Key Considerations for Cyberrisk Coverage

by Joshua Gold

Today's cyberthreats can trigger multi-faceted losses. A serious cyber incident could cause bodily injury, property damage, business interruption, shareholder litigation, customer privacy litigation, regulatory action, terminations or resignations among senior management, and reputation damage. As such, a host of insurance policies may come into play, including directors and officers, errors and omissions, cyber, property and crime.

If a cyber incident occurs, one of the first steps to take is to provide prompt notice to insurers for all potentially implicated policies. Even if you or your broker believe that coverage may not be available based upon recent cases, err on the side of providing notice under most circumstances.

For example, after a social engineering scheme perpetrated by fraudulent emails and phone calls resulted in nearly $5 million in improper wire transfers, a New York federal court recently found that a policyholder had crime insurance coverage under both its computer fraud and fraudulent funds transfer coverage. This was in stark contrast to a previous Fifth Circuit ruling that reversed a Texas court finding of coverage for the policyholder under similar circumstances.

Last year, the United States Fourth Circuit Court of Appeals found CGL coverage for defense of a privacy class action in a case where patient medical data was exposed on a publicly searchable database. This stood in contrast to a prior New York trial court ruling that went the insurance company's way. The bottom line is that the law, the policy language, and interpretations thereof can vary from incident to incident. Consequently, to maximize recovery, it is usually best to provide notice on all potentially implicated lines of coverage.

In addition, it is important to periodically review your insurance coverage to make sure your company is adequately protected. It is particularly important to:

Cover time-element losses: Business income coverage and reputation damage coverage have taken on added importance in the wake of recent cyber events. As a breach can impact the fundamental ability to continue business operations, consider insurance coverage that pays time-element claims resulting from reputation damage and business interruption.

Seek favorable retroactive dates: Push for retroactive coverage on favorable terms whenever possible. It can take a business weeks, months, or even years to become aware of a breach of its systems. Thus, get your insurer to include a retroactive date that precedes policy inception by as much time as possible. There are currently more options to do so than in years past.

Avoid cybersecurity reasonableness clauses: Resist insurer efforts to include exclusions, warranties, representations or "conditions" in insurance policies concerning the soundness or reasonableness of the policyholder's data security efforts. These clauses are a recipe for disputes on potentially every security incident and have already led to insurance coverage litigation under specialty cyber insurance products. Given the pace of technological innovation, almost every security measure can be second-guessed with the benefit of hindsight.

Remember that cyber breaches happen off-line too: Make sure your cyber-specific policies cover claims involving mobile devices, home offices, data that is off-line at the time security is breached, and devices that may not be owned by the policyholder. An incident does not have to involve network intrusion—the simple case of a lost laptop or flash drive can cause an expensive breach if it contains gigabytes of sensitive data.

Cover cloud and third-party vendors: Make sure that your cyber coverage protects against losses where others manage,

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com

transmit or host data for your company. Most cyber policies can be modified to extend claim protection for situations involving cloud computing and instances where data is handled, managed or outsourced to a third party. Such coverage, however, may need to be specifically requested as some insurers' base forms lack express protection for this exposure.

Be prepared for the evolving risk: Cyberthreats are always changing, so continuously monitor trends in hacking and data breaches to ensure that your insurance policy matches your exposure. ■

Joshua Gold *is a shareholder in Anderson Kill's New York office and chair of Anderson Kill's Cyber Insurance Recovery Group. He regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property/casualty insurance coverage issues.*

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com