LAW360

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

Cozen O'Connor Encourages Smart Cyber Subrogation Claims

By **Daphne Zhang**

Law360 (April 12, 2022, 11:17 PM EDT) -- Insurers and their counsel should be creative in making cyber subrogation claims as insured businesses' cyber losses have skyrocketed from multimillion-dollar ransomware, wire-fraud and phishing attacks, two Cozen O'Connor attorneys said in a webinar Tuesday.

When paying big bucks for a policyholder's cyber loss, carriers should be vigilant about who are the potential targets that caused the insured's loss, said Richard J. Maleski and Susie Lloyd of Cozen O'Connor, who represent insurance companies.

Cozen O'Connor attorneys Richard J. Maleski (left) and Susie Lloyd (center) told webinar participants Tuesday that an insured's IT vendors, software firms, background check companies and banks are among the targets a carrier can potentially go after to collect reimbursement from after paying claims for a policyholder's cyber-related losses. Ronald Menold (right), an FBI veteran and director of cybersecurity firm Cosecure who works with Cozen O'Connor, was also on the panel.

There are many targets an insurer can point fingers at and collect reimbursement from, including an insured's contracted IT vendors, software companies, background check companies, and even their retailers and customers, Maleski and Lloyd said. And if a carrier counsel is creative enough, there are a wide range of claims they can bring for cyber subrogation purposes, ranging from breach of contract, negligence and trespassing to fraudulent misrepresentation, among others.

"We are in a very unique position to help create some of these laws and to guide the court and help them understand how cyber subrogation fits into the legal world," Lloyd said. "The case law is just not there. There are not precedents yet."

The first step for a carrier to file a cyber subrogation claim is to figure out the potential targets, Maleski said.

"We generally do not consider the actual hacker or spoofer to be a viable subrogation target," the partner said, because it's hard to track down a sophisticated and anonymous criminal behind the computer.

But an "IT vendor is a perfect target to consider," he said. Insurers should check whether the insured

has a contracted IT vendor that provides cybersecurity protections and if the vendor sufficiently did its job. Many liability policies have added specific coverage for IT vendor liability in a cyberattack, he said. Carriers can also target an insured's software companies to see if there are inherent flaws in the insured's software in terms of how the code is written and how system updates are set up, Maleski said.

Insurers should also keep an eye on whether the policyholder's bank failed to take additional steps when executing a fraudulent transfer, whether the insured's retailer was negligent toward its own cybersecurity system, or whether an insured's customers should have been aware of network flaws before they continued doing business with the insured, he said.

Maleski said he is handling cyber subrogation claims on behalf of carriers against background check companies at the moment. If a background check company failed to vet one potential employee and if that person is subsequently involved in either an identity theft ring or a cybersecurity issue, then the background check company can be liable for improperly doing its job and giving the insured that risk, he said.

Carriers should work with cybersecurity experts to check whether third parties breached their duty of care and contract with the insureds, Maleski said. They can bring trespassing claims if an insured's third-party partner's action introduced a virus or spyware to the insured's computer systems. They can also allege fraudulent inducement if a party encouraged the insured to sign a contract, hire a vendor or perform an action based on a fraudulent intent, the Cozen O'Connor partner explained.

Additionally, fraudulent misrepresentation "is a great claim against a third-party IT or security provider who claims that they can give your insured everything to provide defenses against cybersecurity breaches, and then simply fails to do so," Maleski said.

The most difficult part of dealing with cyber subrogation claims is that there is no statutory guidance, Lloyd said. There is no consistency in federal and state law about how soon a vendor should notify its customers that there's been a breach, she said.

The Health Insurance Portability and Accountability Act requires a breach notification no later than 60 days after the fact, while the Federal Deposit Insurance Corp. requires banking organizations to report to their regulators in no more than 36 hours, Lloyd explained.

"Obviously, 36 hours to 60 days is a very wide range. It's on us to make that reasonableness argument and really gauge what is reasonable within the industry," she said. "Because the courts are also not providing that guidance just yet."

"There are several jurisdictions that are really homing in on this, such as California and New York," Lloyd continued. "They are slowly building on their case law on their statutes to allow us to have a framework in which to file suit on these claims."

Carriers and their attorneys should also keep in mind that a policyholder's cooperation is crucial in cyber subrogation claims because they need so much information with respect to the IT systems, the software that's in use and the third-party vendors, Maleski said.

A lot of times the insured or their employee may just feel "embarrassed if they fall for a spoofing or a phishing attack," the partner said, so an insurer should soften their approach when communicating with the policyholder.

"We've had cases where the IT department was basically afraid they were going to get fired. They think they could lose a job if they cooperate too much," said Ronald Menold, an FBI veteran and director of cybersecurity firm Cosecure who works with Cozen O'Connor on cyber subrogation claims. He served as one of the panelists during Tuesday's webinar.

Insurers and their counsel should not "come on too aggressive and come on speaking with a bunch of legalese," Maleski cautioned. "You want to play with it almost the same way you would with a crime victim, because they are."

--Editing by Bruce Goldman.