

SANS NewsBites - Volume: IX, Issue: 7

Current Newsletters

- [SANS NewsBites](#)
- [@RISK: The Consensus Security Alert](#)
- [Ouch!](#)
- [SANS ExecuBytes](#)



SANS Cyber Guardian Program
**Real Threats,
 Real Skills,
 Real Success**

[Click here to learn more](#)

[SANS Newsletters Home](#)

STANDARDS & BEST PRACTICES

PCIDSS Compliance Products Require Diligence (22 January 2007)

The appearance of "a number of merchant retail solutions that address [the Payment Card Industry Data Security Standard]

compliance" has prompted one PCIDSS auditor to warn companies that simply purchasing these approved products does not ensure compliance with the standard. The auditor notes that organizations need to be cognizant not only of how they implement the solution, but of how they "manage and maintain those systems." Companies found not to be in compliance with PCIDSS could face stiff fines.

[-http://www.computerworld.com.au/index.php/id;962716575;fp;16;fpid;1](http://www.computerworld.com.au/index.php/id;962716575;fp;16;fpid;1)

[Editor's Note (Pescatore): There are payment applications and card processing/handling systems that are validated against the PCI Payment Applications Best Practices, but security products are not. The PCI DSS standards and assessment process are pretty clear on this, and recent clarifications make it pretty clear that merchants are still responsible for protecting customer data whether they use those products or approved service providers.

(Ranum): This is one of the few bits of news I've seen in NewsBites in the last few years that actually cheers me up. The idea that it's not just enough to simply OWN a doo-dad - that you have to UNDERSTAND how it WORKS! Wow! Maybe security is maturing, after all...

(Honan): The auditor Mr. Drazic is highlighting a common problem with many security implementations. Security is not solely about a technical solution or product, but more so on how that product and technology is integrated within a comprehensive security program involving people, policies, processes and technology. Too often companies treat information security as a technical problem and therefore apply technical solutions rather than treating information security as a business issue.

(Liston): Unfortunately PCIDSS compliance, as evidenced by the stories about Nordea and TSP, is only half the battle. Locking down merchants is great, but only shifts the battleground to the consumer's PC. Even if we deny them the "big score" by locking down the basket containing *all* the eggs, the Nordea story clearly shows that there is still a lot of profit to be had by hanging out with the chickens.]

Check Them Out!

- [Network Security 2010](#)
- [Security Awareness Training](#)
- [Top Cyber Security Risks](#)
- [SANS Reading Room](#)
- [Career Roadmap](#)
- [Storm Center](#)
- [WhatWorks™](#)
- [Newsletters](#)

"I learned techniques and processes that I can use as soon as I walk back into work."
 -Michael Marrion

SANS
NETWORK SECURITY
2010

Your personal