INSURANCE JOURNAL

View this article online:
http://www.insurancejournal.com/news/national/2011/08/02/209108.htm

Leisure Industry Tempting Target for Cyber Pirates: Willis

The hospitality industry is a tempting target for an increasing number of cyber attacks.

The vast quantities of personal, identifiable information collected by the leisure and hospitality industry puts the industry at greater risk for cyber attacks, according to Willis Group Holdings. Willis' Cyber Risk Unit reports that cyber-related insurance claims have spiked by 56 percent over the past year alone, with an increasing proportion of victims in the hospitality industry.

Citing a recent survey, the Willis Summer 2011 Leisure Newsletter warns that hotels, resorts, tour companies, and other leisure and entertainment providers are increasingly vulnerable to hackers seeking to steal personal information. The Newsletter highlights the major risks posed by the deluge of personal data and advises companies how to protect themselves against cyber crime.

The Ponemon Institute, a U.S.-based information technology think tank, estimates that the costs of recovering from a cyber attack – including costs associated with notifying customers and implementing credit monitoring software to help ensure victims' credit records are not compromised by the misuse of stolen data – typically range anywhere between $100,000 to $1 million. However, Willis warns that some of the largest breaches can cost in excess of $100 million. More stringent data protection legislation coming into force will only further increase companies' financial exposure to cyber crime, both in terms of liabilities to banks and individuals, and reputational damage.

The main culprits of data breaches include rogue employees, malicious attacks, and innocent

mistakes made by outsourcing firms employed to manage customer data.

"Hackers are getting ever more sophisticated, penetrating firewalls to drain corporate databases of their customers' personal details, including credit card numbers when not encrypted, medical histories and other personal information," said Laurie Fraser, global markets leisure practice leader for Willis. "This year has already seen at least three high profile cyber crime cases where security breaches triggered public outrage and panic over identity theft and fraud. The incidents badly bruised the reputations of popular consumer brands, as well as exposed firms to a host of increased costs as well as potential liabilities."

Businesses such as those in the hospitality industry hold substantial volumes of personal, identifiable data are irresistible to web-based pirates, says Jeremy Smith, practice leader of Willis' London cyber team.

In response, Smith said that cyber liability insurance, which has existed for about 10 years, is evolving to reflect the current environment, helping companies to transfer the risks and costs of data loss and cyber piracy.

"Willis is working closely with the insurance industry to stress test existing policies' ability to address the nature of cyber crime and develop exclusive wordings that assist in the transfer of these risks," he said.

Recent advances in coverage include the introduction of identity theft solutions and Payment Card Industry fines coverage, which helps to protect companies from penalties linked to the mismanagement of credit card data, Smith said.

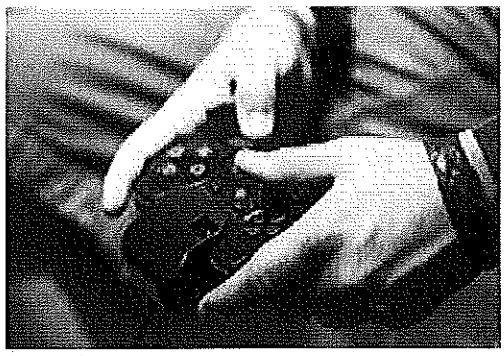
Source: Willis Group Holdings

More from Insurance Journal
Today's Insurance Headlines | Most Popular | National News

» Print

Sony PlayStation suffers massive data breach

Tue, Apr 26 2011



By Liana B. Baker and Jim Finkle

NEW YORK/BOSTON (Reuters) - Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins.

Sony learned that user information had been stolen from its PlayStation Network seven days ago, prompting it to shut down the network immediately. But Sony did not tell the public until Tuesday.

The electronics conglomerate is the latest Japanese company to come under fire for not disclosing bad news quickly. Tokyo Electric Power Co was criticized for how it handled the nuclear crisis after the March earthquake. Last year, Toyota Motor Corp was slammed for being less than forthright about problems surrounding its massive vehicle recall.

The "illegal and unauthorized person" obtained people's names, addresses, email address, birth dates, usernames, passwords, logins, security questions and more, Sony said on its U.S. PlayStation blog on Tuesday.

The shutdown of the PlayStation Network seven days ago prevented owners of Sony's video game console from buying and downloading games, as well as playing with rivals over the Internet.

Alan Paller, research director of the SANS Institute, said the breach may be the largest theft of identity data information on record.

