Verizon 2017 Payment Security Report demonstrates a link between payment card security standard compliance and the ability to defend against cyberattacks
Thursday, August 31, 2017 04:01:00 AM (GMT)

BASKING RIDGE, N.J., Aug. 31, 2017 /PRNewswire/ --

Verizon 2017 Payment Security Report (PSR) Highlights:

- **Payment Card Industry Data Security Standard (PCI DSS) helps protect payment systems from breaches and theft of cardholder data**
- **Of ALL the payment card data breaches Verizon investigated, no organizations were found to be fully compliant at the time of breach, demonstrating lower compliance with 10 out of the 12 PCI DSS key requirements**
- **The total number of organizations Verizon assessed achieving PCI compliance at interim validation has increased to 55.4 percent, up from 48.4 percent in 2015, but maintaining compliance is still an issue**

With cybercrime on the increase, payment card security is increasingly a focus for companies and consumers alike. The Payment Card Industry Data Security Standard (PCI DSS) is there to help businesses that take card payments protect their payment systems from breaches and theft of cardholder data. The findings from the Verizon 2017 Payment Security Report (2017 PSR) demonstrate a link between organizations being compliant with the standard, and their ability to defend themselves against cyberattacks.

Of all payment card data breaches Verizon investigated, no organization was fully compliant at the time of breach, and showed lower compliance with 10 out of the 12 PCI DSS key requirements.

Overall PCI compliance has increased amongst global businesses, with 55.4 percent of organizations Verizon assessed passing their interim assessment in 2016. This is an increase from 2015, when only 48.4 percent of organizations achieved full compliance during their interim validation. This means that nearly half of retailers, restaurants, hotels and other business that take card payments are still failing to maintain compliance from year to year.

"There is a clear link between PCI DSS compliance and an organization's ability to defend itself against cyberattacks," comments Rodolphe Simonetti, global managing director for security consulting, Verizon. "Whilst it is good to see PCI compliance increasing, the fact remains that over 40 percent of the global organizations we assessed – large and small - are still not meeting PCI DSS compliance standards. Of those that pass validation, nearly half fall out of compliance within a year — and many much sooner."

Key insight and real-life examples into business sector compliance

According to the report IT services industry achieved the highest full compliance of all key industry groups studied. Globally, about three fifths (61.3 percent) of IT services organizations achieved full compliance during interim validation in 2016, followed by 59.1 percent of financial services organizations (which includes insurance companies), retail (50 percent) and hospitality (42.9 percent).

The 2017 PSR also flags the compliance challenges faced by specific business sectors including:

- Retail: security testing, encrypted data transmissions and authentication.
- Hospitality and travel: security hardening, protecting data in transit and physical security.
- Financial Services: security procedures, secure configurations, protecting data in transit, vulnerability management and overall risk management.

Real-life examples highlight situations where compliance controls are not followed. For example – a financial services organization seeking exemption from the Wi-Fi requirements of PCI DSS was surprised to learn that it did in fact have a wireless network operating in its building – this lack of knowledge causing it to fail. The IT admin had got tired of traipsing from the server room in the basement to the IT department on the third floor, and so had installed a router to access the servers from his desk.

Mind the 'control gap' – key to compliance sustainability

When looking at the PCI controls that companies would be expected to have in place (such as security testing, penetration tests etc), the report found an increased 'control gap,' meaning that many of these basics were absent. In 2015, companies failing their interim assessment had an average of 12.4 percent of controls absent; this has increased to 13 percent in 2016.

Simonetti continues, "It is no longer the question of *'if'* data must be protected, but *'how'* to achieve sustainable data protection. Many organizations still look at PCI DSS controls in isolation and don't appreciate that they are inter-related - the concept of control lifecycle management is far too often absent. This is often the result of a shortage of skilled in-house professionals - however, in our experience, internal proficiency can be dramatically improved with lifecycle guidance from external experts."

The 2017 PSR offers five key guidelines to assist with control lifecycle management:

1. **Consolidate for ease of management -** Adding more security controls is not always the answer – the PCI DSS Standard already contains numerous interlinked data protection standards and regulations. Organizations should be able to use this to consolidate controls, making them easier to manage overall.
2. **Invest in developing expertise –** Organizations should invest in their people to develop and maintain their knowledge of how to enhance, monitor and measure the effectiveness of controls in place.
3. **Apply a balanced approach –** Companies need to maintain an internal control environment that is both robust and resilient if they want to avoid controls falling out of compliance.
4. **Automate everything possible -** Applying data protection workflow and automation can be a huge asset in control management – but all automation also needs to be frequently audited.
5. **Design, operate, and manage the internal control environment –** The performance of each control is inter-linked. If there is a problem at the top, this will impact the performance of the controls at the bottom. It is essential to understand this in order to achieve and maintain an effective and sustainable data protection program.

Troy Leach, chief technology officer for the PCI Security Standards Council comments: "The report highlights the challenges organizations have to consistently maintain security controls on an ongoing basis, leaving their cardholder data environments vulnerable to attack. This trend was a key driver for changes introduced in PCI Data Security Standard version 3.2., which focus on helping organizations confirm that critical data security controls remain in place throughout the year, and that they are effectively tested as part of the ongoing security monitoring process."

About the 2017 Verizon Payment Security Report

The aim of the 2017 PSR is not to convince readers of the need for PCI compliance, but to track the measurable performance of PCI compliance. 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 2017 PSR is based on actual casework with a specific focus on financial services (47.5 percent); IT services (22.3 percent), hospitality (15.1 percent) and retail (14.4 percent). Geographies include the Americas (42.4 percent), Europe (28.1 percent) and the Asia-Pacific region (29.5 percent).

The 2017 Verizon 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 15,000 security assessments, since 2009, including for Fortune 500 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, has a diverse workforce of 163,400 and generated nearly $126 billion in 2016 revenues. Verizon 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 houses more than 50 media and technology brands that engage about 1 billion people around the world.

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/.

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

Maria Montenegro (US)
312.894.2361
maria.montenegro@verizon.com

Related Links
http://www.verizon.com/
https://www.verizonwireless.com/
http://www.verizonenterprise.com/
http://www.verizon.com/about/

View original content with multimedia: http://www.prnewswire.com/news-releases/verizon-2017-payment-security-report-demonstrates-a-link-between-payment-card-security-standard-compliance-and-the-ability-to-defend-against-cyberattacks-300511761.html

SOURCE Verizon

Countries: United States
Industries: Telecommunications, Banking & Financial Services, Computer Electronics, Hardware & Software, High Tech Security, Multimedia, Internet & Wireless Technology
Languages: English
Primary Identifiers: VZ-US
Related Identifiers: VZ-US