

Why does the PCI remind me of my mother?

At the RSA 2010 conference in March, various speakers slated PCI DSS (Payment Card Industry Data Security Standard) compliance as too difficult. They complained that companies are too busy working on compliance to spend time on actual security, and suggested that complying with the PCI stifled innovation.

As I believe that security is rarely black-and-white, I agree with these opinions arising from RSA 2010. But I also believe that PCI DSS compliance must be enforced anyway, regardless of these—legitimate—complaints. A contradiction? No. Let me explain.

Once more, we see that self-regulation of information security simply does not work—especially when Visa and MasterCard are around to pick up the bill every time another database escapes into the wild

As a child, my room was always disorganized. My mother issued numerous warnings that, unless it was tidied up, everything on the floor would be consigned to the trash. I ignored the warnings. Then suddenly, my stuff was in the truck on its way to a landfill.

Responsibility

This dilemma is similar to the PCI's situation. When it comes to tidying up their information security, merchants that accept payment cards have been asked nicely, given plenty of reasons, nagged, warned and begged. Yet huge numbers have not done it, or have done it badly. Once more, we see that self-regulation of information security simply does not work—especially when Visa and MasterCard are around to pick up the bill every time another database escapes into the wild. In the end, it became necessary for the PCI to force mandatory compliance on the merchant-community—because every other approach has failed.

The rigidity of compliance has a negative effect on some. Organizations complaining about stifled innovation are, for all their technical skill and awareness of risk management, a

tiny minority who are in the technical vanguard. It is likely that they do not even realize the extent of the security problems (technical and cultural) that exist in e-commerce. I sympathize with their grievances, but these organizations must accept that, although the limitations of the less-capable are holding them back, compliance is in the interests of the e-commerce community as a whole.

Furthermore, while the maxim that “compliance does not equal security” is absolutely correct, critics of the PCI's approach should bear in mind that many businesses have neither. If these organizations are forced to comply with a standard like the DSS, then that does not necessarily mean they end up secure, but at least it means they've been forced to invest thought and resources into the matter.

Insecurity blitz

Over the last 15 years the Net has seen one security problem after another (Bill Gates assured us: “Two years from now, spam will be solved”...in 2004). All have impacted the overall Internet community—a community whose innocent majority aren't responsible for contributing to the situation. Now it's happening again: many have already decided to reject e-commerce because they're uncomfortable about trusting their credit- or debit-card details to online retailers. This trend cannot be allowed to continue without action to turn the situation around.

Instead of complaining about the technical limitations of PCI compliance, it's better to take the long-term view. Be grateful that the PCI has shouldered the task of giving the Internet community a chance to improve confidence in the safety of online transactions.

I hope that the PCI will liberalize the DSS in the not-too-distant future, allowing competent and sophisticated organizations the freedom to innovate and to take responsibility for their own security. But there are more important priorities. We must walk before we can run.



Richard Stagg is director and managing consultant of consultancy firm Handshake Networking Ltd (HKSAR). Contact him at rjs@handshake.hk