

The countdown to compliance with PCI DSS v3.0 has begun

ELY , UK, December 10, 2014 /EINPresswire.com/ -- From 1 January 2015 merchants and service providers must ensure that their validation efforts for compliance follow the version 3 requirements of the Payment Card Industry Data Security Standard (PCI DSS).

Along with other important changes, [PCI DSS v3.0](#) has introduced a 'business as usual' approach to help organisations act proactively when it comes to protecting cardholder data.

Yet, worryingly, the Verizon 2014 PCI Compliance Report revealed that only 11.1% of organisations fully complied with the requirements of the PCI DSS in 2013, and only one in five organisations came close to complying and passed 95%+ of controls.

Global cyber security provider and PCI QSA company [IT Governance](#) warns that if a business is found to be noncompliant, it can suffer considerable repercussions.

Geraint Williams, head of technical services at IT Governance, says, "The credit and debit card industry is at particular threat from fraud and data breaches. Evidence suggests that cyber criminals increasingly target retailers and their supply chain to steal customers' credit card details and other personally identifiable information. It is of paramount importance that all organisations that handle credit card data comply with the PCI DSS as the minimum level of achieving cyber security."

PCI DSS v3.0 requires companies to reassess their data protection strategies and implement interventions that embrace a comprehensive approach to security.

The changes introduced by version 3 have been categorised under three headings – namely 'clarifications', 'additional guidance' and 'evolving requirements' – in order to further clarify the often complex elements of the Standard.

Version 3 requires both merchants and service providers to have written agreements on which services are the responsibility of the relevant party for PCI DSS accreditation. This is to ensure that there is no doubt who is responsible and that no requirement is left uncovered. Service providers will need agreements with their service providers. This should ensure that the whole supply chain covering payment card transactions is covered. Retailers will need to ensure PIN entry devices (PEDs) are protected against substitution and tampering.

Williams adds, "Complying with the PCI DSS is a demanding and resource-intensive process, so it is wise for organisations without the necessary PCI expertise to seek out professional guidance and support to ensure they are interpreting the Standard correctly."

IT Governance offers a full range of services designed to help organisations meet the PCI DSS v3.0 requirements. These include:

- PCI Transition Consultancy -www.itgovernance.co.uk/shop/p-1674.aspx
- PCI DSS Documentation Toolkit -www.itgovernance.co.uk/shop/p-1011.aspx

- PCI DSS Implementation Training Course - www.itgovernance.co.uk/shop/p-1279.aspx

For more products and services and further inquiries, call +44 (0)845 070 1750 or send an email to the IT Governance customer service team.

- Ends -

NOTES TO EDITORS

IT Governance Ltd is the single-source provider of books, tools, training and consultancy for IT governance, risk management and compliance. It is a leading authority on data security and IT governance for business and the public sector. IT Governance is 'non-geek', approaching IT issues from a non-technology background and talking to management in its own language. Its customer base spans Europe, the Americas, the Middle East and Asia. More information is available at www.itgovernance.co.uk.

Desi Aleksandrova
IT Governance
+44 (0) 845 070 1750
email us here

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.

© 1995-2018 IPD Group, Inc. All Right Reserved.