Cyber risks

Effects can be wide-ranging: are you covered?

Between 2016 and 2017, the average cost of a cyberattack increased by 23% to $11.7 million globally, according to the Ponemon Institute's study, *Cost of Cyber Crime*. The study also found businesses in the United States have the highest average cost of $21 million per incident (a 22% increase from 2016). Another study by Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview*, reported that the average cost for a data breach is $3.62 Million with each lost or stolen record costing $141. While the cost to recover each record has come down a bit, Ponemon reported that the size of the data breaches are getting larger. Criminals are finding it easier to scale cybercrime globally with ransomware attacks — which have doubled in the last year — putting more and more businesses at risk.

What are businesses doing to protect themselves?

Besides heavily investing in technology and cyber defense, they are implementing a risk transfer strategy in the form of buying cyber insurance. According to the *Cyber Security Report* issued by *Business Insurance*, 76% of businesses have a standalone cyber policy, but this may not be enough. With over 50% of the cost of a cybercrime being indirect costs like business disruption, employers need more holistic solutions.

Some good news – the industry is evolving

As recently as 3 to 5 years ago, cyber insurance coverage focused on privacy protection. We are now seeing more attention being paid to the impact on operations and business interruption including disruptions caused by vendors. We are beginning to see even more evolution in the form of bodily injury and property damage caused by cybercrime. Cyber policies have begun providing business interruption coverage with adequate policy limits. Insurers are also starting to include cyber activity as triggers for other policies such as general liability, product liability and kidnap and ransomware. *Business Insurance* referred to this evolution as the "coming of age" for cyber insurance.

What about today?

While the market is rapidly maturing to meet ever-changing demands, employers may still find they have exposures and gaps in insurance coverage. Employee negligence and third party exposures continue to pose significant risks to businesses, and our expanding reliance on data means a breach could significantly impact your business' revenue stream and sustainability.

- **Your employees:** Technology tools designed to block cybercrime can only do so much. Because cyber criminals know people make mistakes, they design phishing and social engineering scams to take advantage of this weakness. Teaching your employees to identify cyber scams and what to do when faced with one is one of your best defenses against cybercrime.
- **Third-party risks:** You should be reviewing contract language with third-party vendors to ensure your interests are properly protected and data-related

Continued >>

Please see final page for important disclosure information >>

exposures are addressed. If necessary, require your third-party partners to carry first and third-party cyber liability insurance with adequate limits to provide added protection. Also, ask to regularly review your vendors' policies and procedures for handing and protecting data. You do not want their vulnerabilities to materially impact your business.

- **Business income:** Most companies have a business income policy, but according to a study by the Chartered Institute of Loss Adjusters, 40% of policy holders had a limit of insurance that was deemed to be 45% lower than needed. Be sure to review your cyber policy to ensure this coverage is included and analyze your network impact risks to ensure the limits are adequate.

When it comes to cybercrime, threats are constant and happening at an ever increasing pace. Constantly monitoring the landscape, educating your employees, investing in technology and carrying the right insurance coverage are the best ways to protect your business from cybercrime. Our cyber specialists can help you identify exposures and structure a cyber program to meet your specific needs.

For more information, contact us.

Associated

Benefits and Risk Consulting

Phone: **800-258-3190** | Email: **Info@AssociatedBRC.com**