JOURNAL REPORTS: TECHNOLOGY

The Ins and Outs of Cybersecurity Insurance

Policies are designed to help companies survive major cyberattacks. But knowing exactly what's covered can be tricky.

By Dennis Nishi
June 4, 2019 10:03 pm ET

The idea of cybersecurity insurance seems, on its face, pretty straightforward: Being hacked not only can disrupt business, it also can be extremely costly and hurt a company's reputation. Businesses want to protect themselves against those losses.

But in practice, such insurance raises a lot of questions.

JOURNAL REPORT

- Read more at WSJ.com/journalreporttech

MORE IN CYBERSECURITY

- The Quantum Threat to Encryption
- Our Emotional Attachment to Our Passwords
- Can the Sound of Your Typing Be Decoded?
- The Tussle Over Facial Recognition

There's no question that cyber insurance is on the rise, though growth in the U.S. slowed last year to 8% from 37% in 2017, according to Fitch Ratings.

These policies are designed to help companies survive major cyberattacks by offsetting the costs of recovery. But knowing exactly what's covered can be tricky. The cyber insurance category is new, so there isn't much standardization in the way insurers are determining risk or even defining attacks. Coverage gaps can be created by uninformed choices.

Here are some questions companies need to ask themselves.

What do we need to cover?

Companies first need to determine, with the help of a security specialist if necessary, what their biggest risk areas are and what they stand to lose if they experience an attack.That way, they can fine-tune their coverage as much as possible to fit their particular needs.

Among the areas companies need to assess are reputation damage, data-restoration costs and reimbursement for government regulatory fines in the wake of a data breach.

The National Institute of Standards and Technology, which is part of the U.S. Commerce Department, offers security guidelines that can help companies understand and assess their risk, says Gregory Touhill, a cybersecurity expert from Carnegie Mellon University's Heinz College who was the first U.S. federal chief information security officer. Knowing what kind of security provisions insurers expect to see from companies also can provide a helpful overview. Cybersecurity insurance applications can be downloaded that show the standard levels of security insurers expect and highlight other potential risk areas.

What's the difference between first-party and third-party cyber liability insurance?

First-party insurance covers the policyholder's own direct losses from cyberattacks such as data theft, denial of service and extortion. In addition to compensation for lost income, benefits sometimes include coverage for the cost of various steps companies take in the wake of an attack, such as figuring out how their networks were penetrated, notifying customers affected by an attack, restoration or repair of digital content and public-relations efforts to repair a company's damaged reputation.

Companies that store customer credit-card information or other sensitive personal data typically buy first-party coverage.

Third-party insurance covers companies that allowed a data breach to occur on a client network. For instance, an IT contractor that was paid to build a secure website for a client could be liable for damages if there was a mistake or oversight that led to a network intrusion. Coverage could include reimbursement for legal fees, settlements, damages in court cases and fines that may be levied by government regulators.

What cyber incidents do insurers typically exclude from coverage?

Most standard cyber policies exclude preventable security failures that result from failing to maintain a minimum level of security—an improperly configured firewall, for example. The careless mishandling of sensitive information by employees generally isn't covered. Malicious acts by employees also generally aren't covered, or theft of trade secrets or intellectual property.

The most high-profile cyber-related exclusions happened after the 2017 NotPetya ransomware attack that affected companies around the globe. Some companies that filed for cyber-related claims under their business and property insurance policies had them denied—in at least one case due to a rarely used but common contractual clause that excludes "a hostile or warlike attack" by a state actor. The Central Intelligence Agency attributes NotPetya to the Russian military.

If the breach is the company's fault, is the insurer always off the hook?

Not always. Many policies cover employee mistakes such as losing a laptop or falling for phishing scams. But every case is open to interpretation, says Brandon Hickey, president of Insureon Brokerage. If an employee accidentally lost a laptop on the train, for instance, that might be covered. But under the same policy, if that employee lost a laptop that contained sensitive information that wasn't supposed to leave the office, that could be grounds for a claims denial.

How long after a breach occurs does a company have to report it to an insurer?

There's often a big difference between when the breach occurs and when it is discovered. On average, small businesses don't discover that their network has been breached for 197 days, according to a survey by the Ponemon Institute. But once a company is aware of an attack, in general, insurance companies ask customers to inform them of any newly discovered cyber loss when practical. Insurers understand that companies will first want to settle immediate priorities such as securing the network against further intrusions.

Although "when practical" doesn't mean immediately, sitting on the claim for too long might raise a few eyebrows that could affect a company's settlement, says Bob Parisi, managing director at the Marsh brokerage unit of Marsh & McLennan Co s. It would be unusual for a company to file a claim, say, six months or more after it discovered an intrusion, he says.

An insurer's requirement for notification could differ from a company's legal obligations. All 50 states and the District of Columbia have enacted data-breach notification laws that require public and private organizations to notify all customers that are affected by data loss. Reporting times vary by state, but Colorado and Florida, for instance, have 30-day deadlines from the date of discovery, the shortest allowance for any state.

How do insurers price cyber insurance?

Pricing is based mainly on a company's annual revenue—since more income amounts to higher risk exposure—and what industry it is in. The insurer wants to find out what sensitive data the company keeps that would make it a target to cyber criminals. A hospital would be more expensive to cover than a library, since the hospital stores a lot of patient medical records. Patient records are protected by strict state and federal privacy rules, so companies that expose that data could be subject to multimillion-dollar fines.

How much network security a company has can also influence premiums. Insurance companies will often ask companies to detail what kind of security they have during the application process, such as whether employees have been trained to recognize cyber fraud or if company software is routinely updated. Insurers also want to know how frequently companies change their passwords and how much network access third-party vendors and service providers have. They may also ask whether a company has had a third-party audit of its system or whether it has used a so-called external penetration tester, also known as ethical hacking, to root out any network weaknesses.

Mr. Nishi is a writer in Los Angeles. He can be reached at reports@wsj.com.

Corrections & Amplifications

After the 2017 NotPetya attack, some companies that filed for cyber-related claims under their business and property insurance policies had them denied—in at least one case due to a rarely used but common contractual clause that excludes "a hostile or warlike attack" by a state actor. An earlier version of this article incorrectly stated that the claims that were denied were made under cybersecurity policies. (June 10, 2019)

Appeared in the June 5, 2019, print edition as 'Explaining Cyberinsurance.'

- College Rankings
- College Rankings Highlights
- Energy
- Funds/ETFs
- Health Care
- Leadership
- Retirement
- Small Business
- Technology
- Wealth Management