Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

4 Key Cybersecurity Insurance Cases To Watch

By **Jeff Sistrunk**

Law360, Los Angeles (July 14, 2017, 5:06 PM EDT) -- Businesses both large and small are facing an ever-evolving landscape of threats to their cybersecurity, from infiltration by computer hackers to elaborate criminal schemes designed to trick employees into wiring money to overseas bank accounts.

While insurance policies are available for a range of data security risks, disputes between policyholders and insurers are inevitable, as evidenced by a California health network's battle with its insurance carriers for coverage of expenses tied to a data breach and a seafood company's appeal of a ruling that its insurer needn't cover losses it suffered in a money transfer scam.

Here, Law360 takes a look at four cases that could shape the future of coverage for cybersecurity threats.

Cottage Health v. Columbia Casualty Co.

In one of the first cases testing coverage under a cyber-specific insurance policy, Cottage Health System is headed to trial in a Santa Barbara, California, court this fall against its primary and excess insurance carriers over more than $4 million in data breach-related costs.

The case is notable because it marks the first time a court has been asked to interpret cyberinsurance policy language requiring the policyholder to comply with specified network security requirements, attorneys said.

"It is going to be an important reminder for policyholders, however the case may turn out, that care is required with cyber policies that impose requirements for the level of security that the policyholder has to apply," said Anderson Kill PC shareholder Joshua Gold. "That is a shifting analysis, as the threats continue to morph. What may have been a sound security measure 18 months ago may now be outdated. It can be quite subjective and very much in flux."

Cottage, a nonprofit network of six hospitals, was accused in a class action complaint of allowing medical records for 32,500 patients to become publicly available online in 2013, according to court papers. In December 2014, Cottage settled the litigation for $4.125 million. The network remains the subject of ongoing investigations by California and federal regulators over the breach.

Columbia Casualty Co., which had issued Cottage a cyberinsurance policy, initially agreed to cover the class action deal, as well as the hospital network's attorneys' fees and costs to respond to the breach. But the

insurer has since disclaimed coverage, invoking a policy exclusion on the grounds that Cottage failed to apply the security measures it promised when it sought coverage.

Columbia launched a suit in federal court in 2015 challenging coverage, but that case was dismissed without prejudice to allow the parties to engage in mediation. After those efforts failed, Cottage lodged a complaint in California court, naming both Columbia and its excess carrier, certain underwriters Lloyd's of London, as defendants.

Farella Braun & Martel LLP partner Tyler Gerking said that the best move for policyholders to avoid coverage disputes like Cottage's is to negotiate with a cyber insurer up front to try to delete any exclusions for failure to maintain security protocols.

"Exclusions for inadequate security run counter to the purpose of cyberinsurance — to protect insureds from attacks even if they occur because of a mistake made by the policyholder," Gerking said.

The case is Cottage Health v. Columbia Casualty Co., case number 16CV02310, in the Superior Court of the State of California, for the County of Santa Barbara.

Rosen Millennium v. St. Paul

While insurers have largely tried to steer coverage for data breach claims into specialty cyberinsurance policies by introducing broad cyber exclusions into traditional commercial general liability policies, disputes over coverage for cyber-related claims persist under CGL policies lacking such exclusions.

"If a cyber claim is submitted under CGL coverage, that is a recipe for an instant fight," Gold said. "Under a cyber policy, there is a much better chance of a resolution without resorting to litigation."

In one such case, St. Paul Fire & Marine Insurance Co. is seeking a ruling that it doesn't have to cover a Florida-based hotel chain’s information technology subsidiary for $2.4 million in costs and fines stemming from a data breach in its hotel credit card payment system.

The insurer has asserted that Rosen Millennium’s policy covers only personal injuries, property damage and advertising injuries and that the data breach falls into none of those categories. In addition, St. Paul has said the policy's exclusion for breach-of-contract claims bars coverage for fines imposed on the hotel chain by Visa, MasterCard and American Express.

For its part, in an answer and counterclaim, Rosen pointed out that St. Paul could have placed an exclusion for "access to or disclosure of confidential or personal information" in its policy, but chose not to do so.

