Steps to Take Before a Loss to Get a Cyber Insurance Claim Paid

Tips for pursuing coverage for damages and liabilities stemming from a cyberattack.

By **Luma S. Al-Shibib and Steven J. Pudell** | September 28, 2021

This year has seen an escalation not only in ransomware attacks – the chief current headline-grabbers – but also in other forms of cyberattack, including evolving and ever-more sophisticated phishing schemes. Indeed, the 2021 Verizon Data Breach Investigations Report (//enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf), released in May, found a 6% increase in ransomware attacks and an 11% increase in phishing schemes over the last year. More than ever, cyber insurance liability policies have become a critical part of a business's insurance program.

Simply purchasing a cyber policy with sufficient limits is not enough to secure protection, however. Cyber policies are often mined with requirements and conditions to coverage that insurance companies commonly invoke to deny or reduce coverage. Maximizing coverage requires vigilance before an incident occurs and throughout the claims process. The five steps outlined below will help your business reduce its potential exposure and maximize its insurance recovery in the event of a cyberattack.

Shore Up Vulnerabilities in your Cyber Security System

Although the need to regularly evaluate and enhance your cyber security infrastructure may seem like a basic proposition, it is an important step not only in preventing attacks, but also minimizing damage in the event your business does experience one. For example, a system built as a "flat" environment and without segmentation is more vulnerable to damage than a system with a hierarchical infrastructure. A cyber-attacker who gains entry into a "flat" environment can move freely through and access the entire system. An elevated, segmented system, with multiple firewalls and various security enhancements, can minimize and contain the damage.

From an insurance recovery standpoint, the less updated your security infrastructure, the more likely the insurance company will argue that measures undertaken to recover from the attack – regardless of how necessary they are to restore your operations – constitute system "upgrades," "enhancements," or "improvements" which may not be covered under your cyber policy.

Read Your Policy

Ideally, you should do this before you suffer a cyberattack to find out not only what specific types of coverages your cyber liability insurance policy provides, but also to identify any conditions you need to fulfill in order to obtain coverage. You should be able to understand your policy. When you suffer an attack, re-read your policy **before** taking any steps to make sure that you are complying with any requirements under the policy.

Review your non-cyber policies as well, as these may provide additional sources of coverage for cyber-related losses. Such potential coverage may be found in your first party property policy, your D&O policy, and your crime insurance policy. For example, a crime insurance policy may cover the ransom paid to attackers to release access to your system, files, and information as a result of a ransomware attack. *See G&G Oil Co. of Indiana, Inc. v. Cont'l Western Ins. Co.*, No. 20S-PL-617, 2021 WL 1034982 (Ind. Mar. 18, 2021) (concluding that ransomware payment might be covered under crime policy's "computer fraud" provision even though policyholder denied policy extension for computer hacking and virus coverage, and remanding the case back to trial court).

Find Out if You Need to Hire a Pre-Approved Cyber Consultant

Cyber insurance policies may only cover cyber investigation, restoration, and recovery costs that are incurred through the use of insurer-approved cyber security professionals. Before hiring any outside cyber consultants or performing any forensic investigatory, restoration, or recovery work on your system, check your policy to determine whether it requires you to select a cyber-consultant from a pre-approved list of insurer-designated consultants. Some policies allow the policyholder to hire a cyber-consultant that is not on the insurance company's list of designated professionals, but only with prior written approval from the insurance company. If you hire someone not on the insurance company's pre-approved list of cyber professionals, and fail to obtain the insurance company's advance written approval for the retention, the insurance company likely will use this as a basis to deny or reduce coverage for your claim.

Mitigation

Just because the policy requires you to mitigate damages from a cyberattack, do not assume that the insurance company will agree to cover your mitigation costs. If the policy does not explicitly say that it covers mitigation costs, it is likely that the insurance company will use this as a basis to argue that costs incurred to mitigate the effects of the cyberattack are not covered (unless you can otherwise show that they are covered under an explicit coverage grant within the policy). For example, if you use your own IT and cybersecurity salaried-employees to respond to an attack, the insurance company may refuse to cover the employees' salaries for the time when they were responding to the attack, and it may argue that it has no obligation under the policy to cover employee salaries because those are part of the policyholder's normal operating expenses and would have been incurred in the absence of the cyberattack. The insurance company may claim such costs are not covered even though your IT employees are working exclusively to respond to and recover from the cyberattack and are not otherwise performing their regular tasks and duties. Additionally, the insurance company may decline coverage even though the use of your own employees ultimately reduces your cyber-related losses (as well as the insurance company's potential exposure) and allows you to resume operations faster because of your employees' familiarity with your system and their ability to commence breach response immediately.

Do Not Assume that the Insurance Company Is Operating to Protect Your Interests

One common policyholder mistake is to assume that insurance companies' interests are aligned with those of their policyholders. Assume rather that the goal of insurance companies is to maximize their profits, and that they will deploy every coverage defense and policy exclusion available to reduce their payouts.

In the context of cyber liability insurance specifically, the insurance company may require you to hire a forensic accountant or cyber claims consultant from their designated list of valuation experts to assist in valuing your cyber claim. In such instances, do not assume that the insurance-company-recommended expert represents your interests. That valuation consultant's loyalty likely will be to the insurance company, which represents a source of repeated business and revenue stream to the consultant, and not you. If you find yourself in that situation, it is best to retain your own independent professional, skilled in cyber liability insurance claims, to counsel you in your dealings with both the insurance company and the third-party valuation consultant.

It is likely that insurance will be the last thing on your mind, or certainly not at the top of your list, when you have suffered a cyberattack. This is why it is important to plan ahead, educate yourself, and know and understand your rights and obligations under your cyber policy now, so that you are better able to protect your business in the event it ever experiences a cyberattack.

Luma S. Al-Shibib (https://www.andersonkill.com/People/Luma-S-Al-Shibib), a shareholder in the New York office of Anderson Kill P.C., focuses her practice on insurance recovery for corporate policyholders, with an emphasis on directors & officers, general liability, and cyber liability insurance.

Steven J. Pudell (https://www.andersonkill.com/People/Steven-J-Pudell) is the managing shareholder in Anderson Kill P.C.'s Newark, NJ office. His practice concentrates on insurance recovery on behalf of clients including food industry companies, chemical manufacturers, pharmaceutical companies and real estate developers.

Editor's Note: These views are the author's own.