood of consumer and retailer-deployed mobile devices, opens up a whole new galaxy of potential data leaks that have to be plugged.

Loss prevention teams use a range of technologies to protect the security of customer and company data, along with those used to ensure physical security and to combat other types of theft such as shoplifting. Many of these tools are still more focused on past reporting than real-time alerts and actions, although this is changing as retailing moves more quickly and involves more technology.

According to a March 2012 Aberdeen Group survey, 37% of responding retailers have real-time theft analysis, and another 33% are planning to add this capability: 31% use real-time loss prevention monitoring and alerts to store locations, with 22% planning to add these in the future. (See chart, page 5.)

In the interests of helping retail security executives stay out of the spotlight’s uncomfortable glare, following are six mileposts on the road to tighter, more comprehensive data security in retail.

**Milepost 1**

**Map Responsibilities for Mobile Payment Security**

The growing trend of enabling consumers to pay using mobile devices piles new security challenges on top of those that already surround traditional fixed POS systems. “Any risk that exists on a standard desktop or laptop computer may also exist on a mobile device,” according to the PCI Security Standards Council’s recently released “PCI Mobile Payment Acceptance Security Guidelines for Developers.”

The September 2012 guidelines note that many of the features that make smartphones and tablets attractive to consumers and retailers also introduce complications and security risks: GPS, Bluetooth, infrared and NFC (Near Field Communications); removable media such as SIM (subscriber identity module) and SD (secure digital) cards; and internal electronics used for manufacturer testing, embedded sensors (e.g. tilt or motion sensors, thermal sensors, pressure sensors, and light sensors) and biometric readers.
It’s not just that mobile devices are complex and contain numerous high-tech features. Because they operate at the intersection of multiple enterprises and networks, and because the relationships among these entities is still evolving, responsibility for data security and fraud protection is more diffused than it is in traditional payment structures.

“Security risks are also inherent to the developmental life cycle and infrastructure associated with mobile devices,” the guidelines note. “The original equipment manufacturer, the operating-system software developer, the application developer, the integrator, the reseller, the mobile-network operator (or cellular service provider), and the mobile payment-acceptance solution provider each play a part in the overall security of a mobile device.” All these entities and others “represent potential vectors for unauthorized access to device operations or unauthorized disclosure of account data.”

The PCI guidelines include a “Best Practices and Responsibilities” table that identifies best practices and assigns responsibility among manufacturers, developers, merchants and payment solution providers. The complete Mobile Payment guidelines document is available at www.pcisecuritystandards.org.

**Milepost 2**

**Tighten Mobile Payment Security Measures**

The PCI guidelines also list a number of security measures that can be taken to protect the integrity of the mobile platform and application environment, including:

- **Prevent unauthorized logical device access:** Include design features such as one of the more secure lock screens: “Face Unlock,” “Password,” “Pattern” or “PIN.” Don’t rely on “Slide,” since it does not add security. Include a feature that forces user re-authentication to the device after a specified amount of time.

**Six Steps to Improved Data Security**

<table>
<thead>
<tr>
<th>Milepost</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Map Responsibilities for Mobile Payment Security</td>
</tr>
<tr>
<td>2</td>
<td>Tighten Mobile Payment Security Measures</td>
</tr>
<tr>
<td>3</td>
<td>Integrate Video-Based Loss Prevention Tools into Data Security</td>
</tr>
<tr>
<td>4</td>
<td>Improve Security of In-Store Wireless Networks</td>
</tr>
<tr>
<td>5</td>
<td>Make the Transition to EMV/Smart Chip Payments</td>
</tr>
<tr>
<td>6</td>
<td>Protect Customer Data Online</td>
</tr>
</tbody>
</table>
Q: With the amount of change occurring in the retail payments area, what do you see as the biggest data security challenges retailers are facing today?

DAVE GLASER: Innovations in the retail space are trending toward consumer-centricity, putting payment solutions into the hands of the consumer, as well as channel convergence, allowing that same consumer the choice of how, when and where to pay. In that context, the biggest data security challenges retailers face is the loss of their ability to fence payment data within an environment that they can control. This is particularly true as payment data moves onto consumer-owned mobile devices. The big new data security challenge with this trend is ensuring that the consumer maintains a level of security in their own device, but as we all know, consumers are notoriously lax in that department. Fortunately, there are payment solutions that rely on dynamic data, such as Near Field Communications (NFC), which greatly reduce the need for consumers to understand and act on data security on their own.

Q: As retailers become increasingly omni-channel in both their approach to customers and their operations, what are some key best practices for maintaining high levels of data security?

GLASER: There are several. One is removal of static data from the retail environment, by outsourcing to cloud providers. Another is adoption of dynamic authentication solutions, and a third is implementation of secure technologies such as tokenization or point-to-point encryption.

Q: Some retailers are considering making their e-commerce platform their primary transaction engine for all touchpoints, particularly SMBs and those that began as pure-play operators. If retailers use their e-commerce platform in this way rather than a traditional POS, does that create new or different data security issues?

