FEATURE

What is cyber insurance and why you need it

Cyber insurance can't protect your organization from cybercrime, but it can keep your business on stable financial footing should a significant security event occur.

By Kim Lindros and Ed Tittel

CIO |

MAY 4, 2016 4:43 AM PT

Technology, social media and transactions over the Internet play key roles in how most organizations conduct business and reach out to prospective customers today. Those vehicles also serve as gateways to cyberattacks. Whether launched by run-of-the-mill hackers, criminals, insiders or even nation states, cyberattacks are likely to occur and can cause moderate to severe losses for organizations large and small. As part of a risk management plan, organizations routinely must decide which risks to avoid, accept, control or transfer. Transferring risk is where cyber insurance comes into play.

What is cyber insurance?

A cyber insurance policy, also referred to as cyber risk insurance or cyber liability insurance coverage (CLIC), is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event. With its roots in errors and omissions (E&O) insurance, cyber insurance began catching on in 2005, with the total value of premiums forecasted to reach $7.5 billion by 2020. According to PwC, about one-third of U.S. companies currently purchase some type of cyber insurance.

The numbers indicate that organizations are seeing a need for cyber insurance, but what does it cover? Cyber insurance typically covers expenses related to first parties as well as claims by third parties. Although there is no standard for underwriting these policies, the following are common reimbursable expenses:

- **Investigation:** A forensics investigation is necessary to determine what occurred, how to repair damage and how to prevent the same type of breach from occurring in the future. Investigations may involve the services of a third-party security firm, as well as coordination with law enforcement and the FBI.
- **Business losses:** A cyber insurance policy may include similar items that are covered by an errors & omissions policy (errors due to negligence and other reasons), as well as monetary losses experienced by network downtime, business interruption, data loss recovery and costs involved in managing a crisis, which may involve repairing reputation damage.
- **Privacy and notification:** This includes required data breach notifications to customers and other affected parties, which are mandated by law in many jurisdictions, and credit monitoring for customers whose information was or may have been breached.
- **Lawsuits and extortion:** This includes legal expenses associated with the release of confidential information and intellectual property, legal settlements and regulatory fines. This may also include the costs of cyber extortion, such as from ransomware.

[Related: Need for cyber-insurance heats up, but the market remains immature]

Keep in mind that cyber insurance is still evolving. Cyber risks change frequently, and organizations tend not to report the full impact of breaches in order to avoid negative publicity and damage the trust of customers. Thus, underwriters have limited data on which to determine the financial impact of attacks. Essentially, the true risk of cyberattacks is not completely understood.

What to look for as a cyber insurance buyer

Lots of well-known insurance companies offer cyber insurance policies, such as Allianz, Chubb Philadelphia and Travelers, to name a few. Insurance industry watchers believe that clients will soon expect cyber insurance to part of every business insurer's product line. However, like any business insurance, cyber insurance coverage varies by insurer and policy.

When comparing policies among insurers, find out if they cover all of the items listed in the previous section and inquire about the following special circumstances and limits:

- Does the insurance company offer one or more types of cyber insurance policies or is the coverage simply an extension to an existing policy? In most cases, a stand-alone policy is best and more comprehensive. Also find out if the policy is customizable to an organization.
- What are the deductibles? Be sure to compare deductibles closely among insurers, just like you do with health, vehicle and facility policies.
- How does coverage and limits apply to both first and third parties? For example, does the policy cover third-party service providers? On that note, find out if your service providers have cyber insurance and how it affects your agreement.
- Does the policy cover any attack to which an organization falls victim or only targeted attacks against that organization in particular?
- Does the policy cover non-malicious actions taken by an employee? This is part of the E&O coverage that applies to cyber insurance as well.
- Does the policy cover social engineering as well as network attacks? Social engineering plays a role in all kinds of attacks, including phishing, spear phishing and advanced persistent threats (APTs).
- Because APTs take place over time, which can be months to years, does the policy include time frames within which coverage applies?

