Correct scoping and security testing critical for complying with PCI DSS

ELY , UK, April 20, 2015 /EINPresswire.com/ -- The newly released Verizon PCI Compliance Report reveals that not testing security systems properly was the biggest reason for failure to comply with the Payment Card Industry Data Security Standard (PCI DSS) at an interim assessment.
Testing security systems is mandated by requirement 11 of the PCI DSS.
The study found that just 33% of companies passed all of the PCI DSS controls and testing procedures set out in requirement 11, and just 9% of all breached organisations were compliant with this requirement.

Geraint Williams, head of technical services at IT Governance, a PCI QSA and CREST-member company, says: "According to the report, 'In 2014, two-thirds of organizations did not adequately test the security of all in-scope systems'. Failure to correctly define the scope is probably the root cause of breached companies failing to be compliant with the security testing requirements at the time of breach.

“Entities are supposed to declare the scope of their PCI DSS environment, the assessor during the audit is required to validate that the scope of the assessment is accurately defined and documented – they do not define the scope. The assessor reviews the documentation that shows how the entity determined the PCI DSS scope.

"When investigators go in they find systems that should have been in-scope, but had not originally been included in the scope documentation. The investigators will report the entity to be non-compliant.

"This shows how important it is to correctly scope the PCI DSS compliance environment and, if necessary, take advice from PCI-accredited professionals (PCI-P).”

As an approved QSA, with accredited PCI-P consultants and CREST-accredited penetration testing specialists, IT Governance offers a full range of PCI compliance-related services including:

• PCI Gap Analysis and Scoping
• PCI Implementation and continual improvement
• Compliance Audit and ROC
• Validation and SAQ Completion
• Maintenance and Continual Improvement

To find out more about IT Governance’s PCI compliance services, visit: www.itgovernance.co.uk/pci_dss.aspx.

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