

PCI Security Standard Update Does Not Meet Merchants' Needs

Avivah Litan, John Pescatore

The first update to the Payment Card Industry's primary security standard in more than two years still fails to address merchants' most critical security and compliance issues.

NEWS ANALYSIS

Event

On 2 October 2008, the Payment Card Industry (PCI) Security Standards Council (SSC) introduced the first update to the PCI Data Security Standard (DSS) since September 2006. Detailed information on the update, which is effective immediately, is available at www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

Analysis

The updated PCI DSS makes some marginal improvements, bringing clarity to some sections of the standard. However, the update does not address the most fundamental issues facing retailers and other merchants and card-accepting enterprises that are trying to determine and demonstrate PCI compliance — and in some areas, broadened requirements will make it even more difficult for them to do so. For example, the updated PCI DSS fails to:

Recognize the huge differences between different types of merchants. The PCI DSS still places the same compliance requirements on small e-commerce operations as on large retail chains with hundreds of physical stores, even though their data processing environments are entirely different.

Acknowledge the substantial investments in chip and personal identification number (PIN) card technology made in many parts of the world, including most European countries. These investments should limit the scope of compliance efforts, but the updated standard does not even acknowledge these compensating controls and implementations.

Take into account the steps card-accepting enterprise can take that go beyond current PCI DSS requirements of the standard, notably end-to-end encryption of card data inside enterprise networks and the use of identity-aware networks to limit access to card data. Several large retailers are experimenting with these technologies, which should reduce the scope of compliance efforts.

The PCI enforcement process — which is beyond the scope of this update — also continues to be troubled by serious issues. The most important of these issues is inconsistency in the quality of assessments by qualified assessors, and even within the same assessment firms. Assessors also continue to sell remediation and managed security services, which cast doubts on the integrity of the assessment process itself.

RECOMMENDATIONS

Retailers and other merchants and card-accepting enterprises:

- Continue to focus on reducing or eliminating the storage of card data wherever possible, giving the protection of customer card data priority over compliance.
- Consider end-to-end encryption, beginning with the card reader, if you accept physical cards.
- Notify the PCI SSC if assessors that are trying to sell their own products or services or provide poor support.

PCI SSC:

- Update the PCI DSS to address the issues detailed above and offer meaningful guidance on how to properly segment a network.
- Remove firms that sell remediation services from the list of qualified assessors, or demand proof of separation between their assessment and services divisions.

RECOMMENDED READING

- "PCI Compliance Remains Challenging and Expensive" — A Gartner survey of 50 U.S. retailers shows that card-accepting enterprises still face significant technical and budgetary challenges when responding to PCI requirements. **By Avivah Litan**
- "The Payment Card Industry Must Disentangle PCI Assessments From Remediation" — The payment card industry needs to move quickly to address the high potential for conflict of interest in the PCI assessment process. **By John Pescatore and Avivah Litan**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509