Sony Insurer Disputes Breach Insurance Claims

A cautionary tale for enterprises that think they have data breach insurance

By Ericka Chickowski, Contributing Writer
Dark Reading, Darkreading
Jul 22, 2011 | 04:50 PM
URL -

A new court battle reported this week could potentially decide how liability is determined when organizations covered by general liability insurance get hacked and suffer a database breach.

The case at hand pits insurer Zurich American against its client Sony: Zurich has refused to cover the costs of class-action lawsuits stemming from Sony's embarrassing breaches earlier this year, and wants the courts to weigh in with a judgment to clarify the matter.

Sony says it expects the financial fallout from the breaches to add up to more than $178 million this year; the firm is currently fighting 55 class action lawsuits. According to a report from Reuters, Zurich recently stated in court papers that it had received claims from Sony to cover costs related to these lawsuits under a general liability insurance policy written by Zurich.

The insurer says it shouldn't have to pay the claim since the policy is for "bodily injury, property damage, or personal and advertising injury," and none of those apply within the class-action suits.

Given the rising prevalence of data breaches and the increasing storm of litigation companies face from customers furious about their loss of privacy, this case is a must-follow precedence-setter for professionals in IT security and enterprise risk management. Ty Sagalow, an insurance consultant and founder of Innovation Insurance Group, says there are still many within the industry who are under the mistaken assumption that general liability policies will help them out in the event of a data breach.

"There are probably still some risk managers out there that think that their comprehensive general liability policy cover breaches," says Sagalow, who was one of the main experts in charge of first drafting cyberinsurance policies for Zurich when he worked for the company prior to starting his own consulting shop. "These types of cyberevents are not covered in the typical standard forms of insurance."

Sagalow says that as cyber-risks increase in sophistication and pervasiveness, organizations need to think about adding additional coverage that can hold up to court scrutiny when everything hits the fan. But because cyberinsurance is such a new phenomenon, it's a buyer-beware situation.

"Unlike many insurance policies that companies buy, there is no standard form -- it's not like comprehensive general liability or workman's comp or fleet auto -- cyber is not standard," Sagalow says. "Plus, it is in an area which is called surplus insurance, meaning that they're not subject to state filing regulations for state approval, which allows freedom of an insurance carrier to set terms and conditions."

This means that organizations considering cyberpolicies have to read very carefully before signing on the dotted line, says Rick Kam, president and founder of consultancy ID Experts, a firm that helps with pre- and post-breach strategy. He says that companies often buy cyberinsurance expecting it to cover breaches, only to discover after an event that the insurance is primarily for instances such as denial-of-service attacks.

"Insurance has to be very specific to cover those issues related to a data breach," Kam says. "One of the major tips I would suggest is to have their enterprise risk manager -- the person responsible for their insurance policies -- meet with their insurers to validate what's covered and what's not when it comes to a breach."

Have a comment on this story? Please click "Add Your Comment" below. If you'd like to contact Dark Reading's *editors directly, send us a message*.

Print