Payment Card Security Compliance Remains Problematic, Putting Confidential Consumer Information at Risk, Verizon Report Says
Wednesday, September 28, 2011 04:02:00 AM (GMT)

Noncompliance Is Linked to Increased Breach Risk

NEW YORK, Sept. 28, 2011 /PRNewswire/ -- For the second year in a row, a Verizon report has found that too many businesses are struggling to comply with payment card security standards, putting consumers' confidential information at risk.

According to the Verizon Payment Card Industry Compliance Report, most businesses that accept credit or debit cards, or both, continue to struggle to achieve and maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS). As a result, they are at greater risk of losing confidential customer information and falling victim to credit-card fraud.

Businesses are failing to maintain compliance even though they face steep penalties, including fines and increased transaction fees from the credit card brands. Businesses also now face pressure from their partners and customers to demonstrate continued compliance.

In addition to analyzing the overall current state of compliance with the PCI DSS, the report examines how well organizations comply with the 12 specific PCI requirements and provides recommendations that organizations can implement to help them earn and maintain compliance.

"We had hoped to see more organizations complying with the PCI standard, since we believe that compliance will ultimately improve the security posture of organizations and in all likelihood lead to fewer breaches," said Wade Baker, director of risk intelligence, Verizon. "By reviewing this report, organizations can see where to focus their efforts and implement our recommendations for helping to accelerate PCI compliance. Our end goal is a safer credit-card environment for consumers and businesses."

(**NOTE**: Additional resources supporting the report are available, including an audio podcast and high-resolution charts and graphs.)

PCI Report Findings Based on Actual PCI Assessments, Data Breaches

The report is based on findings from more than 100 PCI DSS assessments conducted by Verizon's team of PCI Qualified Security Assessors in 2010, as well as data gathered by Verizon's Investigative Response group while investigating real-world payment card data breaches. Additionally, the Verizon Risk Intelligence team overlaid the assessment findings with data-breach cases from the 2011 Verizon Data Breach Investigations Report, resulting in a richer, more thorough data set.

The assessments include data from organizations based in the U.S., Europe and Asia, representing for the first time the global nature of the PCI standard.

Key Findings

Top findings from the 2011 Verizon Payment Card Industry Compliance Report include:

- **While the compliance situation has neither worsened nor improved, it is still "disappointing."** Only 21 percent of organizations were fully compliant during the initial audit. The report notes that the difficulty in achieving compliance, along with overconfidence, complacency and the need to focus on other compliance and security issues are among the possible reasons for the widespread PCI noncompliance.
- **Lack of PCI compliance continues to be linked to data breaches.** The report demonstrated again this year that breached organizations are more likely not to be PCI compliant and are more likely to suffer from identity theft and fraud issues.
- **Organizations struggle with key PCI requirements.** Organizations struggled the most to comply with requirements 3 (protect stored cardholder date), 10 (track and monitor access), 11 (regularly test systems and processes), and 12 (maintain security policies), all of which are directly linked to protecting cardholder data.

- **Failure to prioritize compliance efforts often means high-risk security threats are ignored.** Launched in 2009, the Prioritized Approach was created to help organizations identify and reduce risk to cardholder data and to ease the annual PCI process. The report found that rather than using a risk-based approach to PCI compliance, organizations instead rely on the PCI DSS for guidance. As a result, many organizations are ignoring security threats with the highest risk and potential for the largest negative impacts.
- **PCI standard offers protection against the most common attack methods.** Malware and hacking are the most predominant methods used to gain access to cardholder data. Several overlapping PCI requirements are aimed at protecting against these attack methods.

Recommendations for Meeting Compliance

Based on extensive analysis, Verizon offers the following recommendations to help organizations meet their PCI compliance goals:

- **Treat compliance as an everyday, ongoing process.** Compliance requires continuous adherence to the standard. This means a daily log review, weekly file-integrity monitoring, quarterly vulnerability scanning and annual penetration testing. To achieve this, Verizon recommends that an internal PCI "champion" ensure that compliance becomes part of daily business activities.
- **Self-validate very carefully – or not at all.** Level 1 and 2 merchants -- who process the highest volumes of cardholder transactions --are allowed to assess themselves against the standard. Due to the numerous issues and conflicts of interest this can cause, Verizon highly recommends that an objective third party validate the scope of the assessment or perform the testing.
- **Prepare to have the bar raised.** In October 2010, the PCI Security Standards Council announced PCI DSS version 2.0. This version requires a more stringent executive summary and validation of methodology for scope definition. Organizations, many of which are having severe issues complying with the existing standards, need to quickly get ready for the new version.

Additional findings and recommendations are available in the full report, which can be downloaded at http://www.verizonbusiness.com/go/2011pci/us. In addition to the report, readers can access all report resources by visiting the Verizon PCI Report Resource Center.

About Verizon

Verizon Communications Inc. (NYSE, NASDAQ: VZ), headquartered in New York, is a global leader in delivering broadband and other wireless and wireline communications services to consumer, business, government and wholesale customers. Verizon Wireless operates America's most reliable wireless network, with more than 106 million total connections nationwide. Verizon also provides converged communications, information and entertainment services over America's most advanced fiber-optic network, and delivers integrated business solutions to customers in more than 150 countries, including all of the Fortune 500. A Dow 30 company, Verizon employs a diverse workforce of nearly 196,000 and last year generated consolidated revenues of $106.6 billion. For more information, visit *www.verizon.com*.

VERIZON'S ONLINE NEWS CENTER: Verizon news releases, executive speeches and biographies, media contacts, high-quality video and images, and other information are available at Verizon's News Center on the World Wide Web at *www.verizon.com/news*. To receive news releases by email, visit the News Center and register for customized automatic delivery of Verizon news releases.

SOURCE Verizon

Contacts: Brianna Carroll Boyle, +1-703-859-4251, brianna.boyle@verizon.com; or Nilesh Pritam, +65 6248 6599, nilesh.pritam@sg.verizonbusiness.com, or Clare Ward, +44 118 905 3501, clare.ward@uk.verizonbusiness.com
Countries: United States
Industries: Telecommunications, Multimedia, Internet & Wireless Technology

Languages: English
Primary Identifiers: VZ-US
Related Identifiers: VZ-US