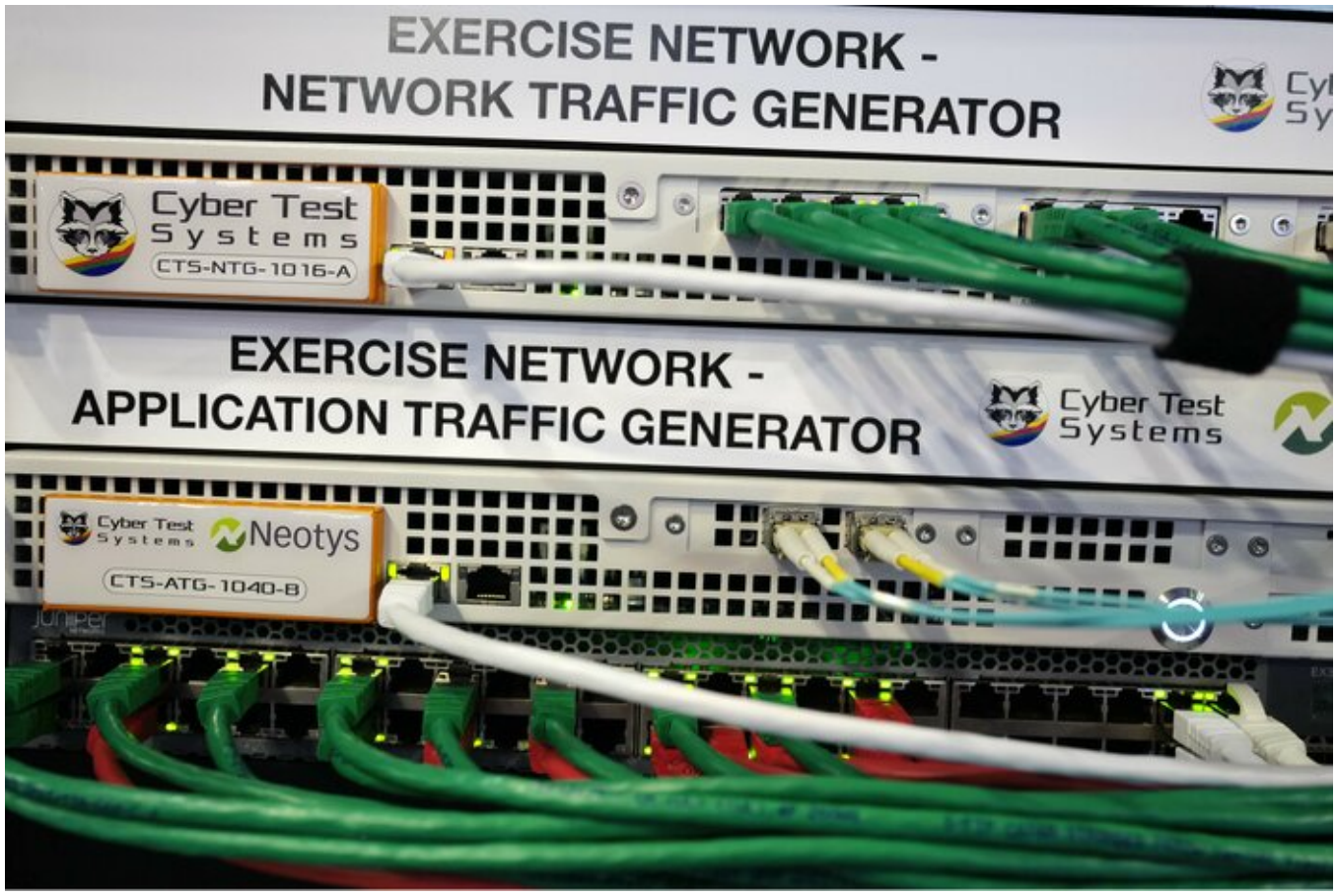
LAW360 Insurance Authority

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

Anderson Kill Managing Shareholder Talks Cybercrime Losses

By **Daphne Zhang**

Law360 (April 22, 2022, 9:01 PM EDT) -- Businesses continue to experience multimillion-dollar losses from ransomware, wire fraud and phishing attacks. While some policyholders have found remedies through crime insurance, most insurers argue that cyberthefts are intangible and not a so-called direct loss covered by the policy.



