Nicole S. Adams-Hess
HESS • BOWER • ADAMS-HESS, PC

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
November 2022

Maximizing coverage under cyber-insurance policies

CYBER INSURANCE IS RELATIVELY NEW AND POLICIES HAVE NOT BEEN WIDELY INTERPRETED BY THE COURTS

Cyber-insurance policies are a relatively new invention, and widespread adoption by policyholders has occurred even more recently. Cyber-insurance policies provide coverage for 21st century risks — with the majority arising out of the perils made possible by the internet. Most commonly associated with data breaches and wire fraud, cyber-insurance policies can provide significant protection. These policies can be an asset, but with a dearth of published opinions interpreting them as well as complexities and variances in policy forms, policyholders must advocate for themselves to maximize their protection and recovery. This article will provide an overview of the types of coverage provided by cyber policies, how a cyber policy has been interpreted by the Ninth Circuit, and practical advice on how to prepare for cyber crime and navigate cyber losses.

Overview of cyber-insurance policies

Cyber-insurance policies typically provide both first- and third-party insurance coverage. Policyholders have the option of purchasing a stand-alone first- or third-party cyber-insurance policy, but it is generally advisable to buy both coverages. First-party coverage provides indemnity coverage for a loss sustained by the insured, like a property-insurance policy. Third-party coverage provides defense and indemnity coverage for liability claims made against the insured, like a general liability policy. A cyber policy's first-party coverage generally provides coverage for a wide range of cyber threats, ranging from data breaches, malware attacks, phishing, and wire transfer fraud. In the event of a data breach, a first-party policy will respond by indemnifying the insured for the costs of investigating the cause of the loss, notifying customers, and complying with regulatory obligations.

First-party cyber coverage may also indemnify loss due to cyber crime. One of the most common types of cyber crime is known as "Social Engineering Fraud." This is a term of art characterizing a type of cyber crime where a fraudster impersonates a legitimate person to trick someone else into parting with money, stock, or other property. This coverage has become extremely important as Social Engineering Fraud has become more common and sophisticated in recent years.

Social Engineering Fraud

Social Engineering Fraud can be accomplished through different methods of deceit. The most common Social Engineering Fraud horror story is that of an employee who has been tricked into wiring thousands (and sometimes millions) of dollars to a criminal who, using a fake email address, posed as a company executive or vendor requesting a payment. Sometimes, a hacker can intercept legitimate wiring instructions sent by email, substitute their own banking information, and send the forged email back to the intended recipient. The recipient has no idea the email has been hacked, and instead of sending the funds to the legitimate recipient, sends it to the criminal following the forged wiring instructions.

Other fraudsters accomplish the crime by creating an email address that is very similar to a legitimate email address. The fake email address contains only minor differences from the legitimate email address, such as changing one letter or making a word plural so that a recipient is not likely to notice it is fraudulent. People suffer losses due to Social Engineering Fraud each day. The first-party coverage sections of a cyber policy can provide insurance coverage to compensate the policyholder when they become a victim of Social Engineering Fraud.

Third-party cyber coverage

Third-party cyber coverage operates like an errors and omissions or traditional malpractice policy. Cyber policies that offer this coverage are written on a manuscript basis and generally provide coverage for claims made against the policyholder arising out of cyber events, such as data breaches, for which they are alleged to have caused damage to third parties. Some cyber policies offer expanded liability coverage to insureds in the internet, technology, broadcast, or other industries. Some policies even provide coverage for claims of violating another's intellectual property, which is a risk excluded by most other insurance policies. Third-party liability coverage sections in cyber policies are highly specialized and customizable – working with a sophisticated broker, a policyholder can procure a policy that is tailored to respond to its specific concerns.

A cyber policy may provide both first- and third-party coverage for claims arising out of a single data breach. For example, if a company suffers a data breach exposing the personal identifying information of its customers, its cyber-insurance policy should provide it with first-party coverage to investigate the loss and notify the customers and also third-party defense and indemnity coverage in response to any claims or lawsuits brought by those customers affected by the data breach.

The main issues with cyber coverage policies

In theory, cyber policies should respond to a majority of internet-related claims. In practice, insurers utilize the paucity of cyber-insurance-specific case law to their advantage. Additionally, cyber policies do not have the benefit of refinement by decades of court decisions interpreting various clauses. As a result, cyber-policy provisions can have more uncertainty than those found in a more traditional insurance policy. Cyber policies are not written on a standard form, but are individually drafted by each insurer. There can even be variances in policies issued by the same insurance company. Cyber-insurance policies are complex, convoluted jumbles of defined terms sending the policyholder back and forth through the policy trying to make sense of it all. Even the most experienced

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
November 2022

coverage attorney struggles with understanding the actual scope of coverage provided by these policies.

