Constant Connectivity, Proliferation of Mobile Devices and Applications Will Create More Security Concerns in 2012
Thursday, December 15, 2011 12:00:00 PM (GMT)

Verizon's ICSA Labs Division Identifies Key Security Threats Aimed at Businesses Consumers in Coming Year

MECHANICSBURG, Pa., Dec. 15, 2011 /PRNewswire/ -- The widespread adoption of mobile devices, proliferation of applications and growth of cloud computing are helping accelerate business innovation and social benefits. However, today's always-on world brings with it a new and ever-changing set of security challenges.

According to the Verizon "2011 Data Breach Investigations Report," the number of data attacks has tripled in the past five years, making the need to balance security with risk an even greater priority for businesses and consumers.

With this trend in mind, Verizon's ICSA Labs division recommends that businesses and consumers guard against the following 13 security threats in 2012:

1. **Mobile Malware Is on the Rise.** Malware targeting mobile devices will continue to increase, and enterprises will wrestle with how to protect users. Obvious targets will be smartphones and tablets, with the hardest hit likely to be Android-based devices, given that operating system's large market share and open innovation platform. All mobile platforms will experience an increase in mobile attacks.
2. **Criminals Target and Infect App Stores.** Infected applications, rather than browser-based downloads, will be the main sources of attack. Because they are not policed well, unauthorized application stores will be the predominant source of mobile malware. Cybercriminals will post their infected applications here to attempt to lure trusting users into downloading rogue applications. Cybercriminals also will find ways to get their applications posted into authorized application stores. And infections can easily spread beyond the smartphone and into a corporate network, upping the ante on risk.
3. **Application Scoring Systems Will Be Developed and Implemented.** To reassure users, organizations will want to have their application source code reviewed by third parties. Similarly, organizations will want to be sure that the applications approved for use on workers' devices meet a certain standard. It is anticipated that the industry will develop a scoring system that helps ensure that users only download appropriate, corporate-sanctioned applications to business devices.
4. **Emergence of Bank-Friendly Applications With Built-In Security.** Mobile devices will increasingly be used to view banking information, transfer money, donate to charities, and make payments for goods and services, presenting an opportunity for cybercriminals, who will find ways to circumvent protections. To help ensure the security of online banking, the banking industry is likely to begin to offer applications that have strong, built-in security layers.
5. **Hyper-connectivity Leads to Growing Identity and Privacy Challenges.** In today's business environment, more users need to legitimately access more data from more places. This requires the protection of data at every access point by using stronger credentials, deploying more secure, partner-accessible systems, and improving log management and analysis. Compounding the issue are a new age of cross-platform malicious code, aimed at sabotage, and mounting concerns about privacy. Enterprises will no longer be able to ignore this problem in 2012, and will have to make some hard choices.
6. **New Risks Accompany Move to Digitized Health Records.** In the U.S., health care reform and stimulus funding will continue to accelerate the adoption of electronic health records and related technologies throughout the industry. The American Recovery and Reinvestment Act calls for all medical records to be electronic by 2014, meaning that much work must be done in 2012 and 2013 to prepare. New devices will be introduced that send sensitive information beyond the traditional boundaries of health care providers, and more and more health care providers are using mobile devices. Along with the need to secure newly implemented EHR systems, securing mobile devices and managing mobile clinical applications will continue to be an ever-increasing focus in the health care industry.
7. **Mobile and Medical Devices Will Begin to Merge.** Mobile devices and health care apps will

proliferate, making it easier, for example, to transform a smartphone into a heart monitor or diabetes tester. As a result, some experts believe that industry health care groups will declare mobile devices to be medical devices in order to control and regulate them. As interoperability standards mature, more mobile devices and traditional medical devices will become nodes on an organization's network. These devices also will share data with other devices and users and, as a result, be susceptible to the same threats and vulnerabilities that computers and other network-attached peripherals, such as printers and faxes, are susceptible to today.

