

Specialty retailer builds goodwill by investing in PCI compliance

Reader ROI

- To combat credit card fraud and consumer information loss, retailers must protect themselves throughout the entire credit card payment lifecycle, from initial point-of-sale capture, to aggregation, billing, reporting, archiving, and disposition.
- Payment Card Industry Data Security Standard (PCI DSS) provides a framework for retailers to invest in protection and reduce business risk.
- One successful specialty retailer has taken a holistic, multi-year approach to PCI compliance by enlisting the help of their strategic business and IT partners, including EMC and RSA, The Security Division of EMC.

Challenge

The estimates are enough to stop you in your tracks. According to Forrester, a single stolen credit card number can mean \$90–\$305 in remediation costs to a victimized retailer. Fines, customer letters, replacement cards, forensics, litigation, and damage to a company's brand trademarks and goodwill contribute to this potentially high cost.

The credit card vendors have taken action. American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. founded the PCI Security Standards Council and defined Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS is a multi-faceted security standard that includes requirements for security management, policies, and procedures. Any retailer who accepts credit card payments must demonstrate movement toward compliance.

Failure to comply with PCI has harsh consequences. Not only are there monthly fines, but retailers may be prohibited from accepting credit and debit cards, severely impacting their sales.

One large, level 1 specialty retailer embraced the need for PCI compliance—starting at the highest level of the company. Not willing to bear the cost and customer loyalty losses caused by a very public security breach, this retailer's Board of Directors asked for a company-wide proposal. How could the company strike a middle ground between excessive implementation costs and the risk of non-compliance? The company engaged their IT outsourcer who in turn engaged EMC® information infrastructure technology specialists and the security experts at RSA®, The Security Division of EMC.

Solution

EMC and the IT outsourcer proposed a phased approach, inclusive of existing infrastructure components and security processes. The proposal was accepted because it met the retailer's requirement for a balanced approach. The multi-vendor, multi-year deployment would provide movement toward compliance across all 1,100 stores, 10 distribution centers, and 150,000 employees throughout the Americas, Canada, and Asia Pacific.

The solution leveraged prior investments and respected the retailer's need to reserve significant budget for more business-growth-directed activities. It was designed around the six foundational directives and 12 prescriptive requirements of PCI DSS.

Because the EMC and RSA teams were able to build upon experience in developing PCI compliance solutions at other retailers, including Giant Eagle and Cyberklix, they were able to apply tested methodologies, products, and services to several requirements. After an extensive evaluation, the integrator and retailer chose to install the following key elements into its security infrastructure:

- **EMC Centera®:** This content-addressable storage (CAS) platform was chosen to safely store each primary account number (PAN), expiration date, service code, and/or cardholder name. (Sensitive data on a credit card's magnetic strip or chip must never be stored.) For additional protection, the retailer replicates all the information stored on one Centera system to another Centera system located in a data center several hundred miles away. (PCI requirement 3)
- **RSA Key Manager (RKM):** With centralized, automated policy management, RKM enables the retailer to automatically rotate encryption keys for each application running on servers in more than 1,000 stores and data centers. (PCI requirement 4)

PCI DSS Requirements

- **Build and maintain a secure network**
 1. Install and maintain a firewall configuration to protect cardholder data
 2. Do not use vendor-supplied defaults for system passwords or other security parameters
- **Protect cardholder data**
 3. Protect stored cardholder data
 4. Encrypt transmission of cardholder data across open, public networks
- **Maintain a vulnerability management program**
 5. Use and regularly update anti-virus software
 6. Develop and maintain secure systems and applications
- **Implement strong access control measures**
 7. Restrict access to cardholder data by business need-to-know
 8. Assign a unique ID to each person with computer access
 9. Restrict physical access to cardholder data
- **Regularly monitor and test networks**
 10. Track and monitor all access to network resources and cardholder data
 11. Regularly test security systems and processes
- **Maintain an information security policy**
 12. Maintain a policy that addresses information security

- **RSA SecurID®:** The retailer uses the RSA SecurID two-factor authentication solution to restrict employee access to sensitive company information (PCI requirement 7). Employees use passwords that change every 60 seconds and are displayed on mobile tokens along with their regular login information to access systems authorized for their use (PCI requirement 8).

Specialists from EMC and RSA continue to work closely with the retailer and the IT outsourcer. Additional components under consideration include EMC IT Compliance Analyzer, EMC Voyence® Control, and Residency Services for Physical Security. They provide strategic business and IT implementation advice as well as support the IT outsourcer's regular progress reporting to the Board.

Next on their docket: Understand the differences between PCI v1.1 (published in September of 2006) and PCI v1.2 (October 2008) and recommend how to cost-effectively bring the retailer back into compliance before the next audit.

Results

EMC and RSA have enabled the Board's goal—demonstrate PCI compliance, at a reasonable cost and stay out of the news. The most important result: This has built consumer goodwill. Because there haven't been any security breaches, consumers are more likely to think there won't be. They believe that their credit card data will be protected, so they're more likely to have favorable thoughts. As a result, they continue and/or start to shop with this retailer. Other benefits include:

- **Risk & Cost Avoidance:** In September 2008, the retailer successfully passed its most comprehensive PCI audit to date, avoiding thousands of dollars in monthly fines and reducing the risk and high costs of security breaches. A breach of just six million card numbers and clean-up cost estimates ranging from \$90 to \$305 per card yields \$5.4M to \$18.3M in avoided expense.
- **Compliance Audit Efficiency:** It is easier and faster to prove compliance to auditors with a centralized, automated system compared to manually demonstrating encryption across several thousand point-of-sale (POS) terminals and hundreds of applications and servers. With RKM, the retailer can show how keys are being automatically changed according to different timing policies and across multiple environments, such as tape operations, live networks, store-based servers, and POS terminals.
- **Operational Cost Savings:** It's estimated that fulltime equivalents (FTEs) consisting of 20 IT and 27.5 store managers would be needed to manually manage encryption keys across the 1,100 store enterprise without RKM. With FTE annual cost estimated at \$72K for both IT and store operations roles, this represents a yearly cost savings of \$3.42M. Human errors and in-store training expenses were also eliminated thanks to the EMC and RSA solution.
- **More Secure In-home Service Delivery:** Technicians who provide customers with at-home support, now log into the retailer's internal systems using their mobile RSA SecurID tokens and the customer's PC. Not only does this validate credentials of the support employees, but it also ensures there is no trace of the remote worker's password on the customer's PC after logging out. Customers are happier due to timely in-home service and the retailer protects company information from any potential compromise.

The engagement with EMC and RSA provided the targeted guidance needed by both this specialty retailer and their IT outsourcer to comply with PCI and ensure continued consumer confidence in their brand and store experience. The solution paid for itself in 12 months with just the operational savings alone.

EMC²

where information lives®

EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com