St. Paul Fire & Marine Insurance Co. v. Rosen Millennium Inc., case number 6:17-cv-00540, in the U.S. District Court for the Middle District of Florida.

Spec's Family Partners v. Hanover

In a clash over a common policy exclusion for contractual liabilities, Texas liquor store chain Spec's Family Partners Ltd. has sought the Fifth Circuit's review of a federal judge's ruling that The Hanover Insurance Co. doesn't have to cover about $4 million charged by its credit card processor following two data breaches. The company's opening appellate brief is due July 20.

Attorneys say that the Spec's and Rosen cases demonstrate that, for companies that handle payment card transactions, it is advisable to buy a cyberinsurance policy that explicitly grants coverage for claims related to payment card issues, especially given the broad exclusions for contractual claims in many traditional policies.

"That's not to say you may not be able to get coverage elsewhere, but it's not even worth the fight if you can get that coverage expressly granted through the auspices of a cyber policy," Gold said.

Spec's, a food and beverage retailer with roughly 160 locations in Texas, brought the suit against Hanover in February 2016 after the insurer refused to pay the costs of its 2014 lawsuit against card processing company FirstData Merchant Services.

Spec's alleged that Hanover had agreed to cover defense costs after the card processor withheld $4.2 million in receipts to help cover nearly $10 million in losses stemming from cyberattacks against Spec's in 2012 and 2014. But when Spec's took FirstData to court in Tennessee over the withheld receipts, Hanover refused to pay any defense costs, the retailer said.

U.S. District Judge Gray H. Miller found in a March decision that Hanover had no duty to defend because the underlying claim was rooted in Spec's contract for credit card transaction services, and Hanover's policy excludes claims for liability solely based on contractual obligations. Spec's then sought the Fifth Circuit's review.

The case is Spec's Family Partners Ltd. v. The Hanover Insurance Co., case number 17-20263, in the U.S. Court of Appeals for the Fifth Circuit.

Aqua Star v. Travelers

While some cyber criminals wield malicious computer programs to access companies' systems and steal information, others carry out sophisticated schemes to deceive businesses into authorizing transfers of money to fraudulent bank accounts. These types of "social engineering" schemes have led to hotly contested insurance coverage fights, mostly under the computer fraud provisions of commercial crime policies.

The Ninth Circuit is considering such a dispute in Seattle-based seafood company Aqua Star (USA) Corp.'s appeal of a Washington federal court's ruling that it isn't entitled to coverage under a Travelers crime policy for more than $700,000 in losses it suffered when it was manipulated into wiring funds to a fraudster. The appeal has been fully briefed, and a panel of the appellate court will hear oral arguments on an as-yet-undetermined date.

The typical structure of social engineering schemes has led to a fevered debate on what constitutes a "direct loss" implicating computer fraud coverage, since most of the scams involve an employee of a company authorizing what is believed to be a legitimate transfer in response to an initial email from a fraudster. Travelers and insurers in similar cases have argued that the actual transfer itself must be carried out through fraudulent means to constitute a direct loss.

"It is interesting how the insurance industry has taken such an aggressive position on the direct loss issue," Gerking said. "If you were to ask a typical businessperson if they think these types of criminal schemes should be covered under their crime policy, the answer would be an emphatic yes. There is a clear disconnect between insureds' expectations and insurers' positions."

According to attorneys, insurers' hard-line position on the direct loss issue may be attributable to a belief that policyholders should take measures to mitigate the risk of losses due to social engineering scams, such as requiring multiple steps to change bank account information or enact wire transfers.

"There is truth to that perception, generally, but appropriate measures are relative to the size and capabilities of the company," Greg Podolak, managing partner at Saxe Doernberger & Vita PC's Southeast office, said in emailed remarks. "At some point, risk transfer — [that is], insurance — as opposed to risk mitigation, becomes a vital component of a well-rounded risk management plan."

The case is Aqua Star (USA) Corp. v. Travelers Casualty and Surety Co. of America, case number 16-35614, in the U.S. Court of Appeals for the Ninth Circuit.

--Additional reporting by Ryan Boysen and Rick Archer. Editing by Emily Kokoll.
