PCI DSS 3.2 set to expose compliance cramming culture, warns PCI Pal

Submitted by: Peptalk Communications
Tuesday, 30 January 2018

• New data security standard comes into force 1 February, requires evidence of constant compliance
• Four out of five companies failing interim PCI DSS assessments*
• Total cost of an average data breach stands at $4M**

The 1st February 2018 marks the deadline for businesses to adopt new industry standard, PCI DSS 3.2, aimed at reducing and better responding to cyber-attacks resulting in payment data breaches.

Originally announced in 2016, the industry has had almost two years to prepare for these increased requirements but a significant percentage of businesses are still not prepared, secure payment solutions provider, PCI Pal (http://www.pcipal.com), warns.

PCI Pal CTO, Geoff Forsyth, explains: “The industry has developed a culture of ‘compliance cramming’, treating PCI as an annual exam to be passed without working towards a culture of continuous compliance. For businesses in this ‘annual pass’ group, PCI DSS 3.2 could be a rude awakening because it requires evidence of continuous compliance instead of a pass/fail.”

Primary requirements of PCI DSS 3.2 include:
Expansion of requirement 8.3 to include use of multi-factor authentication for administrators accessing the cardholder data environment
Additional security validation steps for service providers and others, including the “Designated Entities Supplemental Validation” (DESV) criteria

Despite existing data security standards, many companies struggle to ensure continuous compliance - data taken from a 2017 report found that at the time of data compromise the average merchant is not compliant with almost half (47%) of current PCI DSS requirements. Of those that do pass compliance checks, almost a third are not compliant just 12 months later, according to Verizon’s PCI DSS Compliance report.

Forsyth continues: “To be PCI compliant is a constant process. The annual assessment has, to date, only been able to check that the correct processes are in place. PCI DSS 3.2 will change that approach, requiring evidence that device inventories and configuration standards are kept up to date, and security controls are applied where needed.

"Companies should no longer rely on outdated workarounds such as pause-and-resume, when taking payments over the phone. The recent spate of high-profile security has thrust this issue into the spotlight but this new standard will ensure it stays front of mind for the industry at large.”

For more information, visit www.pcipal.com or call +44 207 030 3770 to arrange a demonstration. Alternatively, follow PCI Pal on Twitter (https://twitter.com/PCIPAL?lang=en).

ends

Notes to Editors:

*Data from Verizon (http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf)
**Data from Ponemon Institute (https://www.ibm.com/security/infographics/data-breach/)

About PCI Pal PLC:
PCI Pal is a specialist provider of secure payment solutions for contact centres and businesses taking Cardholder Not Present (CNP) payments. PCI Pal's globally accessible cloud platform empowers organisations to take payments securely without bringing their environments into scope of PCI DSS and other card payment data security rules and regulations.

With the entire product portfolio served from PCI Pal's cloud environment, integrations with existing telephony, payment, and desktop environments are simple and light-touch, ensuring no degradation of service while achieving security and compliance.

PCI Pal has offices in London, Ipswich (UK) and Charlotte NC (USA). For more information visit www.pcipal.com or follow the team on Twitter: https://twitter.com/PCIPAL

Editor's Contact:
Peppa Sheridan
Peptalk Communications
+ 44 (0)1787 313822 / peppa@peptalkpr.co.uk