Verizon Releases Industry-by-Industry Snapshots of Cybercrime, Based on the Data Breach Investigations Report Series
Wednesday, October 24, 2012 04:01:00 AM (GMT)

Data Provide In-Depth View of Financial Services
Health Care
Retail
Hospitality Sectors and Intellectual Property Theft

BASKING RIDGE, N.J., Oct. 24, 2012 /PRNewswire/ -- Verizon on Wednesday (Oct. 24) released a series of industry-by-industry snapshots of cybercrime, based on the "Verizon 2012 and 2011 Data Breach Investigations Reports." The snapshots, aimed at helping organizations better understand the anatomy of a data breach and how to best provide protection, offer an in-depth view of the financial services, health care, retail and hospitality sectors.

In addition, a fifth snapshot examines intellectual property theft, which has become increasingly difficult to protect against across a range of industries.

"Understanding what happens when a data breach occurs is critical to proactive prevention," said Wade Baker, Verizon managing principal, RISK team. "Through our more targeted analysis, we are hoping to provide answers to businesses around the globe that want to protect not only their data but their reputation."

Key Findings Across Industries

The new data provide the following key findings:

Financial and Insurance

- The financial services industry faces some unique challenges with regard to information protection. The industry's status as a high-value target means it attracts significantly more directed and tenacious criminal attention.
- Overall breaches in this sector were primarily about the money, whether targeting it directly (by accessing internal accounts and applications) or indirectly (through downstream fraud). Many of the attacks are targeted against ATMs, Web applications and employees.
- Areas for improved security include better protection of ATMs, careful monitoring of login credentials, secure application development, and training and awareness among employees.

Health Care

- Most of the breaches within the health care sector fell into the small to medium business category (one to 100 employees), and outpatient care facilities such as medical and dental offices comprised the bulk of these.
- Attacks were almost entirely the work of financially motivated organized criminal groups, which typically attack smaller, low-risk targets to obtain personal and payment data for various fraud schemes.
- Most attacks involved hacking and malware and often focused on point of sale (POS) systems. However, the health care industry also needs to protect medical devices and electronic health records.
- The majority of breaches can be prevented with some small and relatively easy steps, including change in administrative passwords on all POS systems; implementing a firewall; avoiding using POS systems to browse the Web; and making certain the POS is a PCI DSS (Payment Card Industry Data Security Standard) compliant application.

Retail

- The retail industry continues to be plagued with a multitude of data breaches, much of it committed by financially motivated criminal groups that gain access through POS systems that are used to conduct daily business activities. The criminals exploit weak, guessable or default credentials via third-party remote access services.

- The most vulnerable are franchises and other small and medium-size businesses, which often lack in-house resources and expertise to manage their own security. Consequently, these businesses often rely on ill-equipped third-party vendors, which often fail to provide adequate protection; or the businesses use an out-of-the-box solution, without adequately investigating whether the solution will meet their security needs.
- In many cases, employees are involved in the breaches, either wittingly or unwittingly. It is not uncommon for an employee to click on a malicious email attachment or visit a questionable site on a company desktop, infecting the system with malware and enabling an attacker to gain access to other devices within the network.

Accommodations and Food Services

- This industry has been particularly vulnerable to data breaches, and for the past two years has had more breaches than any other industry.
- The POS systems, which are needed to process payment transactions, have proven to be easy targets for organized criminal groups.
- This industry, more so than any other, needs to emphasize preventive actions.

Intellectual Property (IP) Theft

- Overall, finding and identifying the work of IP theft is highly difficult and specialized. Many of these breaches go undetected until long after the damage has been done, and it often takes quite a while to successfully contain the breach. IP attacks often include collusion between insiders and outsiders. Regular employees accounted for the largest percentage (two-thirds) of insiders. Outsiders often acted directly and maliciously, but also regularly solicited and aided insiders.
- Most of the thefts are carried out by determined adversaries who target IP as a shortcut to attaining some manner of strategic, financial, technological or related advantage. The attackers generally mix and match their methods until they find a successful combination. Many of these combinations are multiphased and multifaceted.
- With IP attacks, no single solution can guarantee protection. A common-sense, evidence-based approach is the best defense.

Verizon 2012 Data Breach Investigations Report

The DBIR is now in its fifth year of publication, and this year's edition, released in March, analyzed 855 data breaches involving more than 174 million compromised records – the second-highest data loss that the Verizon RISK (Research Investigations Solutions Knowledge) team has seen since it began collecting data in 2004. Verizon was joined by five organizations that contributed data to this year's report: the United States Secret Service, the Dutch National High Tech Crime Unit, the Australian Federal Police, the Irish Reporting & Information Security Service and the Police Central e-Crime Unit of the London Metropolitan Police.

For the first time in 2012, the report was issued in multiple languages in addition to English: French, Italian, Japanese, German, Portuguese and Spanish. In addition, the 2012 report also is produced as an iBook.

Verizon, through its Terremark subsidiary, helps organizations protect their core asset: data. The company does this through a robust suite of security services -- including governance, risk and compliance solutions; identity and access management solutions; investigative response; data protection and threat management services; and vulnerability management services -- delivered in the cloud or on premises.

For more information on Verizon Security Services, click here. For ongoing security insight and analysis from some of the world's most distinguished security researchers, read the Verizon Security Blog.

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 nearly 96 million retail customers 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 with $111 billion in 2011 revenues, Verizon employs a diverse workforce of 184,500. 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: Janet Brumfield, +1-614-723-1060, janet.brumfield@verizon.com, or Nilesh Pritam, +65-6248-6599, nilesh.pritam@sg.verizonbusiness.com, or Maria Rodriguez, +1-305-961-3181, mrodriguez@terremark.com, or Clare Ward, +44-118-905-3501, clare.ward@uk.verizonbusiness.com
Countries: United States
Industries: Retail, Telecommunications, Banking & Financial Services, Computer Electronics, Hardware & Software, Health Care, High Tech Security, Travel & Tourism
Languages: English
Primary Identifiers: VZ-US
Related Identifiers: VZ-US