Payment Security Compliance drops for the first time in six years, states Verizon's 2018 Payment Security Report
Tuesday, September 25, 2018 04:01:00 AM (GMT)

Verizon 2018 Payment Security Report (PSR) highlights:

- **Full compliance with the Payment Card Industry Data Security Standard (PCI DSS) drops for the first time in six years – 52.5 percent of organizations compared to 55.4 percent in 2016.**
- **Businesses more vulnerable to cybercrime - PCI DSS is shown to help protect payment systems from breaches and theft of cardholder data.**
- **Report highlights the crucial need for ongoing compliance maintenance and measurement.**
- **Includes Verizon's nine factors for controlling compliance effectiveness and sustainability.**

BASKING RIDGE, N.J., Sept. 25, 2018 (GLOBE NEWSWIRE) -- After documenting improvements in Payment Card Industry Data Security Standard (PCI DSS) compliance over the past six years (2010 – 2016), Verizon's 2018 Payment Security Report (PSR) now reveals a concerning downward trend with companies failing compliance assessments and perhaps, more importantly, not maintaining - full compliance.

The Payment Card Industry Data Security Standard (PCI DSS) helps businesses that offer card payment facilities protect their payment systems from breaches and theft of cardholder data. PCI DSS compliance has been shown (via the Verizon Data Breach Investigations Report series) to help protect payment systems from both data breaches and theft of cardholder data, so this trend is alarming.

Data gathered by Verizon's PCI DSS qualified security assessors (QSAs) during 2017 demonstrates that PCI compliance is decreasing amongst global businesses, with only 52.4 percent of organizations maintaining full compliance in 2017, compared to 55.4 percent in 2016. Regional differences are highlighted, demonstrating that companies in the Asia-Pacific region are more likely to achieve full compliance at 77.8 percent, compared to those based in Europe (46.4 percent) and the Americas (39.7 percent). These differences can be attributed to the timing of geographical compliance rollout strategies, cultural appreciation of awards/recognition, or the maturity of IT systems.

By business sector, IT services remain on top when it comes to compliance, with over three-quarters of organizations (77.8 percent) achieving full status. Retail (56.3 percent) and financial services (47.9 percent) were significantly ahead of hospitality organizations (38.5 percent), which demonstrated the lowest compliance sustainability. With businesses often leveraging PCI DSS compliance efforts to meet the security requirements of data protection regulations, such as the European Data Protection Regulation (GDPR), this gap between the various business sectors that deal with electronic payments on a daily basis is significant.

"PCI Compliance standards are slipping across global businesses and this simply can't continue," comments Rodolphe Simonetti, global managing director for security consulting, Verizon. "Consumers and suppliers alike trust brands to secure their payment data, so we must act now to remedy this state of affairs. We urge businesses to reassess their measurement methodologies for PCI control effectiveness, and to concentrate on managing the sustainability of their data protection."

Control effectiveness and sustainability are essential

Simonetti continues: "Verizon has been at the forefront of cardholder data security since 2003, working closely with the PCI community to advance PCI DSS compliance. Based on our expertise and work in the field, we have developed nine factors which help businesses sustain their compliance levels. Our aim is to provide a clear structure and methodology to firstly help compliance personnel, but also equip them to open compliance dialogue with their board members, making the narrative easier to understand. For compliance processes to be effective, they need to be driven from the top, but often progress or challenges are not clearly communicated or understood by executives."

Verizon's nine factors of control effectiveness and sustainability support the 12 key requirements of the PCI DSS standard and are as follows:

