Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A Cyberattack Survival Guide For Policyholders

By **Jeff Sistrunk**

Law360, Los Angeles (October 1, 2015, 6:11 PM ET) -- Litigation faced by Target and Home Depot after massive data breaches highlights the cybersecurity concerns that all companies face. Here, attorneys discuss how insurance policies can protect against potential liability and where companies my have trouble getting coverage.

Card Issuer Liability

Target Corp. and other major retailers hit with cyberattacks have faced claims from financial institutions that issued customer credit cards. Last month a Minnesota federal judge certified a class of about 9,000 banks and credit unions that contend they're entitled to damages to cover fraud losses and costs associated with handing out new credit and debit cards to their customers in the wake of the Target breach, which exposed payment information for more than 40 million people.

Depending on the policy language, companies may be able to find coverage for card issuer litigation under "Coverage A" of traditional commercial general liability policies, said K&L Gates LLP partner Roberta Anderson.

"Property damage, in those policies, is defined not just as physical injury but loss of use of tangible property not physically injured, [in other words], cards cannot be used and need to be reissued," Anderson said. "Financial institutions had to replace physical cards that were not injured but couldn't be used. Those losses fall squarely within the standard form's Coverage A."

Cyber-specific policies available on the market also should clearly cover those claims, as well as class actions filed by consumer plaintiffs, Anderson said.

Even under cyberinsurance policies, though, card issuer liability is an area "where carriers have been pushing back and surprising policyholders with restrictive coverage positions," said Barnes & Thornburg LLP partner Scott Godes.

Ultimately, payment card breaches are unavoidable, and there is no "silver bullet" to eliminating the possibility of a breach, Godes said.

"Look at the large enterprises that were hit with data breaches," he said. "Many, if not all, had to be and were certified as compliant with payment card security rules by a third party. Here are companies that have followed the rules and been certified as compliant but are hit with a data breach nonetheless."

The key for a corporate policyholder in buying insurance for these sorts of risks is to buy a tower of coverage with the fewest restrictions, according to Godes.

"Limits are important, and avoiding hidden trapdoors to coverage may be just as important," he said. "The problem is that the risks are ever-changing. Every few months, there is a discussion of the newest, 'latest and greatest' methods that hackers are using. As a policyholder, you want to ensure that your policy is broad enough and elastic enough to provide coverage for the changing landscape of threats."

Customer Liability

Home Depot Inc. and Anthem Inc. are among the companies that continue to grapple with sprawling litigation brought by consumers who claim their personal information was put at risk by a data breach. While some consumer plaintiffs have seen their claims dismissed for lack of standing due to the absence of concrete financial harm stemming from the cyberattacks, such suits remain a major source of potential liability for companies, according to attorneys.

"Those losses could be tremendous," said Stella Szantova Giordano, an attorney at Saxe Doernberger & Vita PC. "They include not only payments due to injuries suffered by individual customers, but potentially also exorbitant legal fees."

CGL policies may respond to provide coverage for companies' liability to customers, despite the proliferation of cyber-related exclusions in such policies, experts say.

"There are an increasing number of exclusions in CGL policies, but they're not absolute," Anderson said. "Malware is often present in systems long before the hack is discovered. There may be CGL coverage that responds to a cyberattack that wasn't detected until years later."

Joshua Gold, an Anderson Kill PC shareholder and cyberinsurance attorney, said that his firm has secured defense costs for policyholders for class action suits under general liability policies.

Attorneys say future data breach coverage disputes involving CGL policies will continue to focus on whether there was a "publication" of customer data that invokes a policy's advertising and personal injury coverage.

The publication issue was crucial in Sony Corp. of America's now-settled dispute with its insurers over coverage for the PlayStation Network data breach. The state judge presiding over that case held that, while hackers' theft of the personal data of millions of PlayStation users constituted a "publication" of private information as required by the relevant policies, the insurers still owed no duty to defend because the publication wasn't "conducted or perpetrated by the policyholder."

Courts have varied in their takes on the publication issue, with some interpreting the term expansively and others adopting a more narrow reading.

"In the Sony case, the court reasoned that Sony had to do the publication — even though publication 'in any manner' would have sufficed — and that the policy language didn't apply to publication by a third party," Giordano said.

In addition to pressing for CGL coverage, companies can seek out cyber-specific policies tailored to cover

customer and other liabilities related to cyberattacks, experts say.

D&O Litigation

Executives at Target and Home Depot are facing shareholder derivative suits alleging they failed to take proper measures to protect their respective companies from data breaches. In most cases, directors and officers at companies that suffer a cyberattack should indisputably be covered under traditional D&O policies, according to attorneys.

"If there is a cyber claim brought against executives, they should definitely have D&O coverage in the current marketplace," Gold said. "Any claim against the board of directors or senior management alleging a wrongful act will fall under D&O insurance. I haven't yet seen a cyber exclusion in those policies, nor should there be."

Risk managers should make sure that a company's D&O policies are clean of cyber exclusions, according to Gold.

However, D&O policies with cyber exclusions do exist, and almost all D&O policies have bodily injury exclusions, Anderson noted.

"Some of those [exclusions] can be worded broadly enough to include privacy-related torts," Anderson said. "Always be mindful of exclusions to make sure that privacy-related liabilities aren't excluded."

On applications for D&O insurance, companies should make sure there are no questions about cybersecurity preparedness, but if there are, they should "answer carefully and pull necessary data from other departments like IT," Gold said.

First-Party Property Damage

Seeking coverage for first-party property damage tied to a cyberattack presents a more difficult proposition for policyholders, attorneys say.

While no U.S.-based companies have yet reported any major physical damage resulting from a cyber event, the German government last year confirmed that a blast furnace at a steel mill there was seriously damaged when hackers disrupted its control systems.

Most first-party property policies include an electronic data-related exclusion, Anderson said.

"There often is broad causation-related language, such that an exclusion purports to exclude cover if any electronic event is found in the chain of causation," she said.

Moreover, cyber-specific policies generally don't cover first-party property damage but rather loss of digital assets, she said.

"That's the trouble you have, if you have a physical loss," Anderson said. "Say you have malware that causes your system to go down. The system is compromised so you can't conduct business, and perhaps there was an explosion. Neither a traditional property policy nor a cyber policy may offer coverage."

Policyholders may have options, though, as there is a new type of insurance product that sits over

traditional property coverage and essentially writes out broad electronic data-related exclusions, according to Anderson.

"I think that market will come on extraordinarily strong over the next year," she said.

--Editing by John Quinn and Brian Baresch.
