Securing Coverage for Cyberattacks

by Brad Murlick and Joshua Gold

Recent high-profile cyberattacks have demonstrated that hackers do not always intend to steal. Instead, many hacks are designed to disrupt normal business operations and damage computer systems or even brick-and-mortar property.

The reasons for this trend are varied. Some cybercriminals target computer systems to further espionage, extortion, political or "moral" causes. Some of these hacks are merely incidental to technological trends in the internet of things arena that have increased connectivity of a wide range of products and systems. In this new environment, then, risk managers need to closely consider their first-party coverage for losses of business income and damage to reputation.

Companies are vulnerable to a variety of potential cyber events that can trigger coverage. Ransomware can hold entire networks hostage until the targeted policyholder pays the extortion fee. Hidden malware in apps for smart devices can result in data breaches. Indeed, there seems to be an almost unlimited set of tools that hackers can use to steal, impair or destroy information in the cyber world that can result in physical damage and tangible economic impact to a company in both the short- and long-term.

While certain aspects of damages can be straightforward, such as ransom demands or credit-monitoring expenses, first-party policy language, including cyber policy language, can make it challenging to quantify loss of income as a result of a cyberattack. How much does an online retailer lose if its website is taken down on Cyber Monday? Will the insurance company argue that there were make-up sales if the policyholder was able to come back online in a day? What if the impact lasts a week? Is there brand loyalty such that a customer might shop at a physical location instead? Is there long-term reputational harm to the brand? The claim process involving the answers to these questions may not be easy.

Cyber events can cause physical damage to property as well. Machines used in modern manufacturing are often controlled by computer equipment that may be susceptible to cyberattacks. Refineries and chemical manufacturers manage high temperature and high pressure vessels using computers. If a cyberattack does occur, valuation issues will be similar to those common with traditional first-party property claims. The initial period of interruption is tied to the period that it takes to repair the property. There may be an extended period of indemnity issue with ramping up operations after startup.

The valuation of damages starts with the practical ramifications of the event and often involves detailed analysis of financial, operational and market data to derive the best estimate of the impact of the event. Seasonality may be a factor, depending on the nature of the policyholder's business. Notwithstanding all of the factors that go into valuing damages, the "three-column approach" is regularly used to demonstrate losses. With this approach, a top-to-bottom projection of a policyholder's financial statements is done based on financial and operational data. That projection may be compared to actual results, using the difference as the starting point for loss determination. This methodology is not so much a purely mathematical exercise as it is a representation of the facts and circumstances of the loss and resulting impact to the insured.

As with every other policy, particularly in the realm of cyber insurance products, it is important to make sure that the coverage most likely to be triggered is not set to a sublimit that would fall short of what is needed in the event of a serious loss.

There is no doubt that a large effort is now underway to steer policyholders toward new standalone cyber products. With

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com

that said, consider that some standard insurance products provide coverage for cyber-related losses, such as property and crime insurance policies, either under their main terms of coverage or under special coverage sections. This is true of certain business package policies as well. Be mindful of new policy exclusions and questions on insurance applications that touch on cyber perils, which need to be closely examined.

There is no one absolute rule in determining where a policyholder will find insurance coverage and in what amounts. Varying insurance product lines, terms and circumstances of the loss will all normally have a bearing in determining the level of insurance recovery that the policyholder will achieve in the wake of a cyber claim. ■

Brad Murlick *is a managing director in the investigations practice of Navigant Consulting.* ***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