Data breaches keep happening, attack vectors are evolving, and traditional tools are not standing their ground. In today’s internet-connected environment, companies are at risk for incidents both inside and outside the IT environment and can fall prey to a disruptive network intrusion or costly data breach at any time. Nonetheless, cyber insurance has become a hot topic across all companies regardless of size and sector as a way to combat the financial impact of these incidents when they happen.

Considering that today’s cyber and data security threats are tomorrow’s insurance claims, it is important that all companies review their current insurance policies to examine how and if such claims would be covered. Traditional insurance products—such as commercial general liability policies or property policies—are designed to cover bodily injury or damage to tangible property, not cyberattacks or data breaches. Most traditional insurance policies now specifically exclude coverage for such losses. Specialized standalone cyber insurance policies are designed to protect your company in the event of unauthorized access, data theft, data loss, network intrusions, information security breaches, system downtime, and more.

While cyber insurance can’t eliminate a data breach or be a replacement for data security, it can provide a backstop of financial relief, offering a budget dedicated to data breach preparedness and a comprehensive incident response
plan solution to help minimize the financial damage of a data breach or cyberattack. Before purchasing a cyber insurance policy, companies need to consider the company’s cyber and data risks to determine which risks to avoid, accept, mitigate, or transfer through insurance.

With many more insurance carriers now offering standalone cyber insurance policies, companies have many options to choose from and must carefully conduct their due diligence when reviewing varying policies and coverage options. In addition to the many insurance carriers offering cyber insurance, there are several new “Insurtech” startups that offer cyber insurance along with a complimentary risk assessment or cybersecurity plan.[2] Note that these complimentary services do not directly decrease the premium of the cyber insurance. When purchasing cyber insurance coverage direct from an Insurtech company, organizations would be prudent to check on the financial ratings and stability of the company.

Indeed, a company shouldn’t just buy insurance to exonerate itself from its data security responsibilities, which is why it will want to ensure it implements data and cyber security protocols before applying for a cyber insurance policy. In today’s risk environment, cyber insurance underwriters now expect that security measures are already in place prior to purchasing a policy, and companies aren’t typically awarded discounts for implementing them since they are now deemed to be an essential requirement.

When a company seeks cyber insurance, the insurance carrier will ask many questions about the company’s operation, types of data collected, processed, and/or stored, data backup processes, data security controls and third-party relationships. It is highly recommended that companies exploring the purchase of a cyber insurance policy to first conduct a risk assessment to identify the company’s cyber and data risks, threats and vulnerabilities. Risk assessments play a significant role in cybersecurity and can also help streamline the cyber insurance underwriting process; e.g., Where are the gaps? What are the vulnerabilities? Which threats are most likely—and most serious? Which risks can be transferred to a cyber insurance policy to minimize losses when they occur?

By studying past data breaches that have occurred and considering the likely attack methods and routes of exploitation through a risk-assessment process, companies can be better positioned to mitigate the potential impact that data security breaches have on achievement of their objectives by transferring the
associated risks to a cyber insurance policy.

Working with a Cyber Insurance Broker

The complexity of cyber insurance coverages relates to the adage “you would not want your general practitioner offering advice for a condition that only a specialist doctor should be treating.” Therefore, it is highly recommended to work with an experienced cyber insurance broker who understands the complexities of cyber insurance. While there are many general insurance brokers today now offering cyber insurance, beware of those brokers that are more concerned about making a higher commission and may steer your company to a carrier that pays them a higher commission rather than providing your company with the best policy match for your company’s needs.

The types of coverage offered by cyber insurance policies vary dramatically by insurance carrier, so a reputable and knowledgeable cyber insurance broker can help your company carefully evaluate the plethora of cyber insurance policy options from a variety of angles.

Indeed, the cyber insurance application and exploration process is the most critical component in ensuring that the company’s cyber insurance coverage needs are met, and ultimately that coverage will be available at the time of an incident.

Understanding the True Impact and Cost of a Data Breach

A data breach is every organization’s waking nightmare. Nevertheless, data breaches continue to make headlines and aren’t going away, and more importantly, the cost of a data breach is soaring for companies. Certain industries have higher data breach costs. Heavily regulated industries such as healthcare, pharmaceutical, financial, energy, and transportation, communications and education tend to have a higher per capita data breach cost. However, if boards of directors and senior management are actively involved in risk management and security, they can significantly reduce costs related to a data breach. The costliest data breaches tend to be the ones that are highly targeted toward a company for specific reasons. However, with clear
priorities set by the board and senior management, others within the organization, including IT personnel, can focus on the likelihood of an event happening and then mitigate the potential impact that data breaches can have on the company. Preparation is the best defense, and having a breach preparedness plan in place can help the company act quickly if one occurs. Acting quickly can help to prevent further data loss, significant fines and costly customer backlash.

When conducting the company’s cyber- and data-risk assessment, take the time to correctly assess the cost of a data breach in order to determine the costs due to consequences of the breach.

After a data breach, the company will need to figure out exactly what is at stake, the scope of the breach, what it will cost and how it will impact the company, and what to do about it.

These questions can help calculate business losses:

- How much money will the company lose based on the information such as intellectual property (IP), personally identifiable information (PII) or personal health information (PHI) lost through the data breach?

- How much money will the company lose to notification costs, lawsuits, fines, penalties, and reputational damage when the data breach becomes public?

- How much time will it take to resolve the breach—to identify and address all affected systems, and respond?

- How much will the company be fined if its security practices don’t comply with security policies and requirements?