Cyber Claim Trend: Risks Go Beyond Data Breaches

By Jeremy Gittler, Cyber & Technology, XL Catlin
April 11, 2016

When most people think about cyber insurance, they tend to visualize data breaches. In fact, less than one-third of the cyber claims we see are for breaches. The vast majority of cyber claims tendered are for other events, which says a lot about the nature of cyber exposure.

Breaches garner most of the attention, such as those that have made media headlines recently for affecting renowned retail companies, because they can expose millions of personal records and can damage reputations, invite litigation and impair the market share of even the largest corporations. Consumers and businesses are rightly worried about personal information falling into the wrong hands, which can lead to identity theft and trigger investigation and notification.

Organizations of all stripes however, need to be equally concerned about another cyber risk exposure -- media liability. But, if an organization doesn’t consider itself a member of the media, how can that be? Media liability for personal injury arising from libel, slander, defamation, copyright infringement, or plagiarism, for example, can be triggered by wrongful acts resulting from blogging, broadcasting or other channels of disseminating matter. What’s “matter”? Under the policy definition, “matter “is any communication of any kind, public or private.” So if your company, which might be in manufacturing or retail trade communicates with the public, it is exposed to cyber-media liability. Knowing this, it’s not surprising that about 30% of cyber claims we’re seeing is triggering media liability coverage.

Another area of exposure that affects many companies today is technology errors and omissions (E&O) liability and miscellaneous professional liability. This area generates about 40% of cyber claims that my team sees. When a technology product or a technology-supported service doesn’t work properly, companies that provide them can be susceptible to these kinds of cyber claims. For instance, if software provided by a company does not perform as intended, a
consumer could take action against the provider. Or, consider the exposure of a microchip manufacturer, who could be held liable for when a chip failure results in a device malfunction. And many companies which may not consider themselves technology companies, but that use technology as part of their delivery of professional services or products, could see themselves facing technology E&O claims. Such a company might also see a miscellaneous professional liability claim against their cyber coverage if a customer finds some fault in a service they provided, irrespective of their technology service. For example, a company providing clearing services of securities trades could have a claim against it for its technology service, or based on human error irrespective of technology.

"It’s important to understand that the cause of cyber liability can vary."

It’s important to understand that the cause of cyber liability can vary. Most people associate cyber risk with malicious outsiders, such as hackers. But unintentional acts by internal staff or business partners can trigger liability, as well. Sometimes liability arises when businesses are slow to comply with changes in state laws or regulations. In the US, forty-seven of the fifty states have data breach notification laws, an area that is constantly changing. Statutes carry penalties of which the plaintiffs’ bar is acutely aware. Class-action attorneys and regulators pay close attention to such violations, and businesses that are not aware or have not complied to the statutes may find themselves in court.

Hackers are certainly active when it comes to exploiting cyber security weaknesses. Ransomware has become a growing problem for many businesses. The concept is simple: a hacker places malicious software on a system, often through social engineering such as spear phishing, which encrypts the data on the system. To decrypt the data, the hacker demands a ransom payment, which has been reported to be as low as $300. Why so low? Because many people would pay it without thinking twice. But just because a low ransom is paid and the data is freed, the victim may be fooled into thinking that the problem is solved. In fact, there may be a much larger issue that results in cyber liability.

Consider this claims scenario. A small municipality in the Northeast, with an active cyber policy suffered a ransomware attack. Taking into account that their deductible was significantly higher than the ransom request ($10,000 vs $300), the municipality decided to pay the ransom assuming the virus would be harmless once the payment was made. However, when they notified us we advised on the importance of 1) not trusting the criminals, and 2) investigating the malware as they did not know what information had been accessed or what they could do with it. While they were reluctant at first, the municipality agreed to a forensic investigation that found that more than 34,000 personal records, including vital statistics, marriage licenses, death and birthdates, had been exposed. Additionally, the exposure triggered a legal notification requirement. Fortunately, their cyber insurance policy protected them far beyond what the municipality initially thought its loss was. As in this case, both public and private entities can be lulled into a false sense of security – taking one action – like paying ransom to release a computer – only to find that the problem has not gone away, or really hasn’t been addressed at all.

That is one of the great advantages of having cyber insurance. There is indemnity protection for incidents that generate financial loss, but the policy also makes available valuable resources that can respond quickly to help a claimant recover and minimize third-party liability. As our claims trends are showing, there are certainly many reasons why cyber risks require close attention. From media liability to technology E&O to miscellaneous professional liability exposures, for business and public entities alike, cyber risks clearly go beyond data breaches and we see that trend continuing.