Making the policies even more difficult to comprehend is that the policy forms often contain the coverage grants for policy provisions that were not purchased by the insured. While this is not unseen in some other management-liability policies, it is important that the policyholder check the declarations page to determine if it purchased a certain type of coverage. The declarations pages – the part of the policy that lists out the types and limits of coverage purchased as well as the premium paid – are found in the beginning of the policy. Just because a coverage grant is printed in a policy does not mean that it was purchased by the policyholder. It is important to review the declarations pages to see what coverages have been purchased, as well as what the limits and sublimits in the policy are.

Sublimits. Gotcha!

In what seems to be a response to the increase in Social Engineering Fraud claims, many insurers have introduced lower sublimits. Policies that provide $1,000,000 in coverage for other parts may provide limits as low as $50,000 or $100,000 for Social Engineering Fraud claims. Policyholders experiencing a Social Engineering Fraud loss may find themselves with cyber coverage, but with insufficient limits to make themselves whole.

Ernst and Haas Management Company, Inc. v. Hiscox

In a recent Ninth Circuit decision, *Ernst and Haas Management Company, Inc. v. Hiscox, Inc.* (9th Cir. 2022) 23 F.4th 1195, the court broadly interpreted a cyber-insurance policy's "Computer Fraud" and "Funds Transfer Fraud" coverage sections to afford coverage. The facts of this case are simple and common. A fraudulent actor impersonated the managing broker of Ernst, David Haas, and emailed an Ernst accounts-payable employee with instructions to pay an invoice for $50,000. The imposter sent another fake invoice by email for payments of $150,000 and $470,000 to the accounts-payable clerk. Believing the emails to be from the real managing broker, the accounts-payable employee caused the $50,000 and $150,000 invoice to be paid to the imposter. Upon receiving the $470,000 invoice, the accounts-payable clerk became concerned and contacted the real David Haas, who advised her that the emails she had been receiving were a scam and instructed her to not pay the $470,000 invoice. Unfortunately, the $200,000 that had already been wired to the imposter could not be recovered. Ernst and Haas tendered the claim to its cyber insurer, Hiscox, requesting coverage.

The policy language

The Hiscox policy contained two potentially relevant coverage grants, Computer Fraud and Funds Transfer Fraud. The subject policy defined these coverages as follows:

> (1) Computer Fraud
> [The insurance company] will pay for loss of or damage to [currency, coins, bank notes, bullion, checks, money orders], [negotiable or nonnegotiable instruments or contracts representing either currency, … or property], and/or [any other tangible property] resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the [interior of any building Ernst or a subsidiary occupies in conducting Ernst's business] or [the interior of that portion of any building containing a financial institution or similar safe depository]:
> i) To a person (other than [Ernst, a Partner, a Member, or an Employee]) outside [the interior of any building Ernst or a subsidiary occupies in conducting Ernst's business] or [the interior of that portion of any building containing a financial institution or similar safe depository]; or
> ii) To a place outside [the interior of any building Ernst or a subsidiary occupies in conducting Ernst's business] or [the interior of that portion of any building containing a financial institution or similar safe depository].
>
> (2) Funds Transfer Fraud
> [The insurance company] will pay for loss of [currency, coins, bank notes, bullion, checks, money orders] and [negotiable or nonnegotiable instruments or contracts representing either currency, … or property] resulting directly from a [Fraudulent Instruction] directing a financial institution to transfer, pay or deliver [currency, coins, bank notes, bullion, checks, money orders] and [negotiable or nonnegotiable instruments or contracts representing either currency, [etc.], or property] from [an account maintained by Ernst at a financial institution from which Ernst can initiate the transfer, payment, or delivery of [currency, coins, bank notes, bullion, checks, money orders] or [negotiable or nonnegotiable instruments or contracts representing either currency, [etc.], or property]].

Ernst and Haas took the position that both of these coverage grants provided coverage for the $200,000 loss. Hiscox disagreed and asserted that the loss did not "result directly" from the fraud. The district court agreed with Hiscox. The Ninth Circuit reversed, finding that the district court had erroneously relied on an inapplicable, unpublished decision involving embezzled funds authorized for payment (and not stolen by fraud), too narrowly, construed the Computer Fraud coverage to hacking or unauthorized access of the insured's computer, and improperly determined that Funds Transfer Fraud coverage did not apply when fraudulent instructions were given to an employee.

