Five Issues to Watch for Cyber Insurance Coverage in 2025

Micah Ethan Skidmore

Jan 27, 2025 7 min read

Summary

- Policyholders should prioritize their focus on coverage for third-party breach events,
- the wording of the “war” exclusion,
- coverage for phishing attacks and funds transfer fraud,
- cyber-related bodily injury and property damage liability,
- and coverage for emerging algorithmic liability.

Whether you are a policyholder or an underwriter, one challenge unique to cyber insurance that network security and privacy liability risk is constantly evolving. As soon as an insurer can issue an endorsement covering Payment Card Industry Data Security Standard assessments or ransomware or social media losses, the underworld of cyber crime has migrated to a new threat du jour. With this ever-changing landscape, it is impossible to predict what might emerge in the new calendar year. But if the events of 2024 are any guide, here are five issues to watch in the world of cyber insurance for policyholders and insurers alike in 2025.

Coverage for Third-Party Breach Events

Within the cyber insurance space, 2024 may be remembered as the year of the “outage” or “disruption” breach. Historically, large corporate breach events, including the massive credit card breaches in the mid-2010s, may have affected millions of individuals, but only one business at a time. More recent trends involving phishing attacks, social media fraud and even ransomware attacks have impacted a discrete number of businesses in each event. Then, in February 2024, a ransomware attack involving a healthcare claims

clearinghouse, Change Healthcare, brought widespread disruption to thousands of healthcare providers and payors; it continues to have ripple effects throughout the industry. In June 2024, the CDK Global ransomware attack affected thousands of U.S. car dealerships dependent on CDK's software. Only a month later in July 2024, the CrowdStrike system failure, while not a breach event, brought similar interruptions to airlines, banks and hospitals reliant on the company's software.

The secondary, tertiary and extended effects from breach events, service outages and system failures in 2024 underscore the need for coverage that responds, not only when the insureds' computer system is breached, but when a third-party breach event indirectly interrupts the policyholder's business operations. This is not simply contingent business interruption coverage, which may be limited to certain defined relationships between the policyholder and a third-party vendor or customer. As we have learned in 2024, a policyholder's business may be interrupted by a breach event involving a party with whom the insured has no direct contractual relationship. It may involve a third party whose products and services are directly related to information technology. Or it may not. Insureds should carefully consider the cyber policy terms that limit the third parties for whom a breach event triggers business interruption coverage for the insured.

War Exclusion

Recent legal decisions have brought some clarity to policyholders and insurers over the application of a "war" exclusion that does not expressly exclude cyber breach events that happen to involve state actors. For example, in *Merck & Co., Inc. v. Ace American Ins. Co.*, 475 N.J. Super. 420, 425 (N.J. App. Ct. 2023), *appeals dismissed,* 256 N.J. 190, 307 A.3d 533 (2024), the New Jersey Superior Court Appellate Division concluded that a "hostile-warlike action" exclusion in a property policy did not unambiguously include "a cyberattack on a non-military company that provided accounting software for commercial purposes to non-military consumers, regardless of whether the attack was instigated by a private actor or a 'government or sovereign power.'"

However, a single opinion addressing one set of terms in a war exclusion will not necessarily preclude insurers from adjusting language to embrace any breach event in which a state actor participates, regardless of whether motivated by military or other political objectives. Many policies now exclude loss caused by a broad litany of circumstances, including war, hostilities, or acts of foreign enemies, provided that there is usually a common exception for cyber terrorism, *i.e.*, ideologically or politically motivated conduct that stops short of military action. The way such war exclusions are currently drafted, an insurer may argue that the exclusion embraces a cyber breach, ransomware, phishing or other attack in which a state actor is in any way involved; and it may be the

nearly impossible burden of the insured to demonstrate the motives of the faceless cyber criminals responsible for the attack, in order to prove that the claim falls within the exception to this broadly worded exclusion. Policyholders should, therefore, carefully consider the terms of any war exclusion included in their cyber insurance policy, including what burdens of proof are imposed upon the insurer and insured, respectively.

Funds Transfer Fraud

Within this decade, there has been a shift from large data breaches to targeted phishing and ransomware attacks. Cyber criminals have discovered that it is easier and can be more lucrative to steal money, than it is to steal information. According to IBM's annual Cost of a Data Breach Report, 2024 was the second year in a row in which phishing and stolen or compromised credentials were the two most prevalent attack vectors for a breach event. Phishing attacks are also among the most costly form of data breach for policyholders. Cyber insurers know these statistics as well as anyone, and coverage for phishing attacks and related wire transfer fraud is shrinking just as quickly as this sort of crime is increasing among corporate insureds.