GLASER: Leveraging an e-commerce platform in a customer present environment, such as a brick-and-mortar store, requires wrapping card present security best practices around the e-commerce platform – as well as ensuring security features around the sensitive customer and payment data within this new customer present experience. However, it’s better if merchants don’t think about this as a single experience, but instead enable a central customer repository that provides both for singular customer recognition across all retailer interactions and for removal of sensitive data to address security and compliance requirements.

“AN EMERGING CHALLENGE INVOLVES UNDERSTANDING AND SECURELY ENABLING THE ENTIRE CUSTOMER EXPERIENCE BEYOND E-COMMERCE AND POS, INCLUDING, FOR EXAMPLE, THE CALL CENTER. IN ENABLING THIS OMNI-CHANNEL EXPERIENCE, THE RETAILER MUST FULLY APPRECIATE THE CONSUMER’S BRAND ASSOCIATION WITH THAT EXPERIENCE, AND THE RESULTING SECURITY ISSUES THAT PRESENT GREATER BRAND RISK.”

– Dave Glaser, Vice President, Global Services, CyberSource

Q: Are there some common pitfalls or things that retailers often overlook in the payments/data security area, and if so, what are some basic things they can do to remedy these issues?

GLASER: An emerging challenge involves understanding and securely enabling the entire customer experience beyond e-commerce and POS, including, for example, the call center. In enabling this omni-channel experience, the retailer must fully appreciate the consumer’s brand association with that experience, and the resulting security issues that present greater brand risk. Retailers should leverage their payment industry partners in helping solve for these challenges, which represents a significant opportunity for both the retailer and their payment industry partners.
• **Create server-side controls and report unauthorized access:** The payment acceptance solution should include capabilities for preventing and reporting unauthorized access attempts; identifying and reporting abnormal activity; and discontinuing access until an administrator restores access. Controls include support for authorized access, e.g. an access control list; the ability to monitor events and distinguish normal from abnormal events; and the ability to report events such as cryptographic key changes, escalation of privileges, invalid login attempts exceeding a set threshold, updates to application software or firmware and similar actions.

• **Prevent escalation of privileges:** Controls in this area include providing the capability for the device to produce an alarm or warning if there is an attempt to “jailbreak” the device. Jailbroken mobile devices allow access to their proprietary operating system, which then allows the installation of third-party applications not released or controlled by the manufacturer or proprietor.

• **Create the ability to remotely disable the payment application and to detect theft or loss:** Remote disabling should not interfere with the non-payment functions of the mobile device; theft detection processes should include means for testing and confirming that the device remains active. Examples include GPS or other location technology with the ability to set geographic boundaries, periodic re-authentication of the user, and periodic re-authentication of the device.

• **Make supporting systems PCI DSS compliant:** Any system used to support the mobile payment-acceptance solution should be compliant with the PCI Data Security Standards.

---

**Figure 1**

Organizational Capabilities Supporting Loss Prevention

<table>
<thead>
<tr>
<th>Capability</th>
<th>Current</th>
<th>Planned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Historical theft analysis</td>
<td>18%</td>
<td>60%</td>
</tr>
<tr>
<td>Weekly reporting/auditing on channel transaction management functions</td>
<td>23%</td>
<td>50%</td>
</tr>
<tr>
<td>Real-time theft analysis</td>
<td>33%</td>
<td>37%</td>
</tr>
<tr>
<td>Real-time access to returns management solutions</td>
<td>25%</td>
<td>36%</td>
</tr>
<tr>
<td>Real-time loss prevention monitoring and alerts to store locations</td>
<td>22%</td>
<td>31%</td>
</tr>
<tr>
<td>Tracking customer count with camera surveillance and electronic article surveillance</td>
<td>20%</td>
<td>27%</td>
</tr>
</tbody>
</table>

Retailers are moving toward more real-time and video-based loss prevention technologies.

*Source: Aberdeen Group, March 2012*
• **Prefer online transactions:** When the mobile payment-acceptance application on the host is not accessible, the mobile device should neither authorize transactions offline nor store transactions for later transmission.

---

**Milepost 3**

**Integrate Video-Based Loss Prevention Tools into Data Security**

Video surveillance has a long history in retail loss prevention, but traditionally it has only tangentially been involved in data and payment security. Typical uses included monitoring cashiers to help detect instances of “sweethearting,” or tracking customer behavior to guard against shoplifting in dressing rooms or false “slip and fall” accident claims.

While these remain primary uses for video technology, the analytics associated with these systems have become powerful tools for understanding customer and associate behavior. Today’s video analytics solutions can identify common markers of fraudulent activity, and should be integrated into a retailer’s holistic approach to data security. Several solutions offer exception-based reporting integrated with POS records, allowing retailers to zero in on instances of fraud taking place without having to view hours and hours of video feed.

According to a March 2012 Aberdeen Group survey, 28% of retailers have adopted video intelligence to reduce the number of internal and external theft incidents.

---

**Milepost 4**

**Improve Security of In-Store Wireless Networks**

In-store WiFi networks are increasingly necessary to support mobile device deployments, but they also present an easy target for data compromise, according to the PCI Security Standards Council (SSC). The PCI SSC’s wireless guidelines recommend quarterly reviews of all wireless networks in addition to annual PCI assessments. These reviews should combine the use of wireless “sniffers” capable of detecting rogue devices when a technician or auditor walks around a site with physical and logical inspections, because “physical intervention remains the ultimate response to remove the rogue device.”