The breach is a major setback for the Japanese electronics maker. Although video game hardware and software sales have declined globally, the PlayStation franchise has been a steady seller and remains a flagship product for Sony.

Children with accounts established by their parents also might have had their data exposed, Sony said.

Sony said it saw no evidence credit card numbers were stolen, but warned users it could not rule out the possibility.

"Out of an abundance of caution, we are advising you that your credit card number (excluding security code) and expiration date may have been obtained," Sony said.

Analysts said that, while Sony has notified its customers of the breach, it still has not provided information on how user data might have been compromised.

"This is a huge data breach," said Wedbush Securities analyst Michael Pachter, who estimated Sony generates $500 million in annual revenue from the service. "The bigger issue with Sony is how will the hacker use the info that has been illegally obtained?"

Sony said it has hired an "outside recognized security firm" to investigate.

The company said user account information for the PlayStation Network and its Qriocity service users was compromised between April 17 and April 19.

Paller said Sony probably did not pay enough attention to security when it was developing the software that runs its network. In the rush to get out innovative new products, security can sometimes take a back seat.

"They have to innovate rapidly. That's the business model," Paller said. "New software has errors in it. So they expose code with errors in it to large numbers of people, which is a catastrophe in the making."

He suspected the hackers entered the network by taking over the PC of a system administrator, who had rights to access sensitive information about Sony's customers. They likely did that by sending the administrator an email message that contained a piece of malicious software that got downloaded onto his or her PC.

Hackers have stolen personal data in the past from large companies. In 2009, Albert Gonzalez pleaded guilty to stealing tens of millions of payment card numbers by breaking into corporate computer systems at companies such as 7-Eleven Inc and Target Co.

Sony said its users could place fraud alerts on their credit card accounts through three U.S. credit card bureaus, which it recommended in its statement.

Sony, a unit of Sony Corp, said it could restore some of the network's services within a week.

The company declined to comment on whether it was working with law enforcement or other parties in its investigation.

The online network was launched in the autumn of 2006 and offers games, music and movies to people with PlayStation consoles. It had 77 million registered users as of March 20, a Sony spokesman said.

(Reporting by Liana B. Baker; additional reporting by Jim Finkle in Boston; editing by Robert MacMillan, Kenneth Li, Bernard Orr and Andre Grenon)

Claims Journal - Property Casualty Industry News

View this article online: http://www.claimsjournal.com/news/national/2011/07/22/188564.htm

Sony Insurer Sues to Deny Data Breach Coverage

By Ben Berkowitz | July 22, 2011

- Article
- Comments

One of Sony Corp's insurers has asked a court to declare that it does not have to pay to defend the media and electronics conglomerate from mounting legal claims related to a massive data breach earlier this year.

The dispute comes as demand soars for "cyberinsurance," with companies seeking to protect themselves against customer claims and associated costs for data and identity theft.

How to write such policies has become a huge subject of debate in the insurance industry.

Zurich American Insurance Co asked a New York state court in documents filed late on Wednesday to rule it does not have to defend or indemnify Sony against any claims "asserted in the class-action lawsuits, miscellaneous claims, or potential future actions instituted by any state attorney general."

A Sony spokesman in Tokyo said his company does not comment on pending litigation.

Zurich American, a unit of Zurich Financial Services , also sued units of Mitsui Sumitomo Insurance, AIG and ACE Ltd , asking the court to clarify their responsibilities under various insurance policies they had written for Sony.

"Zurich doesn't think there's coverage, but to the extent there may be a duty to defend it wants to make sure all of the insurers with a potential duty to defend are contributing," said Richard Bortnick, an attorney at Cozen O'Connor and publisher of the digital law blog CyberInquirer.

Bortnick, who is not involved in the case, said that while Sony may be able to claim there was property damage as a result of the data breach, Zurich is likely to argue that the sort of general liability insurance it wrote for Sony was never intended to cover digital attacks.

AIG declined to comment, and Mitsui Sumitomo could not immediately be reached.

In April, hackers accessed personal data for more than 100 million users of Sony's online video games. Sony has said it could not rule out that some 12.3 million credit card numbers had been obtained during the hacking.

In May, Sony said it was looking to its insurers to help pay for its massive data breach.

Sony has said it expects the hacking to drag down operating profit by 14 billion yen ($178 million) in the current financial year, including costs for boosting security measures. The company said the figure does not include potential compensation.

55 SUITS TO DATE

Zurich American, in its court papers, said 55 purported class-action complaints have been filed in the United States against Sony. The insurer also said Sony has been subject to investigations by state and federal regulators since the breach.

