Published December 1, 2020

POTENTIAL INSURANCE COVERAGE ISSUES RESULTING FROM A CYBER BREACH

By: Luma Al-Shibib*

The frequency, scale, and sophistication of cybersecurity breaches continues to escalate. In the COVID-19 era, new cybersecurity threats have emerged as a result of the workforce shifting primarily to remote work from potentially more vulnerable home computer systems.

In light of the ongoing and evolving threat of cybersecurity breaches, it is important for companies to be aware of the potential insurance coverage issues that may arise when seeking coverage under cyber insurance liability programs for a cybersecurity incident.

Typical Cyber Insurance Coverages

Although coverage is likely to differ from policy to policy, cyber insurance policies typically include coverage for the following types of losses:

1) Forensic Investigation of Cyber Incident – the costs incurred to hire expert consultants to determine the cause and extent of the breach.

2) Restoration of Digital Assets and Computer System – the costs to restore or replace lost digital assets and restore the capacity or functionality of the Computer System to its pre-breach level.

3) Cyber Extortion – ransomware paid to cyber attackers to stop an attack or return access to a company's system or stolen information.

4) Business Interruption Losses – lost profits resulting from the inoperability of the Computer System because of a cyber incident.

5) Event Management – the costs to notify third parties that their information may have been compromised by a cyber incident and related costs for credit/identity monitoring.

6) Privacy Liability – the costs to defend against a consumer class action or other third-party liability resulting from the cyber incident.

7) Regulatory Fines and Penalties – legal fees, fines, and penalties incurred as a result of a regulatory investigation for violation of privacy laws.

Potential Coverage Issues

Policyholders who are aware of the limitations to coverage under cyber insurance policies will be better equipped to navigate the claims adjustment process should they be faced with cyber-related losses. Because each policy is different it is important to review your individual policy and understand its coverages and exclusions.

1. Insurance Companies Typically Argue that "Upgrades" and "New Functionality" Are Not Covered

Generally, cyber policies cover the costs to restore your digital assets and the capacity or functionality of your Computer System to pre-breach levels. Insurance companies typically take the position that they will only cover the costs to repair or replace that which you had before.

Because cyberattacks often are continuing in nature and compromise the integrity of a Computer System, a policyholder may require additional cybersecurity programs or devices beyond those which it had before a cyber incident to regain and restore the integrity of its system. Arguably such costs should be covered under policies that insure restoration of system functionality to pre-breach levels. Policyholders, however, are likely to face resistance from cyber insurers who will attempt to characterize such costs as "betterments," "upgrades," or "new functionality" so that they can discount those costs as uncovered. Disputes over whether costs constitute uncovered upgrades can become costly and may require experts to opine on the necessity of each challenged cost. To avoid protracted claims adjustment processes and potential litigation, policyholders are advised to assess their cybersecurity systems, controls, and policies before experiencing a cyber incident in order to identify and remediate any system vulnerabilities.

2. Coverage to Restore Computer Systems May Be Limited

Coverage for restoration of a "Computer System" can be broadly defined to include hardware and software, electronic data, firmware, and system devices and peripherals. Some policies, however, define "Computer System" more narrowly, potentially limiting coverage. For example, some policies do not include hardware in their definition of "Computer System," or limit coverage to hardware owned by the policyholder. In light of the increase in remote working, much of which involves the use of personal employee-owned devices, it is particularly

important to understand what your cyber policy covers and whether it limits or excludes coverage for computer hardware that is not owned by the company.

3. Business Interruption Losses Susceptible to Attack Based on Causation and Methodology

Generally, cyber policies will offer coverage for business interruption ("B.I.") loses sustained during the period of interruption caused by a cyber incident. Usually, such coverage is limited to a certain period of time, such as no more than 30 or 60 days from the date of the incident, even though it may take longer to restore the operability of the Computer System.

B.I. claims made under cyber liability policies are susceptible to challenge regarding causation and methodology. Often cyber policies will require the submission of a proof of loss quantifying the types and amounts of losses claimed. In preparing the B.I. component of the proof of loss, it is important to ensure both that the quantification of B.I. losses is calculated using a methodology that is generally accepted within the applicable industry and that a causal connection can be shown between the losses claimed and the cyber incident.

4. Other Insurance Coverage Issues

Other types of insurance policies may provide coverage for particular types of losses resulting from a cyber incident. For example, first party property policies may provide business interruption coverage that may supplement the BI coverage provided under a cyber policy. Additionally, first party property policies may offer coverage for damaged hardware, which may fill the gap in coverage where a cyber policy excludes or limits coverage for hardware replacement. Directors and officers ("D&O") liability policies that do not specifically exclude cyber-related claims may provide coverage for claims of wrongdoing against the company or its directors and officers arising from a cyber incident – such as the failure to disclose cyber vulnerabilities or the extent of a cyber breach to shareholders. Accordingly, in the wake of a cyber incident, policyholders should review all their insurance policies and provide notice under all policies that could potentially provide coverage for possible cyber-related losses.