Following are six physical security recommendations for wireless access points from the August 2011 PCI DSS Wireless Guidelines:

- Mount access points (APs) on (or in) ceilings and walls that do not allow easy physical access, or locate in secure areas, such as locked closets or server rooms.
- Use APs with tamper-proof chassis and mounting options that prevent physical access to ports and reset features.
- Review signal settings and physical placement of APs to provide maximum coverage for the desired service area while minimizing broadcast range outside of the environment.
- Secure handheld devices with strong passwords and always encrypt pre-shared keys if cached locally.
- Enable automatic lockouts on handheld devices after a defined idle period, and configure devices to require a password when powering on.
- Use a wireless monitoring system that can track and locate all wireless devices and report if one or more devices are missing.
Milepost 5

Make the Transition to EMV/Smart Chip Payments

Despite the buzz about new mobile payment technologies, card-based payments are still the predominant transaction medium for retailers. The good news in this area is that new cards adhering to EMV (Europay/MasterCard/Visa) standards and equipped with “smart chips” address one of the most common causes of data breaches: the static nature of data contained on the magnetic strips in current cards. As an example, the recent Barnes & Noble data breach was apparently achieved by collecting customer card data via a single PIN pad at each of 63 stores.

The problem with static data is that as long as the card account is active, anyone who has that card’s information can use it, whether it’s the rightful owner or a thief. In addition, when today’s sophisticated cyberthieves gain access to just some of the data elements required to complete a transaction, they can often piece together the rest of the data they need, or use it as a lever to discover other valuable information about the cardholder. This adds the risk of identity theft to any financial losses incurred by the cardholder or the retailer.

In contrast, the smart chips generate a unique cryptogram for each transaction they perform. Online card authentication typically takes place using symmetric key technology, with the card generating a cryptogram using a shared secret key that is validated during the online authorization request. In person, as at a store’s POS, the chip-equipped cards and terminals use public key technology. Identity and security are further strengthened with Chip & PIN and Chip & Signature transactions.

The downside for retailers is the cost of upgrading their POS technology to handle these transactions, but improved data security should be included in the ROI calculations for these investments.

Milepost 6

Protect Customer Data Online

Data security extends well beyond the four walls of a store. With omni-channel retailing becoming the norm, an omni-channel approach to data security is required. Unfortunately, the siloed nature of many retail enterprises and the security challenges that are specific to e-commerce can make this type of holistic approach difficult.

There are strong signs, however, that retailers need to make a greater effort to tighten the security of online transactions and interactions. As an industry, retail was ranked the worst in website vulnerability in 2011, according to the annual Website Security Statistics Report from WhiteHat Security released earlier this year. Retailers’ annual average number of “serious vulnerabilities” was 121; in contrast, the IT industry’s average was 85, and financial services had 67.

Cyberthieves’ frequent target is customer data, including credit card numbers, Personally Identifiable Information (PII) and e-mail addresses. These were the targets in 89% of investigated data breaches in 2011, according to the Trustwave 2012 Global Security Report. Retail accounted for one-third of all investigated data breaches, second only to food and beverage, at 43.6%.

E-commerce targets rose from 9% to 20% over the previous year, according to the Trustwave report, largely due to additional engagements in the Asia-Pacific region, where e-commerce compromises are more common than software POS system compromises.
Conclusion

It’s often said security is a journey, not a destination. That’s particularly true in retail organizations, which by their nature allow many thousands of people (both employees and customers) to access a wide range of information technology solutions and devices. For good measure, the industry consists of geographically disparate locations, some of which operate across international boundaries, as well as the increasingly complex digital worlds of online, mobile and social networks. And unlike, for example, a financial institution, retailers must maintain a higher degree of openness and accessibility in order to do business.

However, retailers cannot ignore data security, particularly as data itself becomes ever more valuable. Retailers themselves are digging deeper into expanded sources of data, from social network postings to location-based information. Along with this recognition of data’s value, retailers need a holistic yet flexible approach to data security that encompasses all channels and all interactions with their customers, throughout the entire purchase cycle. •
CyberSource*

About CyberSource

We’re more than a global payment gateway—we’re a payment management company. CyberSource provides a complete portfolio of services that simplify and automate payment operations. Customers use our CyberSource and Authorize.Net brand solutions to process online payments, streamline fraud management, and simplify payment security. Born during the dawn of eCommerce in 1994, CyberSource was one of the pioneers in online payment and fraud management services for medium and large-sized merchants. In 2007, we acquired the leading U.S. small business payment services provider, Authorize.Net, thus expanding our market footprint to cover businesses ranging from the smallest sole proprietorships to the largest global brands. In 2010 CyberSource was acquired by, and operates as a wholly-owned subsidiary of, Visa Inc. Today, over 370,000 businesses worldwide use CyberSource solutions. The company is headquartered in Foster City, California, with international offices in the U.K., Brazil, Mexico, China, Singapore and Japan. For more information visit www.cybersource.com.