Zurich American has subsequently received claims for coverage from Sony under its policy, a commercial general liability policy written for Sony Computer Entertainment of America as of April 1.

The insurer said it does not have any obligation to defend any other Sony unit under that primary policy, since it only applies to the specific business in question.

In addition, Zurich American said its policy only covers the Sony unit for "bodily injury, property damage or personal and advertising injury." It said no such claims have been made in any of the class-action lawsuits.

Even if such claims had been made, Zurich American said, the policy had exclusions in place that would deny Sony coverage for the claims made.

The case is Zurich American Insurance Co and Zurich Insurance Co Ltd vs. Sony Corp of America et. al, Supreme Court of the State of New York, No. 651982/2011.

($1=78.7 yen)

(Reporting by Ben Berkowitz, additional reporting by Liana Baker in New York and Taiga Uranaka in Tokyo; Editing by Ted Kerr and Chris Gallagher)

More from Claims Journal

Today's Insurance Headlines | Most Popular | National News

YAHOO!
NEWS

UK Murdoch paper warns website users data stolen

AFP – 5 hrs ago

Britain's Rupert Murdoch-owned tabloid The Sun has sent a message to readers warning them that computer hackers may have published their data online after an attack on the paper's website last month.

The paper's publisher News Group Newspapers (NGN) said in an email late Monday that details of people who took part in competitions and polls on The Sun's website may have been taken.

NGN, which is part of News International and published the Sunday tabloid News of the World until its closure amid a phone hacking scandal last month, said names, addresses and phone numbers may have been published. It said no financial or password information was affected.

Hacking group LulzSec claimed responsibility for the cyber attack, which forced Murdoch's British papers to pull their websites and culminated in The Sun's site being replaced with a hoax story reporting the mogul had died.

"As you may be aware, on July 19 the Sun website was subject to an organised criminal attack," said the email to Sun readers sent out by Chris Duncan, director of customer management at News International.

"It has now come to our attention that some customer information from competitions and polls was breached as part of this attack.

"Details vary, but could include name, address, date of birth, email and phone numbers. No financial or password information was compromised.

"We are contacting you because we believe that information that you submitted to us could have been accessed, and may be published online by the group responsible."

Duncan added the company was working with police and the government's data protection watchdog to try to retrieve the stolen data.

LulzSec has claimed responsibility for a 50-day rampage earlier this year against international businesses and government agencies, including the Central Intelligence Agency and Senate in the United States and electronics giant Sony.

On Monday, an 18-year-old suspected of being a spokesman for LulzSec and another hacking group Anonymous was granted bail at a London court after being charged with hacking into websites.

YAHOO!
NEWS

Hackers access data on 35 mln S. Koreans: agency

AFP – Thu, Jul 28, 2011

Hackers using an Internet address registered in China have gained access to major South Korean websites and may have stolen the private information of 35 million users, authorities said Thursday.

They breached the systems of Nate (www.nate.com) and Cyworld (www.cyworld.com), both run by SK Communications, the Korea Communications Commission said.

Nate is a search engine with 25 million users and Cyworld is a social networking website with 33 million users in a country with a population of 48.6 million.

From the two sites combined, information on about 35 million users such as names, web IDs, phone numbers, e-mail addresses and resident registration numbers appear to have been leaked, the commission said in a statement.

SK Communications has asked police to investigate the cyber attack, commission official Kim Kwang-Su told AFP, adding his office was still investigating the incident.

"We have no information on who the hackers were. This could be the biggest hacking incident in our country," he said.

The previous worst computer security breach was in February 2008, when Internet Auction -- a subsidiary of US firm eBay -- was hacked. This led to the theft of private information on more than 10 million users.

"We took security steps after detecting a malicious code originating from an IP (Internet protocol) address from China on Tuesday," said SK Communications spokeswoman Koo Ki-Hyang.

"Our probe is still under way but we believe information on an estimated 35 million users might have been leaked."

South Korea, the world's most wired nation with more than 90 percent of homes connected to the Internet, has expressed concern about cyber attacks by Chinese and North Korean hackers.

In 2004 hackers based in China allegedly used information-stealing viruses to break into the computer systems of Seoul government agencies.

Seoul accused Pyongyang of staging cyber attacks on websites of major South Korean government agencies and financial institutions in March this year and in July 2009.

In May South Korea said a North Korean cyber attack paralysed operations at one of its largest banks. North Korea reportedly maintains elite hacker units.
