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

Apple, Cisco Venture Could Fuel Cyberinsurance Market Surge

By **Jeff Sistrunk**

Law360 (February 9, 2018, 7:11 PM EST) -- Apple and Cisco recently announced they are teaming with two insurers to offer discounted cyberinsurance policies for companies that use the tech giants' products to help guard against digital threats, a partnership that experts say could spur the sale of cyber coverage among reluctant businesses scared off by high premiums and daunting deductibles.

The "industry-first offering" is designed to provide a "holistic" approach to cyberrisk management, according to a Monday news release by the partners, which also include global risk consulting firm Aon PLC and insurer Allianz Global Corporate & Specialty, or AGCS.

Businesses looking to buy the policy offered by Allianz will have to undergo an assessment of their cybersecurity posture from professionals at Aon, who will then recommend ways to improve their cybersecurity defenses, according to the news release. Interested customers will also be expected to use Cisco Systems Inc.'s Ransomware Defense product or qualified Apple Inc. products such as iPhones and iPads, which Allianz has determined offer a "superior level of security," the release said.

Clients that have "appropriate resiliency postures" may qualify for certain coverage "enhancements" such as lowered or waived deductibles, according to the release. Customers could also see the cost of purchasing certain security products applied against a deductible in the event of a claim, and will get access to Cisco and Aon's incident response teams in the wake of a malware attack, Emy Donovan, Allianz's cyber head, said in a video posted on Cisco's website that explains the new partnership and insurance offering.

According to experts, the incentives tied to the new insurance product could encourage companies that have previously spurned cyber policies due to high deductibles or premiums to sign up for the coverage. Depending on a company's size, annual premiums can easily exceed $10,000, and many policies have deductibles of $100,000 or more for data breach response and other costs.

Matt Cullina, the CEO of information security provider CyberScout, characterized the incentives as a "cyber carrot" to encourage businesses to improve their overall data security safeguards.

"Deductibles are very significant in cyber — it's not like your auto policy where you have a deductible of $500," Cullina said. "They can be in the tens of thousands, hundreds of thousands of dollars, or even millions, particularly around incident response, where you are most frequently seeing claims."

Cullina said that, while awareness of cybervulnerabilities has increased in recent years with the proliferation of high-profile, multimillion-dollar data breaches, some businesses still hold a "not in my backyard" attitude.

"Even though [businesses] may have done a ton of investment in data security or training, there is still that false sense of security, so getting them to take action through incentives is the only way to move the needle," he said. "This looks like the right piece of leverage to get businesses to take action without doing much extra."

Joshua Gold, co-chair of Anderson Kill PC's cyberinsurance recovery group, said the new insurance product's incentives could complement stringent cybersecurity regulations to galvanize businesses to shore up their protections.

Last year, New York's Department of Financial Services blazed a trail by enacting first-of-their-kind cybersecurity rules requiring insurers, banks and certain other institutions to develop detailed data security programs and report breaches within 72 hours, among other measures. Inspired by the Empire State's framework, known as Regulation 500, the National Association of Insurance Commissioners — the standard-setting body composed of all the states' insurance regulators — in October adopted a data security model law to serve as a template for other states to develop their own data security directives.

"Generally speaking, both the incentives and the deterrents are useful to get organizations and individuals keeping up with their cyberhygiene and making it more difficult for criminals to access computer systems in order to steal information or inflict damage," Gold said.

In addition, the new cyberinsurance partnership could help generate a substantial amount of data about companies' cybersecurity practices and claims histories, which could aid in the development of future policies, according to experts.

"The thing that struck me is that the insurance industry should be one of the largest repositories of cybersecurity details, risks and losses. I have long thought the industry should put that knowledge to use to help policyholders," said Barnes & Thornburg LLP partner Scott Godes. "To the extent they are putting their collective knowledge to use, in terms of tracking trends in cyberincidents and claims, that should be good for the insurance industry and policyholders, if done the right way."

The new cyberinsurance is designed to help Apple and Cisco customers better manage and protect themselves from risks associated with ransomware and other malware-related threats, which are currently the most common threats faced by organizations. Malware is now being used in more than half of all breaches, while ransomware has transformed into a "billion-dollar business," Cisco Chief Information Security Officer Steve Martino said in the introductory video on the company's website.

Participating companies will need to have deployed Cisco Ransomware Defense, which leverages threat intelligence from the company to identify threats and block them, or a range of Apple products. These include the iPhone, iPad and Mac, which have features such as always-on hardware encryption, support for secure networking protocols, and operating systems that tightly integrate hardware, software and services to ensure each component is trusted, according to the partners' announcement.

"For them to focus on Cisco's malware and ransomware software is the right angle, because that will help mitigate or eliminate a ton of claim risk," Cullina said. "Apple, because of its closed systems, has always been known to be more secure than a Droid device. They are nudging businesses along to say,

'Hey, maybe Apple wasn't your mobile business solution in the past, but you should think about it, and by the way, they have a bunch of additional features on there for privacy and security.'"

And companies that are already using Cisco software and Apple devices may have a fairly easy route to qualifying for the policy enhancements.

"A company may already have Cisco in their shop and be using Apple devices, so it probably wouldn't take much extra effort for them to take that [Aon] assessment and get that deductible reduction, and then they would be in a better position when a claim arises," he said.

However, some insurance attorneys told Law360 they had a few reservations about the new product. The terms and scope of the policy being offered were not specified in the news release or on the partners' websites, and an Allianz spokeswoman said she couldn't offer additional details on the coverage beyond the contents of the release.

"I like the idea of this partnership between the insurance and technology industries, in theory," Gold said. "Like so much in the realm of cyberrisk management, the proof will be in the actual terms of the protection. There is already a lot of high-quality insurance out there, as well as a lot of low-quality insurance about. If the coverage offered is high-quality, it would be excellent to couple that with tech industry-led tailored cybersecurity for the policyholder."

Farella Braun & Martel LLP partner Tyler Gerking said it is possible that a company that buys the new protection could face a coverage denial in the event of a data breach if it fails to consistently utilize the Cisco software and Apple products. Some other carriers' policies bar coverage if the policyholder fails to maintain specified data security measures, he noted.

"It may be that these requirements increase the risk of the insurance company being able to deny coverage," Gerking said.

Gerking added that a coverage trapdoor could also potentially arise if a policyholder's employee is hacked on a non-Apple device while working from home.

"I could see this environment being a little more restrictive," he said. "If all employees are supposed to be on Apple IOS, and one employee is using Windows to do work at home, what happens then? I wonder how far the restrictions would extend out. Would it be easy for a company to get tripped up and inadvertently void coverage?"

--Additional reporting by Allison Grande. Editing by Katherine Rautenberg and Catherine Sum.
