

PCI Compliance Grows but Major Industry Problems Remain

Avivah Litan

Newly released statistics show Visa making strong progress in driving Payment Card Industry security compliance. But other card brands' compliance efforts, and PCI Security Council communications, still need improvement.

NEWS ANALYSIS

Event

On 22 January 2008, Visa released statistics on merchant compliance with the Payment Card Industry (PCI) Data Security Standard (DSS). Visa reported that as of the end of 2007, 77% of large merchants were PCI DSS-compliant (compared with 12% in March 2006) and 62% of midsize merchants were PCI DSS-compliant (compared with 15% at the end of 2006). These two merchant categories represent approximately two-thirds of Visa's transaction volume.

Analysis

The new statistics are unsurprising, because Visa has been proactively driving PCI compliance into the retailer market, using price incentives for those that comply and fines for those that do not. The Visa deadline of 30 September 2007 for Level 1 retailers (more than 6 million transactions per year) and 31 December 2007 for Level 2 retailers (1 million to 6 million transactions per year) has certainly been a successful compliance driver. Visa has also been open in communicating about both progress and problems.

The PCI Security Council and the other card brands have not, however, kept pace. The PCI Security Council's communications processes remain poor, and retailers still have far too many unanswered questions about PCI DSS requirements. For example, there is considerable confusion about the implications of outsourcing arrangements on the scope of PCI compliance efforts and how to adequately segment networks to reduce the scope of compliance activities.

Moreover, the PCI DSS remains unworkable for smaller merchants with limited payment-card-related infrastructure. The council has not yet distributed drafts of revised self-assessment questionnaires targeted at different types of merchants. It does plan to release its long-awaited final versions in February 2008. This raises the concern that many merchants have had to deal with compliance processes and questionnaires that do not apply to their environments — and are accountable for deadlines they may already have missed.

Moreover, the long-awaited Payment Application Data Security Standard (PA-DSS) — which is still in draft form — is far from what is needed to align payment applications with security best practices. One key problem is that the draft is written partly for companies implementing payment software applications, not solely for its intended audience of software developers, which could confuse the industry further.

RECOMMENDATIONS

Retailers and other card-accepting organizations:

- Use common sense in determining the scope of your PCI compliance efforts. (For example, a retailer that outsources the storage of cardholder data should recognize that — while proper data security must be maintained — it is unnecessary to encrypt data at rest or to audit access to stored data, because no data is stored at the retailer location). Retailers that believe the current self-assessment form is not applicable to their environments (because the form is primarily designed for Level 1 and 2 retailers' store networks) and have not yet filed a Report on Compliance should ask their acquiring banks for permission to wait for the new self-assessment forms.

The PCI Security Council and card brands other than Visa:

- Improve communications with stakeholders by issuing quarterly FAQs and compliance status reports.

RECOMMENDED READING

- "Proposed PCI Changes Would Improve Merchants' Data Security" — The security benefits of no longer requiring merchants to store complete transaction information would outweigh the burdens of the change. **By Avivah Litan**
- "PCI Questions Are Often Clearer Than Their Answers" — Many points of confusion remain as the retail sector marches down the road toward PCI compliance. **By Avivah Litan and John Pescatore**

(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