Give PCI the bullet?

PCI security standards have been riddled with gaping holes since their inception. What's next for this smoking gun?

BY STEPHEN WILSON

Dissatisfaction with the Payment Card Industry (PCI) security standards has been simmering for some time, as the regime grows more and more burdensome. But after the recent data breach at Heartland Payment Systems – possibly the biggest heist of credit card data in history – the PCI debate is boiling over.

Heartland maintains it was in compliance with PCI requirements, and points instead to what it says are deeper problems in the security compliance regime (on this point Heartland is certainly not alone). On the other hand, credit card associations claim that no breaches have occurred at PCI-compliant organisations. This bald disputation is itself unsettling. Surely when it comes to PCI compliance, there should be no room for ambiguity?

PCI security has been called an "elaborate patch", alluding to the way it leaves fundamental weaknesses in card processing untouched. The core challenge is to protect digital identity data against copying and unauthorised replay. Over the years, the industry's chief response to card fraud has been to require merchants to gather more and more corroborating data to prove that a customer is who they say they are. But just as credit card numbers fall into the wrong hands, so too do billing addresses, CVVs and so on. The more identity data customers are required to divulge, the more ends up being stolen and used against them.

Now PCI is even on the agenda of the United States Government. In March, the US Homeland Security Committee held a hearing into whether PCI security standards have been effective in reducing cyber crime. The chair stated that in the wake of major data breaches, "the PCI Standards are of questionable strength and effectiveness".

These are fighting words. Legislators are clearly impatient, sensitive to their constituents' dwindling confidence in doing business online. Even worse for policy-makers is mounting evidence that credit card fraud is helping to finance terrorism. So the chair even flagged the possibility of government intervention if industry-based security standards prove to be ineffective.

The Homeland Security Committee heard from a number of stakeholders, including merchants, law enforcement and credit card associations. The CIO of the US National Retail Federation didn't mince words, submitting that since its inception "PCI has been plagued by poor execution... The PCI guidelines are onerous, confusing, and are constantly changing". He also noted the irony that "the credit card companies' rules require merchants to store credit card data that many retailers do not want to keep" (emphasis in original).

Down the audit trail...

In security circles, critics are revisiting the fundamentals of compliance audit, but in this debate, history is repeating itself. Conformance testing and audit are just not the silver bullets many would like them to be. The past is littered with businesses that have passed various audits only to let down their customers. ISO 9001 quality certified companies can turn out defective products; ISO 27001 security certified companies can get hacked; audited public companies can go bankrupt. In most cases, the auditors can distance themselves from such failures, but that only begs the question: what good is any audit?

The more identity data customers are required to divulge, the more ends up being stolen and used against them

Technical arguments about what an audit really means are often unedifying. Ordinary users have a right to expect that if their service provider passes its audits, then it can be relied upon. For a security audit to be meaningful, surely it has to confirm that the outfit in question is somehow "secure"?

The ugly truth is that most audits are mechanical and intrinsically blinkered. I speak from experience: I've been an auditor, and I've also been audited, under many different conformance regimes. Every six months or so, the auditor rolls in, armed with the report from the last visit, and checks if non-conformities have been remedied. But all too often, the auditor is a brand new junior, looking at the business for the very first time. Worse, the client representative is frequently also new, and had their very first look at the audit report on the way to the meeting. The parties face off across the table, get consumed by the paperwork, and can't see the forest for the trees.

I don't think I'm being overly cynical, but in any case, even the best run audits are inherently limited. Audits find problems, but the absence of findings does not mean an absence of problems.

As the chair of the US Homeland Security Committee put it at the PCI hearings: "The essential flaw with the PCI Standard is that it allows companies to check boxes, but not necessarily be secure. Compliance does not equal security. We have to get beyond check box security."

Everyone agrees that the PCI regime is better than nothing. In my view, like ISO 17799 style policy-based security management, PCI will generally reduce accidental breaches, and it can help fend off amateur attacks. But PCI can do little to thwart inside jobs, nor the sophisticated attacks of organised crime gangs.

The rewards to be gained from credit card fraud are now so enormous that no amount of security policy or conformance audit can defeat cyber criminals. Even data encryption may be futile. When a big data set is worth hundreds of millions of dollars on the black market, criminals will likely find the resources to crack even the strongest commercial encryption.

So the PCI security regime was always going to be a losing battle: an expensive endless loop of collecting ever more personal data to verify identity, and then needing to safeguard it all against theft. It's like putting out fire with gasoline.

It's high time that the underlying problem was dealt with properly. We need to remove the profit motive for stealing and trading credit card data. We need to make stolen data useless. The simplest, most robust, long-term solution probably lies in applying smart technologies like Chip-and-PIN cards to the online channel, to digitally sign each transaction and thus render it unique.

Stephen Wilson, founder of the Lockstep Group, is an analyst, consultant and innovator in digital identity. Lockstep Technologies works on smart solutions to CNP fraud and ID theft.
www.lockstep.com.au