bizcommunity

New PCI security standards: Lock it down, lock it tight

USA: New Payment Card Industry (PCI) regulations are just around the corner, and retailers dealing with credit cards will need to tighten up their standards in order to comply. For instance, your firewall performance will be reviewed more often, and you'll have to use anti-virus protecti even on non-Windows platforms. Also, if you're still using WEP encryption, better get ready to chuck that and move to something better ASAP.

By Jack M. Germain 3 Sep 2008

The PCI regulation changes that take affect on 1 October will mean some additional work by IT departmer - and some new spending.

But the PCI Data Security Standard (DSS) version 1.2 will allow the Payment Card Industry a phase-in per to meet the new rules, according to two security firms that provide compliance tools.

The PCI Data Security Standard, first adopted by the PCI Security Standards Council in 2005, contains 12 rules with several sub-sections. The council amended some of those regulations with Version 1.1 in September of 2006. The PCI DSS standards are a set of comprehensive requirements for enhancing payment account data security.

The standards were developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.

In version 1.2, "there are two dozen small changes, some with fairly significant implications," Mike Loyd, chief scientist for RedSeal Systems, told the *E-Commerce Times*.

Read the full article here.

For more, visit: https://www.bizcommunity.com