Existing policies covering funds transfer fraud may now include a range of qualifications and limitations that substantially narrow this important coverage. Some policies may require adherence to multifactor authentication or other security procedures before coverage will be extended. Other policies may only apply to attempts to impersonate the insured (as opposed to a vendor or customer) or the transfers of money from the insured (as opposed to a bank or financial institution). Still other policies may impose sublimits, and there may be any number of other limitations imposed on this coverage depending on the policy and insurer. Given the extraordinary potential for loss and the increasing frequency of this particular attack vector, corporate policyholders should very carefully review the terms of any cyber policy intended to insure phishing attacks and related funds transfer fraud to ensure that material limitations are avoided and critical coverage is preserved. They also should review other potentially applicable lines of coverage—including especially their crime policies—to determine whether this type of digital crime may fall within a general coverage grant; or alternatively, whether any specific exclusions align seamlessly with a coverage grant in the cyber policy, or whether they leave gaps.

Bodily Injury and Property Damage Liability

Ordinarily, the language in cyber insurance and general liability insurance policies is supposed to dovetail so that each policy provides coverage for different risks without leaving the insured vulnerable to gaps. General liability insurance policies customarily provide coverage for liability because of "bodily injury" and "property damage," while

excluding liability for network security breaches. Cyber insurance is supposed to cover the network security and data breach-related privacy liability that is excepted from coverage under a general liability policy. However, some cyber policies also exclude coverage for liability for bodily injury and property damage claims, while some general liability policies now contain broadly worded exclusions for various cyber or digital perils.

The so-called "cyber-physical" risk to insureds–i.e., liability for physical bodily injury or property damage resulting from an intangible digital cause such as a data breach—is real. For example, a ransomware attack that affects a hospital or other healthcare provider could harm patient health. A system failure involving a utility service provider, construction company or similar business could result in property damage. Other contingencies could also result in an overlap between cyber liability and traditional bodily injury or property damage liability. Which policy applies in these scenarios? In order to avoid a potentially significant gap in coverage, when placing and renewing cyber insurance coverage, corporate policyholders should look for a coverage grant addressing rather than excluding liability for bodily injury and property damage claims. Alternatively, if no cyber insurer is willing to provide such coverage, then the policyholder must carefully review its general liability policies to make sure they contain no exclusions that an insurer might argue would preclude the coverage reasonably expected for traditional physical harms when they happen to result from cyber-related risks.

Algorithmic Liability

In the emerging world of artificial intelligence applications, the line between traditional business operations and risk, on the one hand, and information technology operations and related risk, on the other hand, is getting blurred. A transportation company that relies on an AI database to develop a new marketing campaign is potentially vulnerable to intellectual property claims from content creators, whose data were used in the AI's advertising application. A manufacturing company is named in a product liability lawsuit, where the alleged defect involved faulty data in the AI application used to develop the product at issue. The Department of Justice sues a technology firm for antitrust violations involving so-called "algorithmic collusion" in pricing rental properties. *See* Aaron Gregg & Eva Dou, *Why is rent so high? The Justice Department blames a tech firm's algorithm*, The Washington Post (Aug. 23, 2024). A putative class files suit against health insurers for using algorithms to deny health insurance claims. *See* Jeffrey Bendix, *Cigna using AI to reject claims, lawsuit charges*, Medical Economics (Aug. 7, 2023).

In each of these scenarios, is the risk and liability claimed against the business something that should be addressed by "personal and advertising injury" coverage, commercial general liability coverage for bodily injury or property damage, or a traditional "errors and

omissions" policy? Often such legacy liability policies may have broadly worded exclusions for the unauthorized use or access to electronic data. Since all of these theoretical claims arguably focus on the appropriate use of electronic data, should the risk created by algorithmic liability be addressed instead by a cyber liability policy? As the legal waterfront on AI-related claims develops further, insureds and insurers should also consider where and how this emerging risk will be covered in the corporate policyholder's insurance program.

Conclusion

Insurance would not exist without uncertainty, and if the past year has confirmed anything, it is that there is plenty of risk and uncertainty for corporate policyholders in the realm of network security, privacy liability and breach events. In the midst of this uncertainty, policyholders should prioritize their focus in the coming year on coverage for third-party breach events, the wording of the "war" exclusion, coverage for phishing attacks and funds transfer fraud, cyber-related bodily injury and property damage liability, and coverage for emerging algorithmic liability.

The views and opinions expressed in this article are those of the author and not necessarily those of the firm or its clients.

Author

Micah Ethan Skidmore

Haynes and Boone LLP

Micah E. Skidmore is a partner in the Insurance Recovery Group at Haynes and

Boone, LLP. Micah represents corporate policyholders in litigation and arbitration of significant insurance coverage disputes, including...

ABA American Bar Association

https://www.americanbar.org/groups/litigation/resources/newsletters/insurance-coverage/five-issues-cyber-insurance-2025/?login