ALERT
MAY 10, 2011

GLOBAL INSURANCE GROUP
News Concerning
Recent Professional Liability Issues

COZEN O'CONNOR
www.cozen.com

"ANONYMOUS" HACKS SONY PLAYSTATION NETWORK: THE INCREASING IMPORTANCE OF OBTAINING CYBERSECURITY INSURANCE COVERAGE

Bryan W. Petrilla • 610.832.7459 • *bpetrilla@cozen.com*

Anyone who harbors the notion that video games are simple distractions from the age of "Pong" has not seen the latest statistics. One of the most popular games released last year, "Call of Duty: Black Ops," generated $650 million in the first five days of sales and exceeded $1 billion in record time. The achievement put the game in the company of Michael Jackson's album "Thriller" and James Cameron's movie "Titanic." As a whole, the video game industry has been valued at more than $100 billion. The massive size and scope of the industry make the impact of a cyber attack all the more devastating.

Like most games, video games are more fun to play with others. Games like "Black Ops" are designed specifically with the multiplayer experience in mind. Multiplayer games are made possible by online networks, such as those hosted by Microsoft and Sony, which enable gamers to connect with each other and play together in real time. For example, Microsoft's Xbox Live service not only enables multiplayer games, but offers a host of other services, including the ability to download games directly to a user's hard drive. Like other online shopping experiences, downloading games usually requires the use of a credit card number and the disclosure of personal information. It is a convenient, efficient, and fun service. What could possibly go wrong? Just ask Sony.

On April 20, 2011, Sony suffered a massive security breach of its online PlayStation Network, which has over 77 million users in 59 countries. Credit card and other personal information was compromised. Sony waited several days before notifying its customers of the breach. When it did provide notification, it posted a statement on its corporate website, stating in relevant part:

> [W]e believe that an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birth date, PlayStation Network/ Qriocity password and login, and handle/PSN online ID. It is also possible that your profile data, including purchase history and billing address ... may have been obtained.

Sony blamed the breach on "a very carefully planned, very professional, highly sophisticated criminal cyber attack" in which hackers planted a file on Sony's server labeled "Anonymous," along with the words, "We Are Legion." The "We Are Legion" reference is from a passage in the Bible in which Jesus exorcises an evil spirit from a possessed man. The spirit identifies itself as Legion, adding ominously "for we are many." That seems encouraging.

Judging by public reaction to both the security breach and Sony's response to it, the second part of the "We Are Legion" story may be more relevant. The evil spirit leaps out of the man and jumps straight into a nearby herd of swine, which promptly stampedes madly off a cliff to its demise. Sony has not been run off a cliff exactly, but it has been sued, subjected to a Congressional inquiry, and investigated by the U.S. Department of Justice and various international governmental agencies.

At a congressional committee hearing discussing the breach, one congressman called Sony's delay "unconscionable and unacceptable." Another called the notification effort "half-hearted, half-baked" and complained that "Sony put the burden on consumers to 'search' for information, instead of accepting the burden of notifying them." A Sony

representative reportedly responded that the delay was due to its inability to send out more than 500,000 emails per hour, slowing the massive task of notifying tens of millions of potentially affected customers.

The U.S. Department of Justice complained that Sony did not meet with FBI agents to discuss the breach until five days after it was discovered. The head of the Federal Trade Commission's Consumer Protection Bureau raised the issue of national cybersecurity legislation to establish minimal security standards and notification requirements that could be augmented by state law. There have also been inquires from the United Kingdom Information Commissioner Office and the Australian Privacy Commissioner. Are we having fun yet?

For its part, Sony has stated that "[w]orking closely with several outside security firms, the company has implemented significant security measures to further detect unauthorized activity and provide consumers with greater protection of their personal information." Sony also announced the creation of a chief information security officer to add "expertise in and accountability for customer data protection and supplement existing information security personnel."

For the video game industry, the attack raises some serious concerns about whether the advances in technological infrastructure are being adequately secured, especially with increased talk of eliminating traditional gaming consoles and replacing them with "cloud-based" systems. Cloud-based systems would enable gamers to store all of their information and games at an external source that would be accessed remotely, eliminating the need to purchase a hard drive based console. But storing a gamer's personal information, along with thousands of dollars worth of games, in a digital cloud will only raise the stakes should future security measures prove inadequate.

Then, of course, there are the inevitable lawsuits. Kristopher Johns fired the first shot across the bow with a suit in the U.S. District Court for the Northern District of California. He accused Sony of "negligence in data security" and alleged that it did not take "reasonable care to protect, encrypt, and secure the private and sensitive data of its users." He is seeking class action certification on behalf of all PlayStation Network users and is seeking monetary damages and free credit card monitoring. Following closely behind, a 21-year-old gamer from Mississauga, Ontario filed a proposed class action suit against Sony for breach of privacy. That suit seeks more than $1 billion in damages, including the cost of credit monitoring services and fraud insurance.

The total cost of the security breach and response? According to the think tank Ponemon Institute, the average cost to respond to a security breach in 2010 was more than $300 per affected customer. Given the number of users, Sony's exposure could exceed $24 billion. Does Sony have insurance coverage tailored to cover cybersecurity risks? That is what former Secretary of Defense Rumsfeld would call a "known unknown." More insurers are beginning to offer cyber risk policies as the risk of suffering a security breach and incurring significant damages increases. Coverage limits for a primary layer cyber risk policy may be as much as $10 million, and excess cyber risk insurance policies with increased limits of liability are available at relatively modest premiums, particularly when measured against the potential exposure. A dedicated cyber risk policy may also provide coverage for crisis management costs and attorneys fees in addition to the limits of liability.

It is important to realize that even though a company may not be as large or directly entrenched in online services as a company like Sony, the risk of a cyber attack is very real for any company storing sensitive or confidential information in a computer database. It would be wise to purchase cyber risk insurance coverage before suddenly finding the bottom of that cliff rushing more clearly into focus.

To discuss any questions you may have regarding the issues discussed in this alert, or how they may apply to your particular circumstances, please contact Bryan W. Petrilla at 610.832.7459 or bpetrilla@cozen.com.

© 2011 Cozen O'Connor. All Rights Reserved. Comments in the Cozen O'Connor Alert are not intended to provide legal advice. The analysis, conclusions, and/or views expressed herein do not necessarily represent the position of the law firm of Cozen O'Connor or any of its employees, or the opinion of any current or former client of Cozen O'Connor. Readers should not act or rely on information in the Alert without seeking specific legal advice from Cozen O'Connor on matters which concern them.