

## Three years to catch up on payment security standards

2009 7:07am

Payment card companies have announced that they will toughen security standards for financial institutions, merchants and consumers in 2010 in an attempt to stop the growth of identity theft and other forms of payment system fraud.

The Payment Card Industry Security Standards Council, whose members include Visa, MasterCard, American Express, Discover Financial Services and JCB International, is pushing to have a broader group of merchants and service providers comply with the Council's security standard (PCI DSS).

And Visa has announced that it will start moving to universal chip and PIN technology for credit, debit and ATM transactions next year.

The industry accepts that it has a serious problem, with criminal activity directed at online payment data growing fast. But there is plenty of debate about whether the self-regulatory moves being made by bodies like the Payment Card Industry Security Standards Council are adequate.

Speakers at last week's Payment Card Industry Data Security Standard Compliance Conference in Sydney described the online payments market as "the wild west when it comes to security", a sector under "unprecedented attack" and one where "the cybercrime industry is doing really well".

The managing principal for investigative response at Verizon Business Security Solutions, Mark Goudie, said his team carried out forensic investigations of 285 million individual data breaches in 2008 – all confirmed thefts of card details. Most of these thefts were from US-based payment processors.

Goudie said: "Online data accounts for 99 per cent of those cases and payment card data is 98 per cent of the total."

He said 2008 was a milestone year, with the number of compromised records in breaches investigated by Verizon up from 39 million in 2007 and 75 million in 2006.

"The reason 2008 is such an anomaly is the result of five very large breaches, which account for more than 90 per cent of the records compromised."

He said the crimes were becoming more sophisticated all the time. In one recent case a criminal was negotiating to sell access to retail terminals with skimming devices in them supplying live data.

Visa Australia director of country risk management, Ian McKindley, said the industry was taking a number of steps to address the problem.

Visa announced last month that from January 2010 all new Visa cards issued in Australia will feature smart chips to give higher security. Changes to debit and prepaid cards will follow in 2011. At the same time all non-chip cards currently in use will be replaced so that by 2013 the use of signatures in transactions will be phased out.

Other projects include introduction of chip technology into ATMs. By 2012 card issuers must enrol all cards for Verified by Visa or its equivalents (such as MasterCard's SecureCode), which provides a password for online shopping. These systems have been voluntary up to now and some financial institutions have reported that take-up has been low.

McKindley said that for organisations, the PCI data security standard was "the best defence against theft of payment data." By July next year all merchants taking online payments will have to use software that is PCI DSS validated.

Compliance with the standard is being pushed out to small merchants and service providers. McKindley said a big project was to get card acquirers to work with merchants to remove vulnerable data from their files.

Compliance with the PCI data security standard has 12 requirements, including installation and maintenance of a firewall, protected storage and encrypted transmission of cardholder data, regular updating of anti-virus software, strong user access control systems and regular monitoring and testing of systems.

## PCI DSS little deterrent to payments crime

---

09 December 2009 7:04am

There were plenty of sceptics at last week's Payment Card Industry Data Security Standard Compliance Conference in Sydney, who argued that the industry's security standards were not good enough to stop the rising rate of cybercrime.

A number of speakers took aim at the Payment Card Industry Security Standards Council, saying its PCI DSS standard was flawed.

A director of the security consultant earthware, David Kaplan, said PCI DSS was like an audit requirement – companies did as little as possible to meet the standard and were apathetic about ongoing monitoring and analysis.

He said the other problem with the standard was that it was always catching up with new technology.

“Organisations put in a new widget and they don't know how to keep it secure. They think they are compliant but they don't see the problem coming.”

Kaplan said the claim by members of the PCI Security Standards Council that no organisation that is PCI DSS compliant has been breached was wrong.

The managing principal for investigative response at Verizon Business Security Solutions, Mark Goudie, said: “PCI DSS is not a failure, but it is no more than a minimum acceptable standard.

“The biggest flaw is event monitoring and log analysis. It is complicated to go through that mass of data and a lot of organisations are not doing it. That is why attackers are inside systems stealing data for an average of seven months before they are detected and why most breach notifications come from outside the company affected.

“The other big problem is that companies are storing data they don't even know about. In our investigations two-thirds of data was stolen from companies that did not know they held that data.”

The managing director of Lockstep Technologies, Stephen Wilson, said PCI DSS was a “patch” designed by payment card companies in the hope that they could avoid forcing merchants and financial institutions to use more complex, expensive and time-consuming procedures like encryption and two-factor authentication as a standard part of every transaction.

Wilson said the solution would not come until payment industry participants were all using dynamic data and stopped storing customer information.

Wilson said: “We need a standard like PCI DSS because merchants like to store customer data. Let's overturn that. When the card number is replaced with a token that generates a unique transaction password the problem of storing millions of cardholder identities goes away.”

Published from Melbourne, Australia by Ian Rogers ABN 68 204 093 594

© Copyright 2003— 2009 The Sheet