Alert
March 13, 2014

Global Insurance Alert
News Concerning Professional Liability Issues

COZEN O'CONNOR

PlayStation Problems: No Defense in Sony's Cyberattack Suits

On February 21, 2014, a New York state trial court judge ruled that Zurich American Insurance Company has no duty to defend the Sony Corporation in lawsuits relating to a 2011 cyberattack on its PlayStation network. This decision is among the first in the country to address coverage issues for large scale data security breaches. Judge Jeffrey Oing rendered an immediate decision after hearing oral argument, recognizing the issue's importance and the likelihood of an appeal.

Zurich, Sony's general liability insurer, brought this declaratory action to determine coverage for approximately 60 underlying lawsuits arising out of the PlayStation cyberattack. That attack was then among the largest such events in history: nearly $2 billion in losses were claimed after hackers stole personal information from PlayStation users numbering in the tens of millions. As Judge Oing acknowledged during the hearing, and as the reader is doubtless aware, there have been other well-known data security breaches in the ensuing years since the PlayStation cyberattack, such as the November-December 2013 breach of Target customers' information. Because of the well-known parties involved here, and given the pending appeal, the PlayStation cyberattack decision will likely impact the realm of liability insurance and cyber-insurance significantly.

The Court's Coverage Analysis

The Coverage B provision at issue in Zurich's policy covered "oral or written publication in any manner of material that violates a person's right of privacy." The fundamental question was whether this required Sony to commit the breach-causing act, or if third parties' acts sufficed. The court emphasized that Sony was not at all involved in the "publication": criminal hackers illegally intruded the PlayStation sites, breaching Sony's insufficient security. The court declined to expand Zurich's liability by construing "in any manner" to include the hackers responsible for the data breach. The court agreed with Zurich that in any manner referred to any manner of dissemination, and not "by any actor."

The court found that the Coverage B provision could only be read to require the policyholder to perpetrate or commit the publication, and could not be expanded to third-party actors. It ruled the policy language was unambiguous and commented that it was unwilling to expand coverage beyond what the insurer knowingly entered into. The court alluded to the fact that the insurers were bargaining with only the policyholder, and not with any third parties, when issuing the policyholder's liability insurance.

Sony had asserted that the policy lacked clear language to exclude this type of cyberattack, arguing that the policy did not explicitly require the insured to be the one publishing the data. It stated that if Zurich wanted to restrict the coverage to the policyholder's acts, it should have so specified in the contract. However, Zurich distinguished Sony's cited cases as addressing negligent security that involved the insured's affirmative conduct. Further, Zurich noted that every tort claim listed as within the purview of the personal injury coverage required an intentional act or affirmative conduct by the policyholder. The court agreed with Zurich and concluded the language of the policy was clear and Zurich had no duty to defend Sony.

Further Proceedings

Judge Oing acknowledged on the record during the hearing that an appeal of his order would be likely. Because the New York Appellate Division only rarely issues lengthy opinions, however, any appellate ruling may not provide a comprehensive analytical framework on how a data breach should be construed under general liability policies. Given that Judge Oing's ruling is one of the

Related Practice Areas

- Insurance Coverage
- Privacy & Data Security
- Professional Liability Insurance Coverage

Industry Sectors

first cases in the country addressing coverage for data breaches from negligent security, it is likely to be a frequently cited decision going forward.

Future Implications

The PlayStation network breach was one of the largest recorded data security breaches when it occurred, requiring a complete shutdown of the server for nearly a month. The hackers stole personal information, including names, addresses, birthdates, credit card numbers and bank account information. This breach, while certainly large, has since been eclipsed by the recent Target breach occurring over the pre-Christmas 2013 shopping season. Other similar data breaches are becoming more commonplace, and apparently more severe, in increasingly Internet-driven and Internet-reliant commerce.

This decision has the potential to persuade otherwise reluctant policyholders to buy data breach coverage, given the increased awareness of the risks and the ever-present potential for large-scale response costs or third-party litigation. Some of their reluctance to purchase coverage for data breach losses may have stemmed from speculation that coverage, or at least a defense to lawsuits, would be provided under their existing commercial general liability policies. This decision brings those assumptions into serious doubt. Coverage for these losses under standard commercial general liability policies would be expected to decrease in any event, as new data breach exclusions are issued in most states, addressing misappropriated credit card and financial information, among other increasingly common scenarios. Therefore, companies susceptible to data breach claims would be wise to have a mitigation-of-risk program in place, which includes (but is not limited to) purchasing insurance that specifically safeguards against these risks.

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 Michael D. Handler at (206) 808-7839 or mhandler@cozen.com.