Tip: Many insurers also offer a checklist of coverage items to compare against their competitors. Use those checklists to add to your list before starting your research in earnest.

What do insurance companies look for when deciding coverage?

An insurance company wants to see that an organization has assessed its vulnerability to cyberattacks (created a cyber risk profile) and follows best practices by enabling defenses and controls to protect against attacks as much as possible. Employee education in the form of security awareness, especially for phishing and social engineering, should be part of a protection plan. A boost to best practices may include organizations that have had threat assessments performed (even if not required by regulations). It’s wise to use threat intelligence services for the latest information on zero-day and targeted attacks, and to engage the services of ethical hackers to reveal security weaknesses.

Note: Threat intelligence and ethical hacking services are difficult at best or financially impossible for many small businesses. But investing in some type of vulnerability assessment tool or engaging the services of a penetration tester to probe external network defenses one time can go a long way toward improving security while negotiating cyber insurance.

As cyber insurance coverage becomes more standardized, an insurer might request an audit of an organization's processes and governance as a condition of coverage. And don't be surprised if an insurer agrees to provide coverage but at a level below (sometimes far below) what you feel you need. If so, keep interviewing insurers to find the best deal.

Making the business case for cyber insurance

Any organization that stores and maintains customer information or collects online payment information, or uses the cloud, should consider adding cyber insurance to its budget. Also consider the proliferation of devices that now connect to business networks -- there are simply more opportunities for malicious folks to access an organization's assets.

Attacks against all business are increasing. Small businesses tend to think they are safely tucked away from exposure, but Symantec found that over 30 percent of phishing attacks in 2015 were launched against organizations with less than 250 employees. Symantec's 2016 Internet Security Threat Report indicated that 43 percent of all attacks in 2015 were targeted at small businesses.

On a larger scale, the Centre for Strategic and International Studies in 2014 estimated annual costs to the global economy from cybercrime was between $375 billion and $575 billion. Although sources differ, the average cost of a data breach incident to large companies is over $3 million. Each organization has to decide if they can risk that amount of money, or if cyber insurance is necessary to defray the costs for what very well may occur.

[Related: Farmers Insurance eyes drones, Internet of Things]

Remember, cyber insurance covers first-party losses and third-party claims, but general liability insurance covers only property damage. Sony was caught in that situation after the 2011 PlayStation hacker breach, with hard costs reaching $171M that could have been offset by cyber insurance had the company made certain that it was covered ahead of time. During a court case, Zurich American Insurance Company said that Sony’s policy only covered physical property damage, not cyber damages.

Regarding costs, cyber insurance coverage and premiums are based on an organization's industry, type of services provided, data risks and exposures, security posture, policies and annual gross revenue. As examples only, premiums may range from $800 to $1,200 for consultants, tax preparers and small organizations with revenues of $100,000 to $500,000, to $10,000 to over $100,000 for those with revenues in the millions.

Getting started

A good first step is to create a cyber risk profile for your company, and to create a list of expenses you want to have covered in the event of an incident. Then, you can determine an estimate for third-party costs. Many insurers provide an insurance calculator on their websites to help organizations create a list of coverage and estimate costs. Then, you can begin researching cyber insurance providers. Trade associations in your industry might have some information to share as well as the U.S. Chamber of Commerce.

Next read this:

- *9 lies CIOs tell themselves*
- *8 hot IT hiring trends — and 8 going cold*
- *7 hot new IT jobs — and why they just might stick*
- *9 warning signs of bad IT architecture*
- *Why IT projects still fail*
- *10 hot data analytics trends — and 5 going cold*
- *The skills and traits of a next-generation CIO*
- *12 'best practices' IT should avoid at all costs*
- *6 data analytics success stories: An inside look*
- *10 old-school IT principles that still rule*
- *The 13 most valuable IT certifications today*

Follow everything from CIO

NEW! Download the State of the CIO 2017 report