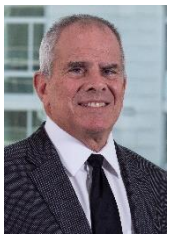
Lawyer Insights

Cyberattacks Lead to Increased Scrutiny: How Can Companies Stay Ahead of the Curve?

By Walter Andrews, Andrea DeField and Sima Kazmir
Published in Daily Business Review | January 17, 2022



Cyberattacks are an unavoidable business risk. A recent U.S. Treasury Department report observed that through June 30, 2021, the total value of suspicious activity associated with ransomware transactions in 2021 was $590 million, exceeding the total value reported for all of 2020.

Though standalone cyber insurance policies are new in the industry, they have grown in the last decade to account for increased risks and corresponding insurer and regulatory scrutiny. According to a December 2020 National Association of Insurance Commissioner's Report, premiums in cyber policies totaled $3.15 billion, doubling since 2015, and demand for standalone policies increased 24%.

The landscape of standalone cyber policies has transformed, and companies must review their existing or proposed cyber coverages carefully.

Increased Insurer Scrutiny

Recently, insurers have been limiting coverage, charging more and changing underwriting standards. At renewal, some insurers have required that companies increase their protections, such as by requiring multifactor authentication; answer more questions about security measures, including supplemental ransomware-related applications; and maintain higher baseline safety measures and controls.

Where a policyholder obtains a cyber insurance quote, they may find that coverage offered is different than before. Some major domestic cyber insurers have added ransomware sublimits or coinsurance provisions, meaning that coverage for all ransomware-related losses are limited to a lower limit than other policy coverages or that the policyholder will pay a proportion of all ransomware-related losses, with some policies requiring the policyholder to pay 50% of all such losses while the insurer pays the remaining 50%, subject to a sublimit. In response to loss ratios over 100% (meaning insurers paid out more in claims on policies than premiums written), some other insurers have issued endorsements at renewal that seek to limit coverage for "widespread events," or those that may impact many different insureds, such as the recently discovered Log4j vulnerability. Even Lloyd's of London has suggested major changes to coverage, including proposing four exclusionary endorsements that attempt to limit or preclude coverage for otherwise covered losses arising out of actions "by or on behalf of a state to disrupt, deny, degrade, manipulate or destroy information in a computer system of or in another state."

Increased Regulatory Scrutiny

Cyberattacks Lead to Increased Scrutiny: How Can Companies Stay Ahead of the Curve?
By Walter Andrews, Andrea DeField and Sima Kazmir
Published in Daily Business Review | January 17, 2022

Regulators have also begun to crack down on companies' cybersecurity disclosures. In June 2021, the SEC fined a company because despite seemingly prompt disclosure, the SEC concluded that the company failed to maintain required disclosure controls and procedures.

In addition, the New York Department of Financial Services recently charged companies under 23 NYCRR Part 500, which established cybersecurity requirements for certain financial services entities. The Federal Trade Commission also regularly investigates and takes action against companies that fail to meet promises to consumers regarding safeguarding personal information. And the Department of Justice recently announced its intent to utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients.

Companies should expect that regulators and agencies will be more active role following a cyberattack. Fortunately, despite reductions in coverage, insurance can help mitigate costs arising out of a cyberattack, as well as defense costs incurred for claims from a cyber incident, and at times, settlements, and judgments.

Analyzing Coverage

Because the market is rapidly changing, policyholders should not expect that they'll be offered the same coverage at renewal. Policyholders should start their renewal process earlier going into this year's renewal so they have time to analyze new pricing, as well as new endorsements that may limit coverage and consider alternative forms, insurers, and policies to maximize coverage.

Along with auditing cyber insurance policies to determine the extent of coverage following a cyberattack, companies should be looking to their other policies that may provide coverage following a cyberattack—Errors & Omissions, General Liability, Kidnap, Ransom & Extortion, Crime, Directors & Officers, and sometimes Commercial Property policies.

When purchasing or renewing policies, companies must look at their program as a whole to ensure there are no gaps in coverage for costs and liabilities the company may face after a cyberattack. While policies are meant to work together, actual coverage afforded across a company's insurance program can lead to a patchwork of policies resulting in coverage limitations or gaps in protection for cyber-related exposures. Care must be taken to fill these gaps at renewal.

Below are a few tips that corporate policyholder should consider in analyzing their coverage:

Ensure that exclusions for bodily injury or invasion of privacy are carved back so that they do not apply to otherwise covered claims arising out of a privacy breach.

Consider optional coverages, such as reputation loss or public relations and crisis management coverage, to mitigate the fallout from any cyberattack.

Review terrorism and war exclusions to ensure they cannot be used to deny coverage for common cyberattacks and that they contain exceptions for cyberterrorism.

Ensure contractual liability exclusions contain carve-outs for liability that would exist absent contract and otherwise covered cyber incidents. Many companies are required to make contractual representations or

warranties on cyber security programs or standards as part of contacts with clients and vendors and these representations may be alleged in a suit following a cyberattack. Consumers also often assert quasi-contract theories of liability about safeguarding of data. If your business is subject to payment card industry data security standards, ensure that the contractual liability exclusion contains a carve-out for payment card claims, fines, and penalties. All of these claims should be covered, but can fall into gaps or exclusions in policies where policyholders have not worked to ensure coverage.

Purchase express social engineering coverage on your company's crime insurance policy to cover losses arising from social engineering schemes and business email compromises that lead to fraudulent transfers.

The coverage gaps above are just a few traps for the unwary insured. Companies are best served by working with experienced insurance coverage counsel and insurance brokers to analyze coverage and fill gaps so as to maximize coverage for the company, board, and executives in the event of a cyber incident.

Walter Andrews, *is a Partner in the firm's Insurance Coverage group in the firm's Miami office. Walter's practice focuses on complex insurance recovery, counseling, arbitrations, litigation, and expert witness testimony. He can be reached at +1 305) 810-6407 or wandrews@HuntonAK.com.*

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.*

Sima Kazmir *is an Associate in the firm's Insurance Coverage group in the firm's New York office. Sima is a proactive commercial litigator whose practice focuses on complex consumer finance, insurance coverage and business litigation. She can be reached at +1 (212) 309-1112 or skazmir@HuntonAK.com.*