US Law Week

Looking for Cyber Insurance? Legal Terms, Issues to Know

By Michelle Kisloff, Jasmeet Ahuja, and Andrew Bank

Sept. 17, 2021, 4:01 AM

The impacts of cyber and ransomware attacks on companies can be devastating, and companies seeking to mitigate these risks are shopping for stand-alone cyber insurance policies. Hogan Lovells privacy and security litigators examine what companies should know and understand when looking for a policy.

A surge in cyber and ransomware attacks is costing companies millions of dollars and causing immense reputational harm, increasing the costs of and requirements for cyber insurance coverage at a time when companies need it more than ever.

In 2020, ransom payments from companies increased more than 300% compared to the prior year and totaled north of $350 million. This trend is holding in 2021, as cybercriminals take advantage of confusion and vulnerabilities exposed or exacerbated by the ongoing pandemic. Because the impacts of cyber and ransomware attacks can be devastating, companies seeking to mitigate these risks are shopping for standalone cyber insurance policies.

There are several key considerations to keep top-of-mind when choosing a policy or obtaining additional coverage.

What Is Cyber Insurance?

Traditional insurance policies were not designed to cover many of today's cyber risks. Such policies—e.g., commercial general liability, professional liability, errors and omissions, directors and officers, and kidnap and ransom—typically do not contain express grants of coverage for those risks. And in recent years, insurers have added cyber-related exclusions to certain policies and/or modified policy language to disclaim coverage for cyber risks.

To avoid uncertainty about where companies can find coverage for cyber risks, insurers are offering increasingly robust standalone cyber policies. Cyber policies manage insureds' potential exposure from, for example, data breaches, ransomware attacks, theft or loss of unencrypted assets, insider threats, denial-of-service attacks, supply chain cyberattacks, business email compromise, exploitation of cloud misconfigurations, and other nation-state and criminal cyber activity.

The scope of cyber policies can vary considerably, and companies should regularly review their insurance arrangements to ensure adequacy of coverage as the cyberthreat landscape evolves.

In light of the evolving cyber risk landscape, insurance carriers also are re-evaluating how much coverage they can afford to offer, taking a closer look at insureds' cybersecurity programs, and raising premiums by as much as 30% or more annually, according to a study by the U.S. Government Accountability Office.

What Does Cyber Insurance Cover?

Comprehensive cyber insurance policies generally cover both first- and third-party losses.

First-party coverage protects against damage and loss to the insured directly, including coverage for:

1. Post-incident forensic investigation;
2. Data retrieval and restoration, including negotiation and payment of a ransomware demand;
3. Breach notification to comply with statutory and contractual obligations;
4. Credit monitoring and identity theft protection services for those impacted by the incident;
5. Public relations and communications management to mitigate potential reputational harm;
6. Network business interruption; and
7. Attorneys' fees related to breach notification.

Third-party coverage, by contrast, addresses insureds' liability to others. Such liability may arise from litigation settlements or judgments, civil penalties resulting from regulatory investigations, and contractual obligations to indemnify clients or business associates.

In selecting cyber coverage, it is critical for companies to understand the types of risks they are likely to face in the event of a serious cyber incident.

What Falls Beyond Cyber Insurance Policies?

As with traditional policies, cyber policies contain important conditions, limitations, and exclusions, and do not cover every type of claim or loss.

Generally, cyber policies do not cover the costs to improve internal systems, such as software and hardware upgrades, and any future lost profits. Bodily injury and physical property damage may also fall outside the scope of cyber policies. Many policies exclude coverage for government-issued fines and penalties.

Key Considerations When Evaluating Policies

In addition to considering the appropriate amount of cyber insurance to purchase, it is important to carefully consider the terms. Key legal considerations when choosing cyber policies or additional coverage include, but are not limited to, the following:

Claims-Made vs. Occurrence Policies

Claims-made policies are triggered by claims made by the insured during the active policy (or extended reporting) period. Occurrence policies are triggered by occurrences during a specific policy period, regardless when claims arising from those occurrences are made by the insured.

By covering both first-party and third-party losses, cyber policies are a bit of a hybrid, requiring careful attention to requirements for notifying the insurer.

Exclusion for Acts of War and Terrorism

Cyber policies may exclude losses resulting from acts of war or terrorism. It is worth considering whether your insurance will apply in certain cases of nation state-sponsored or politically motivated attacks, particularly given the federal government's increased willingness to name and shame countries for specific cyber events.

Known Cyber Risks

Cyber policies often exclude coverage when the insured knew or reasonably should have known about a cyber incident or specific risk before the policy was obtained. Because some types of cyberattacks begin months before they are discovered, it is important to pay attention to policy provisions around discovery dates, as well as exclusions for pre-coverage events. Procuring coverage should begin well before any specific risk arises.

Coverage for Investigations

Many cyber incidents will involve inquiries by government agencies including state attorneys general, the U.S. Federal Trade Commission, and industry-specific regulators. Review whether your policy will cover responses to these sorts of pre-litigation investigations.

With cyberattacks and ransomware incidents becoming more prevalent and increasingly disruptive, it is critical that companies review their risks and consider whether their existing insurance policies cover likely cyber perils.

Author Information

Michelle Kisloff is a litigation partner in Hogan Lovells' Washington, D.C., office. She leads the firm's data privacy and security litigation practice, and represents clients in data privacy and protection litigation and regulatory enforcement.

Jasmeet Ahuja is a senior associate in the firm's New York and Philadelphia offices. An engineer with nearly a decade of national security experience, she represents clients in matters ranging from cybersecurity incidents to complex antitrust litigation.

Andrew Bank is a senior associate in the firm's Washington, D.C., office. He represents clients in commercial litigation and arbitration matters, with a focus on privacy and data security litigation.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Write for Us: Author Guidelines