

New PCI Security Standards Council Needs More Power

Avivah Litan

The Payment Card Industry Security Standards Council's newly elected Board of Advisors will help to improve stakeholder communication. But the advisors need voting power and expanded authority to resolve problems.

NEWS ANALYSIS

Event

On 26 May 2007, the Payment Card Industry Security Standards Council (PCI SSC), an independent industry organization that manages the PCI Data Security Standard, announced the results of partial elections for its Board of Advisors. Fourteen organizations were elected, including three banks, four payment processors, three retailers and four other enterprises (see www.pcisecuritystandards.org/news_events/pci_ssc_announces_elected_board_of_advisors.htm for details). The members were elected by nearly 200 PCI SSC member companies, which can join by paying a \$2,000 annual fee (see www.pcisecuritystandards.org/join1.html). Seven more advisory members remain to be appointed by the PCI SSC's Executive Committee, which has indicated that it plans to seek more international representation.

Analysis

The election of the advisory board is a positive development that will help to improve communications between PCI stakeholders and the PCI SSC's Executive Committee and Management Committee. These committees represent the five major card companies that participate in the PCI (American Express, Discover, JCB, MasterCard and Visa) and hold all the voting power on policy and operational matters. Stakeholders have a strong interest in helping to formulate updates to the standard, as well as in developing clear guidance both on existing standards and on compensating controls when PCI requirements cannot be met. For example, it is often unclear whether PCI standards apply to all systems at card-accepting organizations, or only those segments that handle cardholder data.

Gartner is troubled by the Executive Committee's decision to reserve seven advisory seats to be appointed at its discretion, because the PCI SSC "Participating Organizations" should also be able to ensure international representation. Nonetheless, it is encouraging that major retailers, including Wal-Mart, are already represented. Wal-Mart has been at the forefront of retailers' struggles to lower card industry processing fees. Wal-Mart — which, according to its latest Securities and Exchange Commission (SEC) 10-K filing, paid banks \$882 million in card-transaction fees in 2006 — recently withdrew its request for a narrow bank charter in its efforts to lower its fees.

Gartner is also concerned that many of the most difficult PCI issues remain outside the authority of the PCI SSC, because enforcement remains the responsibility of the individual card brands. These issues include:

- Inconsistent merchant level classifications, enforcement deadlines and compliance requirements across participating card brands.
- Inconsistent international requirements, even within a given card brand. For example, global Level 1 merchants are typically engaged in the PCI compliance process only with their U.S. and Canadian acquirers. Banks in other parts of the world are frequently disengaged, even though retailers want to validate compliance only once across country borders.

RECOMMENDATIONS

Enterprises that wish to help shape the PCI SSC's future should join its Participating Organizations group as a means of:

- Presenting their views on compliance issues to the Board of Advisors.
- Influencing the Executive Committee to take on issues that are currently outside the PCI SSC's authority.
- Lobbying the PCI SSC to adopt a security standard for payment software. The PCI SSC plans to adopt the Visa Payment Application Best Practices (PABP) standard — and is preparing to issue standards for point-of-sale personal identification number (PIN) pads — but this work needs to be expedited.
- Promoting greater transparency among card-issuing banks concerning their own PCI compliance efforts.

RECOMMENDED READING

- "Answers to Common Questions About PCI Compliance" — Gartner clients continue to seek clarification about how best to achieve PCI compliance. **By Avivah Litan and John Pescatore**
- "How to Improve the Ailing PCI Program" — The PCI Data Security Standard was created in 2001, but the card-accepting industry is still struggling to demonstrate 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