Where other types of policies do exist, cyber insurance companies may attempt to avoid or limit their exposure by invoking "other insurance" provisions in cyber liability policies to argue that a different policy must respond to the claimed losses first. The purpose of "other insurance" clauses is to prevent over-insurance and double recovery under different insurance policies. Notably, however, "other insurance" provisions are triggered only where two or more policies cover the same type of risk during the same period of time[1]. Cyber-related claims made under cyber, first-party property, and D&O policies, arguably may cover different risks during different time periods, thereby foreclosing a cyber insurer's ability to invoke the other insurance provision to reduce or limit its liability.

5. Excess Insurance Issues: "Improper" Exhaustion

For claims made under a cyber liability policy tower comprised of primary and excess policies, excess insurance companies may seek to limit their exposure by arguing that their excess policies have not be triggered because the underlying insurance policy limits have not been properly exhausted through the payment of covered claims. Under this "improper" exhaustion argument, excess insurance companies argue that the primary or underlying insurers wrongly paid certain uncovered costs that they should not have paid. For example, an excess insurance company may argue that the primary insurance company wrongly paid 50% of underlying policy limits towards uncovered upgrades. Because those costs allegedly were not covered under the policy, the excess insurance company will argue that the underlying policy limits were never exhausted and therefore the excess policy was never triggered.

In general, courts have held that excess insurance companies are not bound by the coverage determinations of underlying insurers and may make their own determination as to whether a claim is covered under their excess policies. The weight of authority, however, holds that an excess insurer cannot "second-guess" or relitigate the claims adjustment processes and payment decisions made by underlying insurers in the absence of fraud or bad faith or an express provision in the excess policy reserving the excess insurance company's right to payments made by underlying insurers[2]. Thus, an excess insurer should not be able to avoid or limit its liability under an excess cyber policy by arguing that the underlying cyber insurer paid certain costs that it should not have paid and that those costs should not be counted towards exhaustion of the underlying policy limits.

Conclusion

Every cyber liability policy and cyber claim is different. A policyholder can best protect its interests by ensuring that it has adequate cybersecurity controls in place before experiencing a cyber incident and by reading and understanding the coverages provided under its cyber insurance policies. Consultation with a professional broker or coverage counsel may assist in understanding what your cyber policy does and does not cover and offer tangible advice on how to maximize potential coverage.

Attorney **Luma Al-Shibib, Esq.**, is a shareholder in the New York office of Anderson Kill. Luma focuses her practice on insurance recovery for corporate policyholders, with an emphasis on directors & officers liability insurance, comprehensive general liability insurance, and cyber liability insurance. She can be reached at lal-shibib@andersonkill.com or (212) 278-1048.

1 See AMHS Ins. Co. v. Mut. Ins. Co., 258 F. 3d 1090, 1097 (9th Cir. 2001); Fed. Ins. Co. v. Firemen's Ins. Co., 769 F. Supp. 2d 865, 876 (D. Md. 2011); Boston Gas Co. v. Century Indem. Co., 454 Mass. 337, 361 n.36 (Mass. 2009); Travelers Ins. Co. v. Lopez, 93 Nev. 463, 469 (Nev. 1977).

2 See AXIS Reinsurance Co. v. Northrop Grumman Corp., 975 F.3d 840, 846-47 (9th Cir. 2020); see also Costco Wholesale Corp. v. Arrowood Indem. Co., 387 F. Supp. 3d 1165 (W.D. Wash. 2019); Edward E. Gillen Co. v. Ins. Co. of the State of Pa., Case No. 10-C-564, 2011 WL 1694431, at *4 (E.D. Wis. May 3, 2011); ARM Props. Mgmt. Grp. v. RSUI Indem. Co., Case No. A-07-CA-718-SS, 2008 WL 5973220, at *5-7 (W.D. Tex. Aug. 25, 2008); Ins. Co. of N. Am. v. Kayser-Roth Group, 770 A.2d 403, 417 (R.I. 2001).

About Anderson Kill

Anderson Kill was founded in 1969 on the principles of integrity, excellence in the practice of law, and straightforward solutions to complex legal issues. The firm's attorneys approach engagements aggressively, and have earned a reputation for combining corporate polish with pugnacity. Based in New York City, the firm also has offices in Philadelphia, PA, Stamford, CT, Washington, DC, Newark, NJ and Los Angeles, CA, but the attorneys travel around the country and around the world to handle all types of matters. Anderson Kill attorneys work together, leveraging creativity and legal and business acumen to deliver cost-effective resolutions to clients' problems. Many of the firm's professionals are recognized experts in their practice areas, leaders and active participants in professional associations, and are frequently invited to speak to business organizations.

Anderson Kill clients include some of the nation's largest public and private entities, including companies in financial services, retail, oil/gas, telecommunications, construction, food supply, technology, pharmaceutical and life sciences, and utilities, municipalities and state governments, religious and not-for-profit organizations, small companies and individuals. Anderson Kill prides itself on attracting and retaining intelligent, personable and well-rounded attorneys. Smart attorneys with sharp skills, excellent client service, and a track record to prove it: that is the Anderson Kill difference.