

Learn about the top insurance risks manufacturers face today. Sign up for our **FREE** Virtual Consulting Tool.



Get free access



 Printed from BusinessInsurance.com

Sony grapples with data loss

Hacker attacks offer lessons for companies

Posted On: May. 08, 2011 6:00 AM CST

Judy Greenwald (mailto:jgreenwald@BusinessInsurance.com)



More than 100 million customer accounts were accessed in recent Sony PlayStation Network data breaches.

TOKYO—Sony Corp.'s recent data breaches, in which hackers accessed more than 100 million consumer accounts, offer several lessons for companies, experts say.

Among them are the importance of firms frequently monitoring their systems' security, collecting and retaining as little personal information as possible, encrypting what is kept and obtaining cyber insurance, experts say.

Sony shut down its PlayStation Network multiplayer game network on April 20 and disclosed that hackers had stolen names, birth dates and possibly credit card numbers from 77 million accounts on the network.

Then last week, the Tokyo-based firm disclosed that hackers also breached security on a second online service, which provides multiplayer games for personal computers, and gained access to personal information of 24.6 million customers, as well as information from an outdated 2007 database.

In a letter sent last week to the House Subcommittee on Commerce, Manufacturing and Trade, Sony Chairman Kazuo businessinsurance.com/apps/.../article?...

Hirai said no major credit card companies had reported fraudulent activity as a result of the attacks.

Mr. Hirai said steps Sony has taken in response include additional automated software monitoring, enhanced levels of data protection and encryption, enhanced ability to detect software intrusions, implementation of additional firewalls, a plan to move to a new data center with enhanced security and the appointment of a chief information security officer.

At least two lawsuits seeking class action status related to the data breaches have been filed in San Francisco and Toronto. Both accuse Sony of negligence for failing to prevent the attacks and taking too long to inform its clients.

“In many cases, if you had a security incident of this magnitude, it's fairly difficult afterwards to effectively establish that you did everything that a reasonable person would have done under the circumstances” to avoid it, said Robert J. Scott, managing partner with law firm Scott & Scott L.L.P. in Dallas.

The defense of these lawsuits “is going to be very expensive,” Mr. Scott said.

However, observers also said it is difficult for plaintiffs to prevail in such cases unless they can prove actual damages.

Sony has said it has a variety of types of insurance that cover hacking-related damages, and certain insurers have been put on notice of potential claims. A Sony spokesman declined to release additional information.

Observers said while there is no guarantee of security on the Internet, there are steps companies can take to limit their potential liability (see box).

Company executives “need to understand information security is not a commodity, but an ongoing process” that “goes to the very heart of the continuity and value of the enterprise,” said Gene Spafford, director of the Center for Education Research Information Assurance and Security in West Lafayette, Ind.

Mr. Spafford said firms should have appropriately trained personnel who are given the appropriate resources and the authority to take necessary action based on the risk.

“They should regularly monitor and observe what's going on” and have a plan in place to allow a quick response when something goes wrong, he said.

Experts recommend frequent testing of companies' security systems.

Peter S. Vogel, a partner with law firm Gardere Wynne Sewell L.L.P. in Dallas, said it behooves companies “to have their systems tested on a regular basis by third parties to discover where they are vulnerable, to improve security.”

“This is such a fast-moving area...that you can't just put (a security system) in place and then forget about it. It needs constant monitoring and updating,” said Richard J. Bortnick, a member of Cozen O'Connor P.C. in West Conshohocken, Pa. “It's like a game of cat and mouse because as the security systems become more secure, the cyber criminals become more sophisticated...and there's no panacea.”

“The best you can hope for is to keep out” at least the casual hacker, said Shari Claire Lewis, a partner with Rivkin Radler L.L.P. in Uniondale, N.Y.

It helps to limit the information that is obtained and stored, experts said.

Referring to the outdated 2007 database that was hacked, Mr. Spafford said, “So, the question is, why was that kept?”

For information that is necessary, one obvious step is to encrypt all the data, said E. Leonard Rubin, of counsel to law firm Querry & Harrow Ltd. in Chicago.

Another is to make sure information can be disseminated only on a need-to-know basis, said Mr. Rubin. "That's something that companies are often careless about," he said.

Observers say under federal law and most state laws, customers must be informed when personally identifiable information has been breached.

It took Sony several days to inform clients of the breach. In his letter to the House subcommittee, Mr. Hirai said Sony was concerned that releasing partial or tentative information would cause confusion.

Mr. Bortnick, said, however, "There comes a point where you have to stop waiting for information and you've got to make a decision....Inaction is no action."

Observers said cyber insurance can help companies with the costs associated with hacking incidents, including the expense of notifying clients of the breach.

Towers Watson & Co.'s 2011 risk and finance manager survey found, however, that 73% of companies surveyed have not purchased network liability insurance coverage, with one-quarter of those saying either they were not overly concerned about the risk, or were unable to understand the value of information or the cost of a breach.

Jeanne Oronzio, senior technical specialist at Philadelphia-based brokerage and consulting firm The Graham Co., said cyber policies, which are manuscripted, are offered by all the major insurance markets, with premiums varying based on the coverage.
