Lawyer Insights

Cyber Insurance Lessens the Sting of Corporate Cyber Attacks

By Andrea DeField
Published in Bloomberg Law | October 11, 2023

The average cost of a data breach has risen to an all-time high of $4.45 million globally and $9.48 million in the US. Cyberattacks are growing in frequency and severity as regulatory requirements, particularly for public companies, continue to increase.

Fortunately for executives, a robust insurance program can mitigate the fallout from a cyberattack. Cyber insurance should be an organization's first line of defense against cyber risks. These policies comprehensively respond to cyber risks and provide both "first party" and "third-party" coverage.

First-party coverage typically reimburses a policyholder for costs incurred and losses suffered as a result of the cyberattack. First-party coverage generally includes:

- Breach response costs of hiring legal and forensic IT vendors to investigate the cause, scope, and extent of the attack; determine whether confidential information has been accessed; and contain it
- Business interruption costs, including lost profits while the policyholder's attacked systems were down and expenses to restart or continue business as close to normal during the incident
- Lost profits incurred as a result of cyberattacks on a key vendor or supplier's system
- Cyber extortion expenses, such as ransom demands, and costs to retain an extortion specialist
- Digital asset and information restoration costs to restore or rebuild stolen or destroyed data
- Public relations and crisis communications expenses and costs associated with reputation loss
- "Bricking" costs of replacing computers and other hardware made useless by malware

For privacy breaches, first-party policies also cover the costs of counsel to advise on legal obligations, vendors for notification to impacted individuals, call-centers, and identity theft or credit monitoring.

Third-party coverage, in contrast, helps fend off claims against the company, directors, or officers including third-party lawsuits or regulatory actions, and investigations. These policies should cover defense costs, settlements, and other costs arising out of third-party claims; regulatory investigations and formal actions; and, in some cases, costs associated with media or intellectual property wrongful acts involving the internet, such as those arising out of a company's website or social media.

Cyber Insurance Lessens the Sting of Corporate Cyber Attacks
By Andrea DeField
Published in Bloomberg Law | October 11, 2023

Many third-party policies cover payment card industry data security standards investigations, fines, and penalties, as well as technology errors and omissions for third-party claims alleging wrongful acts by the company or its employees, directors, or officers in providing internet or technology services.

Companies should audit their insurance programs holistically to determine complimentary coverage for cyber risks on traditional insurance policies. For example, many directors and officers policies lack broad cyber exclusions and may respond to lawsuits arising out of a cyberattack. This coverage can be important if the company exhausts the limits of its cyber insurance policy after an attack and can help defend against lawsuits that trigger the D&O insuring agreement.

For fraudulent transfers, the company's crime insurance policy should respond. And, for certain data restoration expenses, executives should review property and crime policies to determine if a cyber or other endorsement may offer some limited coverage.

Having a cyber insurance policy isn't enough to ensure the robust coverage that's needed to recover from a cyberattack because policies aren't one-size-fits-all. Companies should consider the following when renewing their cyber insurance plans:

Pre-approve key vendors. When a cyberattack occurs, companies must retain appropriate outside vendors quickly to contain the attack. This includes legal counsel, IT forensics, public relations, and potentially an extortion specialist, among others.

Most cyber insurers require policyholders to use panel vendors or other pre-approved vendors. Companies can avoid a coverage fight over vendor approval (and rates) in the critical hours following a cyberattack by ensuring they have the vendors they want on the policy.

Have complementary incident response. Organizations should ensure that the pre-approved vendors (or those on the insurer's panel) match those vendors identified in the company's cyberattack response plan and ransomware playbook.

Avoid or narrow cyber exclusions. These exclusions are often overly broad and usurp coverage that otherwise should be available. For example, public company D&O policies should still respond to securities claims arising out of a cyberattack, even if the policies otherwise wouldn't respond to consumer claims based on disclosure of personally identifiable information.

Cyber exclusions shouldn't be so broad as to affect coverage for what would be an otherwise covered claim. Cyber policies typically don't cover property damage; however, this may be a major risk for certain companies, particularly with internet-of-things risks. Companies should ensure the risk is picked up on other policies like property, commercial general liability, or pollution insurance policies.

Executive officers, risk professionals, in-house legal counsel, and in-house IT must work together before a cyberattack occurs to ensure all teams are on the same page about incident response and how cyber (and other types of) insurance will respond. Analyzing each line of coverage will help ensure that the company's insurance program adequately responds to a company's unique cyber risks.

Cyber Insurance Lessens the Sting of Corporate Cyber Attacks
By Andrea DeField
Published in Bloomberg Law | October 11, 2023

Andrea DeField, *is a Partner in the firm's Insurance Coverage group in the firm's Miami office. Andrea finds risk management, risk transfer, and insurance recovery solutions for public and private companies. She can be reached at +1 (305) 810-2465 or adefield@HuntonAK.com.*