



# Commentary

April 2008

## Beyond Minimum Compliance: PCI Risk Management

By Gideon T. Rasmussen, CISSP, CISA, CISM, CIPP  
Global Information Protection Business Continuity

The PCI Data Security Standard is nearly two years old. Organized crime has shifted focus to new attack vectors and theft of card data has become big business. To adapt, business management must adopt a comprehensive risk and compliance-based approach to safeguard card data.

### Trends and Emerging Threats

According to Visa compliance statistics, 99% of Level 1 and Level 2 merchants have confirmed they do not store prohibited data. [Visa compromise statistics](#) document an even split between physical and web stores in 2007. The next logical targets are Internet-connected merchants, applications and data in transmission.

### Consequences of Compromise

The costs associated with a card data compromise are well known from the TJX<sup>®</sup> incident (nearly \$65 million). There are many additional business impacts, including:

- Costs associated with legal actions:
  - Legal battles with issuing banks
  - Lawsuits from states and the FTC
  - Class-action lawsuits from consumers
- Brand impact resulting in loss of consumer and stockholder confidence
- Impact to customer relationships, possibly resulting in a loss of business
- Increased oversight internally and from external entities
- Costs of a public relations campaign

### Top 10 PCI Best Practices

- 1. Determine where card data resides.** Create data flow diagrams to document where card data is stored, processed and transmitted. Identify associated networks, systems, applications and databases as PCI systems within system inventories. IT personnel should be aware of all systems within the PCI cardholder environment.
- 2. Become PCI compliant.** Review the [PCI Data Security Standard \(DSS\)](#) with operations personnel and ensure the appropriate controls are in place. Ensure sensitive authentication data (track data, CVV2 and PIN block) is not stored after authorization. Note that requirement 6.6 becomes mandatory effective June 30, 2008 (install an application layer firewall or have custom code reviewed by a security firm). Conduct quarterly external vulnerability scans using an [Approved Scanning Vendor](#). If card data is shared with service providers, ensure they are PCI-compliant. Merchants are responsible for the actions of a service provider if a compromise occurs. A new version of the DSS will be released in October 2008.

- 3. Use secure payment applications and devices.** All merchants must begin using technology that adheres to the Payment Application Data Security Standard (PA-DSS). Refer to their Payment Application Security Mandates for specific timelines. The mandates document and a list of validated applications are available at [www.visa.com/pabp](http://www.visa.com/pabp). Ensure your PIN entry devices are on the PCI Security Standards Council's [approved list](#).
- 4. Reduce the scope of card data environments.** Reduce usage of card data to save on the costs of PCI safeguards and assessment activity. This quote from the DSS provides rationale: "PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply." Truncation can be used to reduce scope. Store only the last four digits of each card number.
- 5. Validate PCI compliance.** Ensure all card data environments are evaluated by a qualified assessor. Per Visa, on-site assessments can only be conducted by an internal auditor or a [Qualified Security Assessor](#). Internal auditors should not have operational responsibilities associated with the card data environment. Auditors should be experienced in conducting IT security audits and be familiar with the PCI DSS. PCI on-site assessments must be conducted in accordance with the [PCI Security Audit Procedures](#).
- 6. Listen to the assessor.** Do not attempt to unduly influence an assessor's findings. If security vulnerabilities remain in place, a compromise and associated liability impact to your business may soon follow.
- 7. Remediate quickly.** A card data environment is vulnerable when a security finding is identified. Raise awareness to the appropriate management level to help ensure out-of-budget funding does not become a constraint. Conduct aggressive remediation to prevent compromise.
- 8. Keep card data secure throughout the year.** Assessments are a snapshot in time. Do not breathe a sign of relief and neglect PCI security until the next annual assessment cycle. Establish a security culture throughout the organization. Build security into new initiatives from the start. Mergers and acquisitions can take an organization out of compliance. Ensure mergers and acquisition targets are as compliant as well.
- 9. Advice for security teams.** Be passionate about security. Apply compliance and risk-based approaches. Make a compelling case for new security initiatives.
- 10. Advice for business management.** Carefully consider the security team's recommendations. Meet them halfway if the message is not quite tailored for you as an audience. Ensure the security program is adequately staffed and funded.

## Exceeding PCI DSS Requirements

The security safeguards listed below exceed current PCI requirements and help address emerging threats. One or more of them may be incorporated into a future revision to the DSS.

- Database Activity Monitoring (DAM).** Use DAM to monitor database queries for malicious activity. After establishing a baseline, configure DAM to deny requests for more than a certain number of card numbers. DAM also has audit trail functionality and can record a history of queries.
- Data Loss Prevention (DLP).** Use DLP to prevent leakage of card numbers over unauthorized networks and systems. Configure thresholds and notification alerts appropriately.
- Network Admission Control (NAC).** NAC authenticates systems before granting access to a network. Authorized systems with security vulnerabilities can be redirected to a quarantine network for remediation (for example, installation of patches, anti-virus definitions and so forth).

**Tokens.** Use a token-based solution to replace primary account numbers (PANs) as unique identifiers. Tokens reduce the risk and cost associated with processing card transactions. PCI compliance requirements are tied to PANs.

**Internal network segmentation.** PCI does not include a requirement to isolate card data internally. However, it is considered a best practice to use firewalls to segment card data from other internal networks to reduce the scope of the card data environment.

**Encryption of private networks.** While there is no requirement for encrypting data on private networks, it makes sense to do so. Attackers may find it relatively easy to penetrate perimeter defenses. Once inside, they can tap into an internal network and “sniff” card data as it flows by. Do not be guilty of “candy security”, hard on the outside, soft on the inside.

**Wireless networking.** Use WPA or WPA2 to secure all wireless transmissions. The current version of the DSS allows for the use of WEP with additional controls such as VPN or SSL/TLS.

**Restrict traffic.** Consider how card data is processed. For example, 80 gigabytes of card data was transferred during the TJX incident. In addition to source and destination, think about file sizes that traverse card data networks. Determine the maximum number of card numbers that should be returned in a SQL query. When you have thoroughly analyzed expected traffic, implement controls that limit data flow to those constraints. If traffic does not need to flow between stores, do not allow it.

**Risk assessments.** Monitor technology and incident trends and conduct predictive analysis from the data. Failure Mode and Effects Analysis can also be used to conduct risk assessments of processes and systems. Threat modeling is also a useful tool for evaluating the effectiveness of a control environment.

Adhere to PCI compliance requirements, monitor threats and address residual risk. PCI compliance represents the minimum necessary to protect card data.

Does your organization adequately mitigate the risk of compromise? Be certain of your response.