8. **Smart Grid Security Standards Will Keep Evolving.** In the U.S., public utility commissions, along with the National Institute of Standards and Technology, will continue to develop smart-grid standards. State PUCs will begin to agree on a standard in the coming year. The government will increasingly require utilities to demonstrate that their smart grid and advanced metering infrastructure solutions protect not only the privacy of consumers and consumer usage data but also the security of the AMI infrastructure. At some point, a single federal framework will supersede state regulations and requirements.
9. **New Concerns Will Surface About IPv6.** The federal government is still struggling with the rollout of IPv6-enabled devices as organizations migrate from IPv4. This will be an ongoing concern, and IPv6 specific vulnerabilities and threats will continue to cause trouble during 2012. In addition, the other two fundamental mechanisms of the Internet -- Border Gateway Protocol and Domain Name System – also now offer a next-generation version. In 2012, many will start migrating to these newer versions, generating a new round of vulnerabilities and exploits.
10. **Social-Engineering Threats Resurface.** More targeted spear-phishing -- an email-fraud attempt that targets a specific organization, seeking unauthorized access to confidential data – will be the major social-engineering threat of 2012. Efforts to educate user communities about safe computing practices will continue to be a challenge as the user base of smart devices increases dramatically. Social networking sites will continue to implement protection for users from malware, spam and phishing, but sophisticated threats will continue to seduce users to visit a rogue Website or reveal personally identifiable information online.
11. **Security Certification Programs Will Increase in Popularity.** Certifications will continue to increase, especially as the government accelerates IT mandates for its agencies in the areas of cloud and identity; and in turn, the private sector will follow suit. Internet threats will continue to affect business, government and user confidence and wreak havoc on computing devices in the office and at home. The challenge for all testing bodies will be to stay ahead of the ever-changing threat landscape and to evolve testing accordingly. Some testing bodies may suggest certifying the security of companies as a whole, not just their products or services, as a way to build trust online.
12. **'Big Data' Will Get Bigger, and so Will Security Needs.** "Big data" -- large data sets that can now be managed with the right tools -- will be popular in 2012 as more companies derive greater value through analytics. Companies will use the data to create new business opportunities while empowering evidence-based decision making for greater success. However, companies will need to secure this data in order to achieve the gains they seek.
13. **Safeguarding Online Identities Will no Longer be Optional.** With the rampant growth of online identity theft, consumers, businesses and government agencies are seeking ways to better protect their identities. These groups will look to the private sector to provide a cost-effective solution that helps to safeguard their identities and create greater online trust.

"The proliferation of Internet connectivity, mobile devices and Web applications are helping to enrich lives and advance global business opportunity in new meaningful ways," said Roger Thompson, emerging threats researcher, ICSA Labs. "But in this new era of hyper-connectivity, which is compounded by the blurring of lines between our professional and personal lives, it's everyone's responsibility -- whether as a business user or a consumer -- to safeguard our online activities and interact with technology responsibly to protect our assets, identity and privacy."

About ICSA Labs
ICSA Labs, an independent division of Verizon, offers third-party testing and certification of security and health IT products, as well as network-connected devices, to measure product compliance, reliability and performance for many of the world's top security vendors. ICSA Labs is an ISO/IEC 17025 accredited and 9001 registered organization. Visit *http://www.icsalabs.com* and *http://www.icsalabs.com/blogs* for more information.

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 107 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 with $106.6 billion in 2010 revenues, Verizon employs a diverse workforce of more than 195,000. 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 Brianna Boyle, +1-702-859-4251, Brianna.Boyle@verizon.com
Countries: United States
Industries: Telecommunications, Computer Electronics, Hardware & Software, Consumer Electronics, Entertainment & Leisure, High Tech Security, Multimedia, Internet & Wireless Technology
Languages: English
Primary Identifiers: VZ-US
Related Identifiers: VZ-US