

ADVERTISEMENT



[Join SearchSecurity.com.AU for free access to security resources pertinent to your needs in Australia and New Zealand.](#)
[Home](#) > [Topics](#) > [Security management](#) > [Security risk management](#) > Credit card security standard largely ignored

Security AU News:

Credit card security standard largely ignored

By Patrick Gray

01 Aug 2007 | SearchSecurityAU

 [Digg This](#)  [Stumble](#)  [Delicious](#)

When the payment card industry introduced its Data Security Standard (PCI DSS) in 2005, the sad fact is many Australian organisations didn't notice.

In September 2006, Visa released figures showing less than half of Australia's credit card processors and merchants were aware of their obligations under the PCI DSS standard.

"Merchants are very aware of the significant risks to their businesses and reputation if customer data is mishandled or they fall victim to the growing threat posed by computer hackers," Visa's Executive Vice President in Australia, Bruce Mansfield, said when the survey data was released. "But the latest research tells us that we have a long way to go to educate merchants on what is required to protect cardholder data."

In other words, being concerned about customer data is one thing, but complying with a prescriptive set of mandatory guidelines like PCI DSS is another thing entirely.

PCI DSS, for the 51 percent apparently in the dark, is the data security standard developed by credit card providers which sets out minimum security standards for organisations that handle credit card data.

That's any organisation that processes or stores credit card information.

Merchants must demonstrate compliance to maintain access to processing facilities. They must build and maintain a secure network, install and maintain a firewall configuration to protect cardholder data, remove default passwords, encrypt transmission of cardholder data across open, public networks, use up-to-date anti-virus software, implement real access control measures and much, much more.

While the standard is long established -- now in its second release, 1.1 -- compliance rates, at least anecdotally, are slim.

"We have seen very few companies that are even close to compliance. The majority are nowhere near it when we walk in," says Drazen Drazic of Security-Assessment.com. "A lot of them will get to a stage where a decision has to be made. We have seen companies who've seen the results of a gap analysis ... question whether it's worth their while to continue processing credit cards."

Things have improved over the last six months, Drazic says, as banks have moved to pressure merchants into complying with the scheme. Large merchants must demonstrate compliance through regular scanning and on-site auditing from pre-approved PCI security assessors.

"A lot of them feel like it's been very sudden ... a lot of them had never heard of this from the acquiring banks, and all of a sudden these letters are arriving saying you've got to be compliant in six months time," Drazic says. "There's a couple that we've done in NZ that are really on top of it, but in Australia we're yet to find one organisation that was close to compliance."

While larger vendors are forced to engage external auditors, smaller merchants submit a self-assessment questionnaire. It works in theory, with the grapevine scuttlebutt suggesting 70-80 percent of self-assessed organisations are reporting 100 percent compliance with PCI DSS.

Yet with consultancies like Security-Assessment.com yet to encounter a single compliant organisation during an audit, it's more likely the smaller merchants are being a tad creative when filling out their self-assessments.

In any case, compliance to PCI DSS is not yet mandatory. As long as organisations can demonstrate a roadmap that will get them to the end goal of DSS compliance within a reasonable timeframe, they're safe. If they consistently fail, they may have their merchant facilities taken away by the payment card industry.

This fear has proved a significant business driver in the security business, as Drazic explained.

He's not the only one to notice the extra dollars ringing up in the till.

Rick Logan, Attachmate's senior technical consultant on compliance and security, says privacy legislation designed to protect consumer data hasn't had an effect on organisations' security budgets, in stark contrast to PCI DSS. "I haven't seen any projects being driven by that (privacy act) in particular," he says. "PCI DSS, that's probably a regulation that's seen more adoption in Australia."

Logan says the legislative framework in the United States has ensured companies there are a more compliance savvy than their down-under counterparts. "I think we're in the earlier stages compared with the US in regard to compliance. We have good regulations from a technology perspective but the drivers to comply aren't as severe as in the US," he says. "[For example], if you're out of compliance with Sarbanes Oxley, the CEO and CFO can be jailed, whereas I don't see that level of [threat here]," he says. "The threat is a larger threat than what they're currently putting in place in Australia. That threat has driven them to put in place compliance programs to meet their auditing programs to reduce the risk of them being imprisoned."

So at last we understand what it takes to get businesses implementing meaningful security programs: Threats of imprisonment or the cancellation of credit card processing rights. Stern threats work. Standards may not work as well!

REFERENCE DESK

Security risk management

NEWS, TIPS & MORE

- [Credit card security standard largely ignored](#) (NEWS)
- [How to create and enforce employee termination procedures](#) (TIP)
- [The roots of the Schneier/RSA spat](#) (NEWS)
- [Senate Select Committee on the NBN gives fiber security...](#) (NEWS)
- [Gartner security summit outlines 'Security 3.0'](#) (NEWS)

[→ VIEW MORE](#)

Introducing SearchSecurity.com.AU

Get the Security News and Tips that Matter to YOU!

Visit today, Bookmark the Page and Sign up for Email Updates

[Activate your membership today!](#)


SEE ALSO

- **Related Topics:**
[Security risk management](#), [Information security certification and career advice](#), [Australian security market](#)

GET E-MAIL UPDATES

Submit your e-mail below to receive searchSecurityAU-related news, tech tips and more, delivered to your inbox.

 Data Protection

 Email:

Not a member? We'll activate your FREE membership with your subscription.