

Apparel

August 2006

Why Apparel Retailers Must Secure PCI Data

By Brian Contos, ArcSight Inc.

If you're selling apparel to consumers and accepting payment via credit cards, the acronym "PCI" needs to be a key part of your business and IT infrastructure focus.

This is particularly critical for apparel brands that may be relatively new to the retail realm as they open their own stores and sell directly to the consumer online. Online fraud is higher than that associated with brick-and-mortar retailing.

What is PCI?

It stands for the payment card industry. More specifically, the Payment Card Industry Data Security Standard (PCI DSS) 1.0 is a compliance standard adopted by the major credit card companies (American Express®, Diners Club®, Discover® Card, JCB®, MasterCard International® and Visa® U.S.A.).

It is a merger of the Visa USA Cardholder Information Security Program (CISP) and the MasterCard Site Data Protection (SDP) program.

The PCI standard applies to all merchants and service providers that store, process or transmit cardholder data.

Card associations have implemented the PCI standards to help manage risk related to fraud and other card-related crimes. Retailers must pass audits to verify their compliance with the PCI standard. Those that do not comply can be subject to penalties such as fines or be excluded from processing credit cards.

Consider the case of DSW. Credit card information stolen from 108 of its stores contained the data from 1.4 million credit card or debit card numbers. In addition, information related to 96,000 checks was stolen, including checking account numbers and driver's license numbers. Within 24 hours DSW notified federal law enforcement, retained a security firm to conduct a forensic investigation and notified cardholder associations. They also issued a press release and customer alert and shared information with the card associations to better assist the investigation and sent notification letters to customers. Clearly, DSW took information theft seriously and spent real time and money to respond to the incidents.

Polo Ralph Lauren faced similar issues when its customers' credit card information was breached.

Any brand or retailer facing PCI compliance issues is at risk for public relations costs, decreases in shareholder faith, regulatory fines, legal fees, tarnished brand image and lost revenue — all of which has prompted these companies to start taking PCI security extremely seriously.

Issues that interfere with compliance

Over the years, the term *compliance* has been linked with vague, loosely interpreted standards. The PCI standard sets itself apart from many by explicitly stating 12 requirements that must be achieved to comply, including incident prevention, detection and management. The PCI standard will be updated later this year. There will be several

adjustments, including an additional level of focus on application security and various alternatives to some of its existing safeguards.

Still, while the PCI standard clearly spells out compliance requirements, many retailers find themselves challenged to secure their organizations.

Visa has reported that 22 percent of Tier 1 merchants (organizations processing more than 6 million transactions per month) are PCI compliant, and 72 percent are on their way to becoming fully compliant.

What are some of the issues and concerns that are preventing apparel retailers from being compliant?

Legacy and proprietary software applications. Many organizations still require legacy and/or proprietary applications to be operational for their business to function. This is especially common for retailers. Many of these applications were designed for much older retail environments and don't offer important functionality such as:

- encryption capabilities for protecting cardholder data;
- support for strong authentication for implementing strong access controls;
- alternatives to embedded passwords to build and maintain secure networks;
- logging capabilities for regularly monitoring and testing networks.

Multiple regulations. The PCI standard is not the only one that retailers must watch. There are others, and complying with all of them can be daunting. At the same time, if your company has a strong compliance program in place related to other standards, this investment of time and resources can help with your PCI compliance effort. For example, your PCI push will be easier if you already have a strong IT governance program built on ISO 17799 security standards and NIST 800-53 (National Institute of Standards and Technology's Recommended Security Controls for Federal Information Systems). If your organization is resource-constrained and has not tackled these other standards, PCI compliance could be more difficult to implement.

The costs. Some retailers struggle with the costs of PCI compliance. There are costs associated with

- procuring security hardware and software;
- hiring consultants and auditors;
- training staff; and
- testing and verifying the solution.

Lingering risks. Many retailers are daunted by the PCI issue because they realize that even if they put all of the required PCI countermeasures in place, they still face an unsettling degree of risk from external attackers, malicious insiders and the like.

That fact is that preventive measures only scale so far. This is why

incident detection is an imperative. Simply putting preventive controls such as firewalls and encryption solutions in place will not create a strong security posture — people will eventually find ways around them.

As General George Patton Jr. once said: “Fixed fortifications are monuments to the stupidity of man.” This is why section 10 of the PCI standard (track and monitor all access to network resources and cardholder data) is so critical, especially for apparel organizations with large, distributed networks.

How to monitor your PCI environments

Data collection. One of the most important preventive safeguards is to secure your data collection. To do this, you must implement safeguards that feed critical data into a PCI monitoring solution. For starters, the following types of systems within your company must generate logs that feed into a real-time monitoring solution for PCI risk analysis: operating systems, mainframes, anti-virus programs, firewalls, network/host intrusion prevention tools, routers, databases, authentication solutions and applications and vulnerability and asset management solutions.

At the point of data collection, the logs should be filtered, normalized, aggregated, compressed and encrypted per NIST 800-92 (Guide to Computer Log Management) guidelines. Information from mission-critical systems should take precedence in the monitoring strategy.

Analysis. Following log collection, the logs should be processed through an automated analysis mechanism. The most effective and efficient method for detecting PCI-specific events within these logs is to map them against analysis capabilities such as correlation, pattern discovery, anomaly detection, user tracking, visualization and reporting. Here are some examples of types of capabilities and user activity to watch:

- User account activity such as unauthorized access, privilege escalation, terminated account usage, password changes, account creation and failed access;
- User access to sensitive information that he or she may read, modify, print and copy;
- Default and insecure services detection;
- Encryption and anti-virus verification;

- Patch, vulnerability and change control tracking;
- Physical access controls such as badge readers and biometric devices; and
- Network settings such as firewall rules, ports, VPNs, ACLs and IDS signatures.

Analyzing this information automatically will help to reduce false positives and data overload and help you prioritize the most critical events, and yield actionable output that is specific to PCI.

Management. Finally, based on organizational policies and procedures and the output from log analysis, a PCI program should include incident management capabilities such as:

- Tracking and auditing (for monitoring time to resolution, open cases and operational impact);
- Alerting and escalating;
- Collaborating; and
- Responding to stop the attack automatically; stopping the attack with human intervention; quarantine suspicious activity; and disable accounts.

This type of incident management helps analysts more efficiently review information with their peers and escalate and assign cases as necessary. It also helps to ensure adherence to change management procedures and authorization channels. Having end-to-end workflow allows an organization to track how well it is responding to incidents over time. It also allows managers to track resolution status, assign resources and make better budgetary decisions.

Summary: Parting PCI points

Key priorities for apparel retailers to implement a successful PCI program are: incident prevention, detection and management. Mapping the PCI-specific requirements against an automated monitoring solution will help mitigate risk, increase operational efficiencies, and improve an organization’s overall security posture. While PCI is more than just about technology, having a strong, automated monitoring solution at the center of a PCI program will go a long way toward addressing compliance.

(#12094) Excerpted and adapted from the August 2006 online issue of Apparel. © Edgell Communications, Inc.
For more information about reprints from Apparel, contact PARS International Corp. at 212-221-9595.



ArcSight, a leader in Enterprise Security Management, provides solutions that serve as the mission control center for real-time threat management, compliance reporting and automated network response. By comprehensively collecting, analyzing and managing security data, ArcSight solutions centrally manage and mitigate information risk for security, insider threat and compliance. ArcSight’s customer base includes leading global enterprises, government agencies and MSSPs.