The Ninth Circuit ruling

The Ninth Circuit determined that Ernst and Haas suffered a "direct loss" as a result of the fraudulent emails. The court explained that Ernst and Haas suffered a direct loss when the accounts-payable clerk caused the funds to be transferred to the imposter. The court rejected the argument that the accounts-payable clerk's conduct was an intervening act, and instead found that

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
November 2022

the fraudulent email directly caused the loss: "Ernst immediately lost its funds when those funds were transferred to [to the imposter] as directed by the fraudulent email. There was no intervening event – Allen [accounts-payable clerk] acting pursuant to the fraudulent instruction 'directly' caused the loss of the funds." (*Ernst and Haas Management Company, Inc. v. Hiscox, Inc.*, 23 F.4th at p. 1202.)

The court also found that the policy's Funds Transfer Fraud coverage clause applied. The court evaluated the policy language and determined that its plain language provided coverage for losses caused by fraudulent instructions initially received by an employee. Although the policy stated that it covered loss resulting directly from a fraudulent instruction "directing a financial institution" to transfer funds, the court explained, "Either type of fraudulent instruction that results in 'directing' a financial institution to transfer funds is covered by the policy." (*Id*. at 1202.)

The *Ernst and Haas* decision provides a roadmap to policyholders to secure coverage for Social Engineering Fraud claims under their cyber-insurance policies. These coverage grants should be interpreted broadly in favor of coverage, especially when it comes to defining the scope of "direct loss." This decision reminds insurers that the guiding tenets of California insurance law apply to cyber policies. (See *MacKinnon v. Truck Ins. Exch.* (2003) 31 Cal.4th 635, 648) [Grants of coverage are liberally construed and exclusions are strictly construed to maximize coverage and protect the policyholder].) It also reminds policyholders that more than one coverage section in a cyber policy apply to a single loss, and that they should challenge insurer denials based on narrow constructions of coverage grants.

What to do before a loss

The best time to prepare for a cyber loss is before it happens. Having paid numerous claims, many cyber insurers are now implementing loss controls requiring that certain security measures be in place before issuing a policy and denying claims if those security measures are not in place at the time of a loss.

Required loss controls may include procedures that prevent fraudulent wire transfers, which also benefits the policyholder. Such procedures may include prohibitions on sending wire instructions initiated by email without a confirming phone call. While hackers only continue to become more sophisticated and there is no guaranteed method of preventing fraud, a two-step authorization before initiating wire transfers will reduce fraud.

The broker makes a difference

Having a knowledgeable insurance broker can also help prepare for a cyber event. Not all brokers have access to the same markets, and not all brokers have expertise in the types and scope of coverage on the market. It is advisable to retain a broker with an understanding of the relevant business sector and cyber insurance. This broker can have a conversation with you about industry risks, the risks your specific business is exposed to, and the insurance products available. Detailed written correspondence with your broker will provide them with a clear understanding of your concerns and requests, as well as provide a record of the coverage you requested if the policy issued does not match that request. In this circumstance, the policyholder may have a claim against the insurer and/or the insurance broker.

Social Engineering Fraud coverage is now often an optional coverage that must affirmatively be selected by the insured for additional premium. This premium is not always significant, but Social Engineering Fraud coverage should always be purchased unless there is a well-grounded decision to decline it. There are very few, if any, circumstances where an insured should decline Social Engineering Fraud coverage if purchasing a cyber policy. This may take place if the premium is prohibitively expensive, the insured is confident in its loss controls, and the insured is willing to bear the risk of this type of fraud.

Mitigating after a loss

In the unfortunate circumstance that you or a client suffers a cyber loss, immediately notify the cyber insurer. The cyber policy may provide resources that can immediately help with legal, regulatory, and notification requirements and indemnification. Most cyber-insurance policies have strict reporting requirements that require timely reporting. For coverage to apply, most policies require that the loss be suffered during the policy period, and also reported during the policy period or within a 30-, 60-, or 90-day grace period following the policy. Forfeitures of coverage due to late reporting are an unearned windfall by the insurer. Unfortunately, California case authority permits this harsh penalty in most circumstances. To be safe, be sure to report a cyber claim immediately – not only to obtain benefits to assist with navigating the loss, but also to ensure entitlement to those benefits.

Conclusion

Cyber-insurance policies provide important protections for internet-based risks. The best practice is to procure a cyber policy with a knowledgeable broker with access to a variety of insurers. With the benefit of cyber loss procedures in place to avoid becoming victim to cyber crime, coupled with a robust cyber policy, a policyholder will be better prepared for the risks of the 21st century.

Nicole S. Adams-Hess is a shareholder with Hess • Bower • Adams-Hess, PC. *Her practice focuses on obtaining insurance recoveries for individuals, non-profits, public entities, and corporate policyholders under all types of insurance policies. She also litigates insurance bad-faith cases. Ms. Adams-Hess is a graduate of Santa Clara University School of law and earned her undergraduate degree at the University of California, Berkeley.*