RBJ RBJ.NET ROCHESTER BUSINESS JOURNAL
Part of the BridgeTower Media network
MARCH 16, 2021

Determining which cyber insurance policy is best for your company

As cybercrime continues to rise, companies are increasingly looking to obtain cyber insurance, but those in the field say it is important for businesses to know what types of policies are available and how they can best be used to protect firms in the case of a cyberattack.

Dylan Bittlingmaier, insurance advisor with Lawley, says the effects of the COVID-19 pandemic, including having more people working remotely, have made companies more vulnerable to a cyberattack.

"Everyone is at risk, and there's no end in sight," Bittlingmaier says.

He recommends companies in all sectors consider such insurance but adds the type of policy a firm secures depends on its industry.

Lawley has taken a proactive approach, reaching out to clients to let them know about the insurance options they may want to consider when it comes to cyber insurance, Bittlingmaier says.

Reggie Dejean, specialty insurance director at Lawley, agrees there has been increased interest in cyber insurance over the past few years and the demand escalated as a result of COVID-19.

While cyber liability insurance is not mandatory, customers and suppliers are including it more regularly in contracts with firms they will be doing business with as an added safeguard to protecting their data, Dejean says.

Having a clearer picture and understanding of exactly what is covered — and what is not — is vital for policyholders, he says.

First-party cyber liability insurance helps a business respond to data breaches on its own network or systems. Third-party cyber liability insurance helps pay for lawsuits caused by data breaches on a client's network or systems.

Having a cyber insurance policy can help minimize business disruption during a cyber incident and afterwards, he adds.

Often included in coverage is the assistance of a breach coach after an incident who reviews what happened and looks at next steps, including the possibility of paying a ransom. Regularly, a legal team is also brought in, as is a team of cyber experts that can help get a business back online.

Dejean agrees the coverage is something firms of all sizes, in all sectors, should consider.

Plans can be individually structured and include deductibles, both of which can make a policy more affordable.

"Any business should at least investigate the cost," Dejean says.

Gregory Knicley, senior vice president at Tompkins Insurance Agencies Inc., says increased interest in cyber insurance over the past few years, along with an increase in claims, is leading to increases in premiums and stricter requirements for companies looking to obtain such policies.

"The application is more robust in terms of what they are asking and more technical in nature," Knicley says.

Insurers are also asking for a company's finances to see how the business weathered the pandemic since, sometimes, when a business is struggling financially, cybersecurity efforts can be the first thing suspended, he notes.

Mark Battaglia, an account executive at Tompkins, says cyber insurance is a regular part of the renewal discussions he has with clients.

While the interest was not as great when Battaglia first started with the firm over six years ago, he is seeing more companies be receptive to the idea of a cyber insurance policy.

Factors driving that change range from the increase in remote work as a result of the pandemic, to the nearly daily headlines of companies and organizations of all sizes dealing with a cyberattack.

"I say it's not if it will happen, it's when," Battaglia says. "That speaks to a lot of companies."

Before a client takes out such a policy, Battaglia also works with them to find out where they stand with their cybersecurity efforts. He notes having a cybersecurity plan in place is essential.

"Having a strong information technology security program in place is the first step; insurance is the second piece," Battaglia says, noting cyber insurance does not prevent a company from having a breach; it, instead, provides protection after one occurs.

In addition to increased interest in cyber insurance, other types of companies are forming to help businesses navigate the changing federal and state regulations related to cybersecurity. Being on top of such areas can also have an impact on insurance coverage, they say.

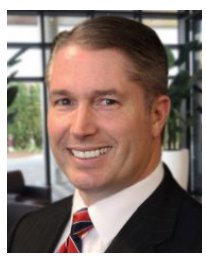
One such company is Caetra.io, a subsidiary of Harris Beach PLLC, created in 2019.

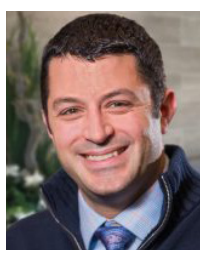
The business offers a cloud-based subscription software tool to help companies with regulatory compliance. The product streamlines the process of developing policies and controls to comply with state and federal laws regarding data privacy and cybersecurity.

Michael Compisi, president and general manager of Caetra.io, says the goal was to create a relevant, user-friendly tool for companies to help with what is a relatively complex issue.

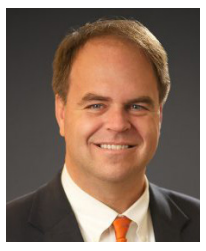

Bittlingmaier


Dejean


Knicley


Battaglia


Compisi


Winchester

Compisi has seen an uptick in the number of firms interested in cyber insurance. He says the software platform Caetra.io offers can not only help companies with their cybersecurity efforts, but the controls the software can put in place can help make the underwriting of a cyber insurance policy a relatively easy process.

New York is increasing its focus on the importance of cybersecurity for businesses, and the role insurers play, says Alan Winchester, chief development officer and founder of Caetra.io and partner at Harris Beach. Winchester also leads Harris Beach's cybersecurity protection and response practice group.

In a legal alert last month, Winchester spoke of the New York State Department of Financial Services urging of cyber insurance companies to require the insured to implement robust security programs with adequate security controls in place to address their risk.

If an organization fails to pass the risk testing performed by their potential insurance carrier, or passes the test but is then found to not have actually followed their written program, they risk being either denied coverage or having their claim disclaimed for misrepresenting their security defenses, Winchester wrote in the alert.

Sometimes, a business may feel having cyber insurance is enough protection if a breach occurs, but Winchester says that is not the case, noting cyber insurance is only one piece of a thorough cybersecurity plan.

"Companies are making a mistake if they think they can transfer the risk," he says.

Andrea Deckert is a Rochester-area freelance writer.