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

4 Insurance Takeaways From Lloyd's Cyberattack Report

By **Jeff Sistrunk**

Law360, Los Angeles (July 13, 2015, 8:31 PM ET) -- Insurance market Lloyd's of London recently co-wrote a report predicting that a major cyberattack on the East Coast could trigger $70 billion in insurance claims, highlighting potentially glaring deficiencies in traditional and cyber-specific policies. Here, Law360 examines the important takeaways for insurers and policyholders.

A Major Attack Would Affect a Wide Range of Policies

In the joint report, Lloyd's and the University of Cambridge Centre for Risk Studies laid out a hypothetical scenario where computer hackers infect electricity generator control rooms with malware, plunging 15 U.S. states into darkness and leaving 93 million people without power. According to the study, total economic losses from such an event could reach $1 trillion, with up to $70 billion in covered insurance claims.

The massive cyberattack envisioned by the report would affect a broad array of policyholders, including power generation companies, companies that lose power and homeowners, implicating both cyber-specific and "traditional" insurance policies.

For instance, a power generation company whose generators are physically damaged may be able to tap coverage under its property insurance or a dedicated cyberinsurance policy that covers property loss. One or both of those policies may also cover the company's costs of investigating and responding to the incident.

Meanwhile, a food processing company that finds itself without power may make claims for spoiled goods, as well as service interruption under the so-called suppliers extension of a policy covering contingent business interruption. Furthermore, if the company loses its market position or sees it stock price slip as a result of the outage, its executives may face shareholder claims that are covered by a directors and officers policy.

"While this hypothetical event is an extreme one, it highlights how coverages other than cyber are implicated in various types of cyber events," said Farella Braun & Martel LLP partner Tyler Gerking. "What comes through loud and clear in this report is that, while cyberinsurance would be implicated for certain insureds in this type of event, others would be looking to a property policy or general liability/D&O policy."

Cybersecurity Deficiencies Can Be Predicted

The report noted a number of unique challenges insurers face in trying to predict and model cyber risks in order to tailor insurance products, including the evolving, dynamic nature of the threats. However, the study concluded that cyberattacks are not "unlimited or infinitely scalable."

"They can have significant constraints that limit attack severity and curtail the amount of loss that insurers may face," the report said. "A successful cyberattack has to overcome all the security systems put into place to protect against it, requires expertise and resources by the perpetrators who face their own risks of identification, prosecution and retribution, and the loss consequences of attacks are mitigated by risk management actions."

Barnes & Thornburg LLP partner Scott Godes said the report "contradicts the assertion that the insurance industry is perplexed at how to underwrite and model" cyber risks "because it can't understand what's out there."

Joshua Gold, an Anderson Kill PC shareholder and cyberinsurance attorney, said he agrees that cyberthreats are dynamic but parted ways with the report's assertion that such risks are relatively new.

"The insurance industry has been dealing with claims involving computer-related problems such data destruction and loss and business interruption to some degree since at least the 1980s," Gold said.

Still, because there isn't as much of an established track record with cyber incidents as with other perils, it is "hard to look back and say how current modeling stacks up against history," said Gregory D. Podolak, head of Saxe Doernberger & Vita PC's cyber risk practice.

"As a result, you see a lot of these policies with built-in escape hatches," Podolak said. "They ask a lot of information about security measures in the application and incorporate those representations into the policy and subsequent iterations, giving the carrier considerable ammunition to pull the ripcord and bail on coverage if it can make a viable argument that a policyholder's security protocols were not maintained or improperly described."

The report said that the sharing of cyberattack data "involving a wide range of parties with an interest in developing resilience to cyberattack offers the most promise for enabling the insurance solutions required to meet" the risks.

From a policyholder's standpoint, extensive sharing of cyber risk information can be a double-edged sword, some attorneys say.

"We know that insurers as an industry collect data and share it with each other on first-party loss experience," said Manatt Phelps & Phillips LLP partner Stephen Raptis. "What that does is supply enough information to the industry that they're able to set premiums that will realistically reflect the risk. That could be positive or negative for policyholders: it may make premiums more expensive, but could also make them less expensive."

Traditional Policies Are Often Ambiguous on Cyber Coverage

Within traditional insurance policies, there are a number of areas where "there could be significant ambiguity around how coverage will be interpreted and whether claims could reasonably be expected to be successful or denied," the report said.

If insurers are silent on cyber coverage, "then it is open to interpretation whether or not the general policy covers certain cyberevents," the report said.

"For example, Lloyd's notes that 'all risk' property policies are often silent on coverage for cyber-related losses, and there are certain exclusions that still could be ambiguous," said Susan White, a partner at Manatt Phelps & Phillips LLP.

Among other issues, there is ambiguity in some traditional policies as to whether an incident stemming from a cyberattack is a covered peril, and whether an insurer would be obligated to pay cyber-related property damage, suppliers extension or "critical vendor" contingent business interruption claims, according to the report.

"There can be coverage lurking in the policy explicitly, or it can be interpreted to provide coverage for a cyber incident," Godes said. "The entire report belies carriers' bald-faced assertions that certain policies were never intended to provide coverage for cyber events."

The report suggested that insurers and their corporate customers engage in open discussions over any uncertainties about cyber coverage in traditional policies in order to avoid a "mismatch of expectation and reality."

"This is really about a level playing field: what do the parties expect? For example, when is a commercial property policy supposed to respond, and when is the cyber policy supposed to respond?" Podolak said. "Importantly, the answers to those questions change from situation to situation, and are further complicated by an evolving marketplace where traditional lines are aggressively reacting to cyber exposures and working to limit related obligations. It could very well happen that you have a traditional policy with added endorsements that scale back coverage to exclude a loss involving a cyber component."

He added, "If policyholders don't proactively have that dialogue with their insurers, there is a much greater risk of a miscommunication about how the policies are supposed to work together."

Policyholders "need to keep an eye on their policies at renewal time as insurance companies grapple with these risks," Gerking said.

"They may see new language or exclusions," he said. "As insurers gain more information, premiums and sublimits may be affected."

Cyber-Specific Policies May Be Limited

The report highlights the importance of policyholders closely scrutinizing specialized cyber policies, as they may not cover as broad a range of risks as buyers may hope, attorneys say.

"As a policyholder, you want the broadest possible coverage," said Pillsbury Winthrop Shaw Pittman LLP partner Vince Morgan. "As companies continue to innovate technology, they are finding new and different ways for technology to improve our lives, but that also creates new vulnerabilities from a cybersecurity standpoint."

Indeed, policyholders "reasonably expect these [cyberinsurance] products to cover all cyber risks,"

said Hunton & Williams LLP partner Lon Berk.

"However, the products primarily address privacy issues and typically exclude bodily injury or property damage-type losses," Berk said. "Simultaneously, on more traditional policies, insurers have introduced exclusions that bar coverage for issues related to code or data. Unless policyholders and representatives are careful, they're therefore buying a dispute over their coverage."

Godes suggested that the insurance industry should introduce a cyberinsurance policy parallel to a commercial package policy, providing coverage for all types of losses resulting from a cyber event.

"Rather than picking and choosing coverage based on slivers of losses, there should be a broad package that can provide policyholders the peace of mind they need in the event of a major cyber incident," Godes said.

The insurance industry's current approach of rolling out a new product every time there is a "supposedly 'new'" cyber peril that the industry is uncomfortable with "would be a terrible model going forward," Gold said.

"Having to fill that coverage gap by constantly buying a new insurance product is bad customer service," he said.

--Editing by John Quinn and Brian Baresch.
