

## Sony Hack Shows Need For Cyber Coverage On Many Fronts

By Jeff Sistrunk

*Law360, Los Angeles (January 09, 2015, 2:04 PM ET)* -- The massive Sony Pictures Entertainment Inc. hack raises concerns beyond the privacy and data liability issues seen in other recent high-profile cyberattacks, underscoring the need for companies to acquire comprehensive insurance coverage to shield themselves from other cyber-related risks such as business interruption, attorneys say.

The monumental cyberattack, which first made headlines in late November, shut down the Sony Corp. unit's network for two days and compromised personal information for 47,000 past and present employees, as well as several new or unreleased movies and internal emails containing confidential corporate data. Sony also responded to the breach by offering only a limited release of the controversial comedy "The Interview," which was cited by hackers as the impetus for the attack.

The multiple potential sources of lost revenue tied to the Sony hack, coupled with the sheer volume of the company's own proprietary information that was compromised, distinguish the incident from previous large-scale data breaches at major retailers such as Target Corp., which mostly involved the theft of customers' credit card data and other personally identifiable information.

"It was a nightmare as far as data breaches go, with political, nationalistic, proprietary property, reputational and employment overtones," said Joshua Gold, an Anderson Kill PC shareholder and chair of the firm's cyber insurance recovery group. "There was also business interruption fallout. It was really the perfect storm of everything that could be disastrous about a data breach."

With many insurers removing cyber coverage from commercial general liability and other "traditional" policies, the Sony breach highlights the need for companies to pursue robust specialized cyber policies that can cover them against business interruption and other risks associated with hacking incidents, according to attorneys.

"Privacy laws and regulations have really been driving the U.S. market for cyber insurance," said K&L Gates LLP partner Roberta Anderson. "However, incidents like the Sony incident drive home the fact that cyber risks go far beyond privacy issues. Focusing principally on privacy and data breach liability could mean that a company is overlooking potentially more severe threats resulting from the impact of a malicious threat or a technology failure, including the failures of vendors and cloud providers, on supply chains and day-to-day business operations."

While some cyber insurance policies focus specifically on privacy and data loss concerns, providing

coverage for remediation costs associated with a cyberattack such as breach notification and public relations efforts, other policies also offer business interruption and media liability provisions, according to attorneys. Some insurers allow policyholders to combine first-party and third-party cyber coverage, providing savings on premiums, said Erin L. Webb, an associate in Dickstein Shapiro LLP's insurance coverage group.

Sony could potentially assert business interruption claims for numerous events stemming from the hacking incident, including the company's temporary loss of its network capabilities and its decision to cancel the wide theatrical release of "The Interview" in response to hackers' threats, as well as the dissemination online of five films, according to experts.

Other companies should take note and take steps to ensure that the business interruption coverage in their cyber policies is sufficiently broad to cover a wide variety of scenarios that could result from a cyberattack, attorneys say.

"When considering business interruption coverage, it is important to consider the trigger of coverage at all times and also the scope of contingent business interruption coverage — business income lost as a result of a cyber event affecting the computer systems and networks of key suppliers, customers and business partners," Anderson said.

The internal Sony emails leaked by hackers — which included messages containing disparaging remarks about celebrities such as Angelina Jolie — could give rise to privacy-related tort claims against the company, including defamation, attorneys say. Companies that suffer similar leaks could find coverage in the media liability provision of a cyber policy, depending on how the provision is worded, according to attorneys.

"Cyber policies, including the separate media coverage, can cover a very broad range of privacy-related issues, including potentially those related to the release of private emails and other publications, and cover a wide range of privacy-related torts resulting from publication of information, such as defamation, as well as intellectual property infringement," Anderson said.

In addition, coverage for such claims may also be available under traditional policies, attorneys say.

"If someone is going to sue you because emails were released that made them look bad, coverage may be available under an errors and omissions policy or potentially under Coverage B of a CGL, which usually covers claims for invasion of privacy," Webb said.

The alleged involvement of the North Korean government in the Sony hack also raises coverage questions, as many cyber insurance policies contain broad exclusions applying to acts of war or terrorism, according to attorneys.

"The terrorism implications of the Sony hack could be problematic," said Gregory D. Podolak, head of Saxe Doernberger & Vita PC's cyber risk practice. "Most companies don't view themselves as a high-profile terrorism risk, yet many hacking events involve some form of political motivation."

However, Anderson said she has found that terrorism exclusions in cyber policies are "highly negotiable" and "can often be removed or modified to provide an exception to the exclusion for cyber terrorism events."

"Even policies that do not contain a terrorism exclusion will almost always contain a separate war exclusion, and insurers are likewise usually willing to offer a cyber terrorism exception to the war exclusion, which again lends greater peace of mind," Anderson said.

Ultimately, because there is little uniformity in specialized cyber policies and relevant case law is underdeveloped, close inspection of key terms in such policies is essential, according to attorneys.

"I think the cyber market is one that is very much in flux," Gold said. "It makes a risk manager's job very difficult in deciding how to protect a company against cyber-related perils. The Sony hack demonstrates that what companies need most is broad cyber protection. While there is a lot of good coverage out there, there is also a lot of bad coverage masquerading as good coverage. A lot of policies are a recipe for insurance disputes. If a form isn't clear, it's going to lead to problems down the road."

--Editing by Kat Laskowski and Mark Lebetkin.