RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com

Adjusting Insurance Coverage to Meet Shifting Cyberattack Risks

by **Joshua Gold**

These days, keeping up with all of the recent examples of cyberattacks seems almost impossible. They continue to strike at an amazing clip, with some far worse than others. The attacks tend not to discriminate—they regularly hit individuals, businesses, hospitals, universities and other institutions.

For those in the risk management business, the insurance focus over the past several years has mainly been fixed on the potential liabilities of a cyberattack. This certainly has proven wise given the recent ruling by the United States Court of Appeals for the Seventh Circuit. In that case, retailer Neiman Marcus had been attacked by hackers who were able to access customer account information and was subsequently sued by its customers for harm arising from the hack. The federal trial court dismissed the action, finding that the plaintiffs did not have legal standing to maintain their lawsuit as they suffered no recognizable injuries.

But the Seventh Circuit reversed the trial court's dismissal, finding instead that the plaintiffs did have standing, and that thousands of plaintiffs who had suffered fraudulent charges on their accounts and even those who had no fraudulent activity on their cards all suffered "actual" injury. The appeals court concluded that injury to the plaintiffs occurred even where customers were fully reimbursed for fraudulent charges and where no identity theft had taken place. Thus, the court said, the plaintiffs could move ahead with the lawsuit.

Accordingly, cyber insurance that promises coverage for third-party liability claims, including class action lawsuits, remains an important component of a risk management strategy. If anything, its importance has even increased in the wake of the Seventh Circuit's ruling.

Many policyholders have also concluded that liability insurance is important for claims and lawsuits from state and federal regulators and law enforcement. If there is a breach of customer information, investigations are highly likely and there may be subsequent litigation with state attorneys general and the Federal Trade Commission. In fact, any breach of sensitive customer information affecting residents of more than one state is likely to at least draw inquiries from multiple state attorneys general.

MONITORING FIRST-PARTY COSTS

While liability insurance has understandably been the focus of addressing risk transfer for cyber-related claims, policyholders should not forget the importance of first-party insurance as well. In fact, this should be a growing area of importance for risk managers. Several hacks over the past year indicate that cybercriminals are not always interested in pilfering customers' financial account numbers or health data. Some hackers want the target's own assets, whether for espionage, extortion, or political or "moral" causes.

Some hacks are designed to inflict damage, even where motives may be unclear. In the past year, hackers using social engineering, and other methods, infiltrated the computer network of a European steel factory and were able to cause massive damage to the blast furnace by gaining access to the plant's computer-dependent controls. Put simply, we are in an era where cyberattacks can destroy brick-and-mortar busi-

ISTOCK/DASEUGEN

nesses. As we have continued to expand the Internet of Things, hackers have been able to gain remote unauthorized control of internet-enabled automobiles and the turbo fans powering commercial aircraft. Cyberthreats to these and other products and equipment have important implications for property damage, business interruption and corporate reputation. While there are also serious liability implications, policyholders must ensure their insurance programs will cover first-party loss attributable to such cyberattacks.

As the Sony Pictures Entertainment hack illustrated, some breaches may have limited third-party liability risks associated with them, but significant implications for the protection of proprietary information, employment issues and public reputation. As such, policyholders will need to kick the tires on first-party coverage that is offered for losses of business income and damage to reputation. As with every other policy, particularly in the realm of cyber insurance products, make sure that the most valuable coverage is not set to a sub-limit that would fall short of what is needed in the event of a serious claim.

BEYOND CYBER INSURANCE

There is no doubt that a large effort is now underway to steer policyholders toward new standalone cyber products, but it is very important to keep a wider view of these matters from a risk management perspective. Despite the breadth of coverage promised by many cyber policies, there is also a lot of untested and non-uniform fine print that some insurers will surely seize upon to challenge claims, despite the original intent of the parties. There have already been insurance coverage lawsuits involving cyber insurance products because the insurer refused to provide coverage for a claim.

When a claim arises, also remember that some standard insurance products provide coverage for cyber-related losses, such as D&O, E&O, general liability, property and crime insurance policies. But be mindful of new policy exclusions and questions on insurance applications. If, for instance, your cyber policy has an exclusion for securities claims, then it is critical that your D&O coverage pick up such a claim, even where the precipitating circumstances are strictly due to a cyberattack.

Technology and our dependence on it are in an ever-greater state of flux and evolution, permeating all aspects of our business and personal activity. With the wide range of opportunities afforded by technical innovation also comes an especially challenging environment for risk managers. As always, it is important to stay vigilant and attuned to developments on both the risk and insurance product fronts. ■

Joshua Gold *is a shareholder in the New York office of Anderson Kill and chairs the firm's cyber insurance recovery group.*

WHILE LIABILITY INSURANCE HAS UNDERSTANDABLY BEEN THE FOCUS OF ADDRESSING RISK TRANSFER FOR CYBER-RELATED CLAIMS, POLICYHOLDERS SHOULD NOT FORGET THE IMPORTANCE OF FIRST-PARTY INSURANCE AS WELL.