WHAT YOU NEED TO KNOW ABOUT CYBER LIABILITY INSURANCE

In today’s news headlines, a week doesn’t pass without a mention of a large company experiencing some type of cyberattack or breach. Examples of high-profile cyberattacks in the news over the last year include the Equifax breach, which has cost the company over $242 million, and the WannaCry attack, which has cost companies a total of $4 billion. In fact, it was estimated that cyberattacks in 2017 cost companies over $500 billion.

The price tag of cyberattacks are not only limited to first party costs but can also result in millions – or in some cases, billions – in third-party costs, like regulatory fines. Uber recently settled an investigation into its 2016 data breach for $148 million, a consequence of not disclosing the breach in the required timeframe. Not to mention Facebook could face a $1.63 billion fine from the EU for not adhering to the recently enacted General Data Protection Regulation (GDPR) standards.

Cyber liability insurance was created to address this exposure and help protect businesses from financial pain and reputational damage. Prior to this type of insurance, general liability policies typically excluded covering cyber exposures, leaving companies vulnerable and in a tough financial spot should an attack or breach occur. Now, with cyber liability insurance, companies have both first party coverages – such as data destruction, theft, business interruption, and denial of service attacks – and third-party coverages – like fines for failure to safeguard data. Other benefits that come with cyber liability policies include reimbursement for security audits, post-incident public relations and expenses that stem from the investigation of a breach or attack.
However, one new challenge has emerged related to cyber liability insurance: the crossover it has with other policies, such as professional liability and commercial property insurance. If an insured company doesn’t have a common carrier for cyber and professional policies, it typically leads to finger pointing by the respective carriers since incidents can be covered by both policies.

An example of when this may occur is if Personally Identifiable Information (PII) or Protected Health Information (PHI) is compromised. This could be covered by the cyber liability policy as a cyber breach or by professional liability policies as the insured didn’t do enough to protect the data. In this case, there would be unnecessary red tape trying to decide and recover the expenses for indemnification of individuals affected by the attack, payment card industry fines, and costs associated with regulatory defense and fines. Another example is when commercial property is intentionally damaged by a bad actor, such as a hacker setting off a building’s sprinkler which causes damage to the property. This instance could be covered by both cyber liability insurance and commercial property insurance.

While the interplay of various coverages may create some temporary challenges, those challenges should not diminish the value, and necessity, of cyber liability insurance. The numbers speak for themselves. Currently, the annual gross written premiums of cyber liability policies are over $5 billion, with the market expected to grow to $7.5 billion by 2020. Cyber liability insurance is increasingly embraced in industries where attacks or breaches are becoming more prevalent, yet, many industries still lack necessary protections. While 50 percent of healthcare, technology and retail companies in the U.S. currently have cyber liability insurance, only 5 percent of manufacturing companies in the U.S. have coverage. This exposes manufacturing firms to tremendous risk.

Regardless of industry, every company has cyber exposures that are not limited to
only attack or breach expenses. For example, a manufacturing company could be affected by a cyber-attack that locks it out of its system, leading to no access to company orders, product designs or production equipment. Cyberattacks could also target companies’ equipment or property and result in property damage by causing the equipment to malfunction. This was the case in 2014, when hackers caused a German steel mill’s blast furnace to overheat, leading to millions of dollars in property damage.

The good news is that an insurance broker can help companies navigate any challenges and industry-specific risks. By working closely with an experienced broker, who understands these nuances, companies can ensure the appropriate policy is in place and there are no crossover issues. Each business needs a partner that understands the unique exposures it faces to be able to design a tailored risk management and insurance program that provides comprehensive protection from cyber threats.

[whitewpaper-oneill]