- **Factor 1: Control Environment:** The sustainability and effectiveness of the 12 Key Requirements depends on a healthy **Control Environment**.
- **Factor 2: Control Design:** Proper control operation to meet DSS security control objectives depends on sound **Control Design.**
- **Factor 3: Control Risk:** Without on-going maintenance (security testing, risk management, etc.), controls can degrade over time and eventually break down. Mitigation of control failures requires integrated management of **Control Risk.**
- **Factor 4: Control Robustness:** Controls operate in dynamic business and ever-changing threat environments. They must be **robust** to resist unwanted change to remain functional and perform to specifications (configure standards, access control, system hardening, etc.).
- **Factor 5: Control Resilience:** Security controls can potentially still fail, despite adding layers of control for increased robustness, therefore control **resilience** with proactive discovery and quick recovery from failure is essential for effectiveness and sustainability .
- **Factor 6: Control Lifecycle Management:** To achieve all of the above it is necessary to monitor and actively manage security controls throughout each stage of their **lifecycle** from inception to retirement.
- **Factor 7: Performance Management:** Establishing and communicating **performance standards** to measure the actual performance of the control environment improves control effectiveness, and promotes predictable outcomes of your data protection and compliance activities, allowing for early identification and correction of performance deviations.
- **Factor 8: Maturity Measurement:** A control environment should never be stagnant – it must improve continuously. To do so, businesses need a roadmap, a target level of process and capability **maturity** to track the degree of formality and optimization of processes as indication of how close developing processes are to being complete and capable of continual improvement.
- **Factor 9: Self-Assessment:** Achieving all of the above requires in-house proficiency – resource capacity (people, processes and technology), capability (supporting processes), competency (skills, knowledge and experience) and commitment (the will to consistently adhere to compliance requirements) – in short a **self-assessment** proficiency.

“Data-sharing and cross-industry collaboration is vital to understand the evolving threat landscape and to progress global payment security. As evident in this report, organizations continue to face challenges maintaining high-levels of security and demonstrating ongoing compliance in rapidly changing environments,” said Troy Leach, Chief Technology Officer of the PCI Security Standards Council. “Organizations should pay close attention to the findings in the report to remain vigilant for key learnings on how to remain secure. Compliance should never be seen as the end goal for security but rather a measurement for an organization’s continued success in protecting data.”

In order to keep businesses on the right compliance track Verizon has also developed a comprehensive timeline within the report which charts timing for specific compliance activities.

About the Verizon 2018 Payment Security Report

The aim of the 2018 PSR is not to convince readers of the need for PCI compliance, but rather to emphasize the value of measuring performance and control effectiveness. This year's report includes the results from PCI assessments conducted by Verizon's team of PCI Qualified Security Assessors for Fortune 500 and large multinational firms in more than 30 countries.

Similar to Verizon's Data Breach Investigations Report series, the 2018 PSR is based on actual casework with a specific focus on financial services (58 percent); IT services (15 percent), retail (13 percent) and hospitality (11 percent). Geographies include the Americas (48 percent), the Asia-Pacific region (30 percent) and Europe (23 percent).

The Verizon 2018 Payment Security Report can be downloaded here.

About Verizon Security Professional Services
Verizon is a highly respected security consultancy and a trusted voice in the PCI Security community, having conducted over 16,000 security assessments, since 2009, for Fortune 500 and large multinational companies. Verizon manages over 4,000 customer networks worldwide, and itself operates one of the world's largest global IP networks, giving the company a unique perspective on security operations. Verizon offers a variety of consulting and assessment programs related to payment security and compliance (PCI-

DSS, PA-DSS, P2PE, EI3PA, PIN and ECB); and healthcare security and compliance (HIPAA, ONC Health IT, ConCert by HIMSS); and also offers security testing and certifications for security hardware, software, solutions and IoT (through Verizon ICSA Labs) and threat and vulnerability testing. For more information please click here.

Verizon Communications Inc. (NYSE, Nasdaq: VZ), headquartered in New York City, generated $126 billion in 2017 revenues. The company operates America's most reliable wireless network and the nation's premier all-fiber network, and delivers integrated solutions to businesses worldwide. Its Oath subsidiary reaches people around the world with a dynamic house of media and technology brands.

VERIZON'S ONLINE MEDIA CENTER: News releases, stories, media contacts and other resources are available at www.verizon.com/about/news/. News releases are also available through an RSS feed. To subscribe, visit www.verizon.com/about/rss-feeds/.

Verizon global media contacts:

Nil Pritam (APAC)
+65.6248.6599
nilesh.pritam@intl.verizon.com

Clare Ward (EMEA)
+44.118.905.3501
clare.ward@intl.verizon.com

Ilya Hemlin (US)
+1.908.295.7677
ilya.hemlin@verizon.com

Primary Identifiers: VZ-US
Related Identifiers: VZ-US
Subjects: Market Research Reports