Risking Exposure
Wednesday, September 05, 2012 09:16:00 AM (GMT)

Data Beaches Continue to Frustrate Companies and Consumers

By Wendy Bowman-Littler

LAGUNA BEACH, Calif., Sept. 5, 2012 (GLOBE NEWSWIRE) -- You've heard the terrifying stories about consumers' sensitive personal and financial data such as social security, bank account and drivers license numbers being lost, stolen or exposed through online break-ins at companies and organizations. Maybe you've even been notified that your information has been compromised by one of these security breaches and have been left with the daunting task of having to deal with harassing debt collectors, police, credit bureaus and government agencies on your own—just to recover or repair your good standing.

Numerous data breaches occur frequently in the US, from the recent Yahoo security breach that exposed 450,000 usernames and passwords from a site on the huge web portal, to the hijacking of credit card information belonging to hundreds of thousands of Wyndham Worldwide Corp. customers, to the online theft of 6.5 million user passwords from the popular social networking site LinkedIn.

At the end of July, 254 breaches were reported for the first seven months of 2012, compared with 250 during the same period in 2011, according to the San Diego-based Identity Theft Resource Center (ITRC), which has been tracking breaches since 2005.

The ITRC uses information from attorney general websites and media reports to compile its reports, but many breaches still go unreported or under-reported, says ITRC program director Karen Barney. "We know that the breaches we have on our list is not a complete list," she says. "Breaches will continue to be under-reported, because companies don't want to suffer the costs they may face if they do come out."

As the global leader in cyberintelligence, Pennsylvania-based Tiversa sees unreported data breaches of all sizes on a daily basis. "Not only does data get inadvertently exposed, but Tiversa continues to track viral replication of data over time, from the perspective of file spread itself as well as with cybercriminals worldwide that actively acquire and harvest it," says Bob Boback, CEO of Tiversa, cyberintelligence experts, as well as the industry leader in peer-to-peer (P2P) technology that processes as many as 1.8 billion P2P searches per day.

Many states including Maine, Maryland, New York, New Hampshire, North Carolina and Vermont don't even require organizations to report breaches to a centralized database. This might change soon, however, if the recently introduced Data Security and Breach Notification Act of 2012 is passed, leading to the adoption of a national standard for data breach notification. Consumers in all states also would be notified of a data breach that could impact them.

While hacking accounts for almost 30 percent of the reported data breaches so far in 2012, according to the ITRC, no one should underestimate the losses taking place through peer-to-peer (P2P) file-sharing software and networks, which at any point in time have more than 20 million users worldwide. Emerging on the scene in the late 1990s with the introduction of the online music service Napster, P2P networks have since offered a gateway for users worldwide to share digital content—most notably music, movies and software—with other users free of charge.

"P2P file-sharing programs index hard-drives and business networks, allowing anyone with the basic understanding of how these programs work to download personnel records, tax returns and confidential company documents," Boback says. As P2P has continued to grow in size and popularity during the years, its use has resulted in the loss of millions of highly sensitive files that have affected consumers, large and small businesses, the US government, nation's financial infrastructure, national security and even military.

In addition, many of the measures companies take to prevent data loss through P2P networks, such as firewalls, ID management and monitoring of the World Wide Web, often are ineffective against P2P files sharing disclosures, according to Dr. Larry Ponemon, chairman and founder of the Michigan-based Ponemon Institute, which conducts independent research on privacy, data protection and information security policy.

"P2P shouldn't be used anywhere there is personal information," says Nikki Junke, ITRC's social media coordinator and victim adviser. "People shouldn't be able to do that at work or on any devices which have access to any of that info or any infrastructure. Companies need to make sure they have that stated in their policies and procedures. With P2P you're opening up a doorway and not just taking things in, you're opening up your system so things can be taken out. You're opening yourself up for a cyber attack or letting out personal info about the company that would help facilitate an attack."

P2P file sharing plays a larger role in corporate data losses than most organizations will admit, mostly because organizations don't have a firm understanding of what employees have on their laptops or desktops, Boback says.

Testifying before Congress in 2009, Boback shared that Tiversa conducted research involving more than 30,000 consumers and found that 86.7 percent of the individuals whose information was found on the P2P networks had been breached by a third party. Many of these individual's information was exposed by their doctors, lawyers, hospitals, accountants, employers, banks and financial institutions, and payroll companies, meaning that less than 15 percent came through hacking or other losses.

"Some of the best methods companies can institute to try and protect themselves from all types of data breaches include adhering to the red-flag rules, screening employees and having a solid IT security system in place," says Carol Fredericks, a Tallahassee, Fla.-based instructor for the FBI-LEEDA program on identity theft. "Organizations also should adopt more proactive and comprehensive cyber protection that goes beyond traditional measures."

The entire idea behind stealing personal data is to make money, including completing purchases with credit card numbers, opening new lines of credit with social security numbers and birth dates, draining money from a bank account, obtaining a job or medical treatment, filing a fake tax return to get the refund and more. Consumers might only know they have been affected by a data breach in the form of an email or letter from the source of the breach, from something they see or hear on the news, or when their bank or credit card statement, insurance or credit report arrives. By then, it's usually too late and criminals have had plenty of time to not only use the information themselves but to sell and share it worldwide.

That's where the work on the consumer's behalf begins. "We find undisclosed losses of data every day and work with the organizations to resolve the issue if the data has been shared globally," Boback says. "Our goal is to detect and remediate data breaches quickly, before cyber criminals have an opportunity to acquire the sensitive data that has been exposed."

Correcting a problems stemming from a data breach has occurred can be very time-consuming and frustrating for consumers. Often informed long after the breach has occurred, by the organization that suffered the breach requires its customers to contact the fraud department of the company where the breach occurred, as well as the three major credit reporting agencies to place a fraud alert on their credit reports and to order a complimentary credit report. Breach victims are also asked to file a police report that includes documented proof, and to send a copy of that report and all of the supporting documents to any company that lists a fraudulent account on their credit report.

Some of the best pre-emptive moves include asking your employer, accountant, hospital and attorney what they are doing to secure your information from P2P file-sharing networks; understanding the risks associated with file-sharing applications and general Internet risks; and being careful of what type of information you share and whom you share it with.

"When dealing with data-holding organizations, consumers shouldn't assume they would be the first to know about any data breach issue or would be actively working to combat it," Boback says. "From my experience, a small percentage of data-holding organizations have the proper plan in place to handle a data breach situation, including any system in place to monitor for these problems. It's another reason why consumers should always ask about the protection of personal information before just handing it over."

Wendy Bowman-Littler is a Laguna Beach, Calif.-based freelance journalist with 25-plus years experience in writing and editing.

http://www.cisionwire.com/tiversa/r/risking-exposure,c9293069

The following files are available for download:

wkr0006.pdf	PDF

Primary Identifiers: TNL-US
Related Identifiers: TNL-US
Subjects: Product / Services Announcement