While insurance companies contend that cybertheft is not defined as a direct loss or covered by a crime insurance policy, Anderson Kill's Pamela Hans says many courts aren't buying that argument. (AP Photo/Michel Spingler)

Pamela Hans, a managing shareholder of Anderson Kill's Philadelphia office, told Law360 that most courts have found that cybertheft constitutes a direct loss covered by a crime insurance policy. But she cautioned that policyholders need to carefully read their policy language and work closely with brokers when getting the policy and handling a cyberloss.

This interview has been edited for length and clarity.

What kind of cyberlosses are covered under crime insurance?

Pamela Hans

Many crime policies do cover cyberlosses. Courts have been looking at the policy precondition of a direct loss to determine coverage. Insurance companies are saying cybertheft, like spoofing and various frauds, is not defined as a direct loss or covered by the crime policy. They are saying a crime policy only covers a theft that happened immediately in time and that a cybertheft which requires multiple steps, such as manipulation of a computer system, sending and receiving an email, and wiring or transferring funds to fraudsters, is not a direct loss covered by the policy.

Courts have not uniformly accepted that argument. The majority of courts are finding in favor of coverage under a crime policy for cyberlosses as direct loss. They are looking at how to determine whether a loss is direct and examining the proximate cause. In American Tooling Center Inc. v. Travelers Casualty and Surety, the court reviewed an unbroken chain of events that led to the theft and determined what constituted direct loss. A couple of courts, certainly in the minority, have said "direct" must mean immediate in time. So any meaningful delay between the initial cybercriminal's act makes it not a direct loss. Cybertheft is not as simple as a bank robbery, but involves a series of events executed from far away that ultimately leads to theft of funds.

What other cyberlosses have courts said are covered by crime policies?

All different kinds, such as phishing, spoofing and other types of fraud. There have been cases where a bad actor impersonated a principal of a company by tweaking the email and then presented themselves as the boss and told the employees to take certain steps to transfer funds. Courts have held that that was a covered loss under a crime policy.

Have you seen any insurers putting different kinds of cyber exclusions in their crime policies?

Some policies have specific exclusions for cybercrime. So there may be limited coverage or no coverage at all by the policy form itself, or an endorsement to further narrow coverage. Insurance companies have the ability to add endorsements to specifically and cleanly exclude cybertheft. But they do not always do that. However, carriers that do not have the exclusions still try to argue that cybertheft is not covered. From my experience as a coverage litigator for 20 years, the larger a loss, the more an insurance company looks to deny coverage.

Policyholders need to look carefully at the exclusion language and definition of policy terms such as "asset," "funds," "on the premise" and determine, for example, whether an alteration of an email address due to hacking is an alteration of property. Some insurance policies define physical assets as tangible assets.

What other challenges do policyholders face when trying to get cyber coverage under crime policies?

Insurance companies are not necessarily jumping at the chance to insure cyber-risks. Policyholders need to pay close attention to the policy limits being offered in relation to the premium and their business risks. They should look at internal system controls to prevent cyberattacks and also counterparties' risks and how their business partners' cybervulnerabilities may impact their own network.

Insureds need to think about the different ways to transfer those risks through insurance, as well as their contracts with vendors and business partners to see who bears the risk of a cyberloss. They should look over how their contracts protect them from potential cyberlosses. And if your business partner has a problem with their network, do they have insurance that will cover your loss? It's not as simple as just asking, "Do I have enough insurance?"

What is your advice for attorneys who represent policyholders on cyberloss in crime policies?

First and foremost, understand the policy language. Second, understand the facets of a loss and the clients' business. And work closely with your insurance broker to maximize insurance recovery in any loss. Brokers are often an overlooked resource when an attorney is assisting a policyholder to recover a loss. At the end of the day, understand what the courts have said about the policy language and how they determined if a loss is a direct loss or not.

Don't automatically think that because there are several steps between the entry of the thieves and the exit of the funds that it wasn't a covered direct loss. The most important thing for any policyholder advocate is to always keep in mind what is your client's objective. Is it to make sure there's 100% of the insurance dollar paid in full no matter what, or is there a business solution to the problem? What are your client's objectives in resolving a claim? Does your client want to maintain relationships with their business partners after a cyberattack or not?

--Editing by Emma Brauer.
