90 percent of industries experience patient data breaches, finds Verizon 2015 Protected Health Information Data Breach Report
Thursday, December 17, 2015 01:00:00 PM (GMT)

BASKING RIDGE, N.J., Dec. 17, 2015 /PRNewswire/ -- Stolen medical information is a much more widespread issue than previously thought, affecting 18 out of 20 industries examined, according to the just released Verizon 2015 Protected Health Information Data Breach Report. Yet, most organizations outside of the healthcare sector do not realize they even hold this type of data. Common sources of protected health information are employee records (including workers' compensation claims) or information for wellness programs and are generally not well protected.

These findings are part of a first-time report from Verizon's Data Breach Investigations Report (DBIR) team that provides a detailed analysis of confirmed PHI* breaches involving more than 392 million records and 1,931 incidents across 25 countries.

"Many organizations are not doing enough to protect this highly sensitive and confidential data," said Suzanne Widup, senior analyst and lead author for the Verizon Enterprise Solutions report. "This can lead to significant consequences impacting an individual and their family and increasing healthcare costs for governments, organizations and individuals. Protected health information is highly coveted by today's cybercriminals."

According to recent studies called out in the report, people are withholding information – sometimes critical information – from their healthcare providers because they are concerned that there could be a data breach.

"Healthcare organizations need to realize that patients trust them with their data and if that trust is broken, the implications can be huge," Widup added.

For example, the report points out, an unwillingness to fully disclose information could delay a diagnosis of a communicable disease. This is especially true if the disease has an attached social stigma.

How PHI Breaches Differ From Other Types of Breaches
PHI breaches stand out from prior DBIR data sets in a number of ways. One area of difference is who is carrying out the attacks. In PHI breaches, the number of external and internal actors is nearly equal with just 5 percentage points difference, meaning there is a lot of insider misuse.

According to the report's findings, medical record data is often taken with malicious intent; however, it is frequently the personable identifiable information (PII), like credit card and social security numbers, that attackers are really after in order to facilitate financial crimes and tax fraud.

Differences are also evident in how the breach occurs. The primary action of attack is theft of lost portable devices (laptop, tablets, thumb drives), followed by error which can simply be sending a medical report to the wrong recipient or losing a laptop. Third is misuse that can result from an employee that abuses his/her access to the information. These three actions make up 86 percent of all breaches of PHI data.

In addition, the time to discovery most frequently falls into the months and sometimes years category. For those incidents taking years to discover, they were three times more likely to be caused by an insider abusing their LAN access privileges and twice as likely to be targeting a server, particularly a database.

What Can Be Done About PHI Data Breaches
While detailed health records make it easier for criminals to engage in both identity theft and medical billing fraud, the media and industry researchers continue to shine a light on the loss of highly personal data in order to bring much needed attention to this issue.

Sadly nearly half of the population of the Unites States has been impacted by breaches of PHI since 2009, finds the report. Furthermore, the FBI issued a warning to healthcare providers in early 2015 stating that "the healthcare" industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is "likely."

To help address this issue, Verizon offers insights and recommendations in the report on how to best protect

data in addition to illuminating the fact that PHI data is contained in many more places than organizations realize.

The full report can be found here: http://news.verizonenterprise.com/2015/12/2015-protected-health-report-info.

Verizon 2015 Protected Health Information Data Breach Report
As part of Verizon's Data Breach Investigations Report (DBIR) series, the PHI Data Breach Report is based on actual casework and is the most comprehensive report of its kind in the industry. This report analyzes protected health information data breaches with a focus on the healthcare industry including ambulatory healthcare services, hospitals, nursing and residential care; and social assistance across North America, Europe and the Asia-Pacific region.

The report contains incidents contributed by the following organizations: ACE Group; the CERT Insider Threat Center; CrowdStrike, Deloitte; the Dutch National High Tech Crime Unit, G-C Partners, LLP; Kaspersky Lab; Mishcon de Reya; NetDiligence; and the U.S. Secret Service. The study also includes the U.S. Health and Human Services incident database (for incidents affecting at least 500 individuals) and a significant number of incidents from the U.S. Veteran's Administration as reported to Congress (from the VERIS Community Database project).

Verizon's DBIR series is aimed at helping organizations across all sectors understand the importance of identifying and protecting this information before a data breach occurs.

*For this report, PHI is defined as personally identifiable health information on an individual covered by one of the state, federal or international data breach disclosure laws.

Visit the Verizon Enterprise Solutions' Products and Services Center to learn how Verizon can help secure your business with the latest technologies and solutions backed by our unparalleled expertise and visibility into the global security landscape.

Verizon Communications Inc. (NYSE, Nasdaq: VZ) employs a diverse workforce of 177,900 and generated more than $127 billion in 2014 revenues. Verizon Wireless operates America's most reliable wireless network, with 110.8 million retail connections nationwide. Headquartered in New York, Verizon also provides communications and entertainment services over America's most advanced fiber-optic network, and delivers integrated business solutions to customers worldwide. For more information, visit www.verizon.com/news/.

Verizon Enterprise Online News Room: News releases, blog posts, media contacts and other information are available at *Verizon Enterprise Solutions News & Insights* *(news.verizonenterprise.com)*. News from Verizon Enterprise Solutions is also available through an RSS feed at http://www.verizonenterprise.com/rss-options/.

To view the original version on PR Newswire, visit: http://www.prnewswire.com/news-releases/90-percent-of-industries-experience-patient-data-breaches-finds-verizon-2015-protected-health-information-data-breach-report-300194378.html

SOURCE Verizon

Countries: United States
Industries: Computer Electronics, Hardware & Software, Health Care, High Tech Security, Medicine & Pharmaceuticals
Languages: English
Primary Identifiers: VZ-US
Related Identifiers: VZ-US