



Cyber Insurance...What is it?

A cyber insurance policy, also referred to as “cyber risk insurance” or “cyber liability insurance” coverage, is a financial product that enables businesses to transfer the costs involved with recovery from a cyber-related security breach or similar events.

Typically, the most important aspect of cyber insurance will be network security coverage. This coverage will respond in the event of a network security failure or insider breach – such as data exfiltration, malware, ransomware attacks and business account and email compromises. However, the policy will also respond to liability claims and ancillary expenses of an attack or breach. Additionally, if your business’s revenue stream has any contact with European consumers or businesses, then the recently implemented General Data Protection Regulation (GDPR) likely applies to you.

Many US-based businesses have already taken measures to be GDPR compliant but that doesn't mean your insurance has followed suit. Are you buttoned up?

Many are surprised to learn the real costs associated with a breach. According to a Ponemon report from 2017, cyberattacks cost small and medium-sized businesses an average of \$2.235 million. On top of that, the study showed that 60 percent of the businesses that were polled said that attacks are becoming more severe and more sophisticated each year.

There is, however, no doubt that the cyber insurance space will continue to grow rapidly and offers will certainly be expanded and customized. Also, as is the case with most other types of insurance offers, cyber insurance policies are evolving towards more industry-specific solutions and becoming less general.

Is it Complicated?

Cyber risks and coverages are complicated. In a recent Advising survey of brokers, agents, and underwriters from around the world—all involved in cyber—77 percent said one of the biggest obstacles to sales is the fact that potential insureds don't understand the exposures. Further, 56 percent indicated that prospects don't understand the coverages offered. This shouldn't be a surprise. Cyber is a relatively new market, and the products can vary considerably based on an insured's industry and size. Differences also exist with respect to what coverage is included within policy limits, what may be covered within a sublimit, whether cyber coverage is provided via a separate endorsement, and what's excluded. These variations can be challenging, especially for small and midsize enterprises (SMEs) that may lack the technical resources and knowledge to manage cyber risk.

Does One Size Fit All?

Cyber insurance is as dynamic as the companies it protects and is consequently far from standardized. However, some of the issues that cyber liability insurance typically covers include:

- **Data loss, recovery, and recreation**
- **Business interruption/ loss of revenue due to a breach**
- **Loss of transferred funds**
- **Computer fraud**
- **Cyber extortion**

If hackers expose or steal personal information, such as Social Security numbers, driver's license number (in some states), address, and bank account information, a cyber liability insurance policy pays for:

- **Notification Costs: This expense is significant because the company bears the burden of both identifying potential victims, which requires an internal investigation, and providing notification that's reasonably calculated to give actual notice.**
- **Credit Monitoring: In effect, your cyber insurance policy pays for victims' insurance policies. Regulators usually dictate the kind of credit monitoring to provide and it's a safe bet they will not be satisfied with the cheapest available protection.**
- **Li Damages: Most of these liability lawsuits are class actions, with hundreds of thousands of dollars in damages at a minimum, even for a very small company.**
- **Computer Forensics: This covers costs to hire computer forensics consultants working under the direction of your attorneys to determine whether a data breach occurred, to contain and prevent further damage, and to investigate the cause and scope of the breach.**
- **Reputational Damage: Data breaches can have profound PR implications for any business. A preferred policy will help you handle the potential fallout by covering the damages stemming from brand aversion due to a cyber incident for a certain amount of time after the breach. It can also help mitigate the potential cost by paying for PR management experts.**

Small Companies are Not Targets...Right?

Too small to worry? Think again.

Small business owners may believe they're too small to be the target of a cyberattack. This is a dangerous misperception.

Hacks into large companies' systems may grab headlines, but according to ISO analysis, 80 percent of data breach victims are small to midsize enterprises, with under \$250 million in revenue. These incidents increased 20 percent in 2017, and the industries most affected were healthcare, professional services, and information, which includes publishing, broadcasting, telecommunications, and other information and media services.

Smaller firms may be targeted because they may be perceived as less likely to have sophisticated or up-to-date protections in place. Under this view, they are likely to be particularly susceptible to ransomware—software that seizes control of a computer system's files, encrypts them, and demands payment from the owner to regain control. Some business owners may believe it makes more sense to risk having to pay blackmail than to spend a lot of money up front on security and insurance coverage.

What's Not Covered?

Like most coverages, there are certain exclusions that a cyber policy usually will not cover. The policy will not respond if you are sued for any potential vulnerabilities in your systems before a breach occurs. Most notably, cyber insurance policies will typically not reimburse you for future profits lost due to a cyber-attack or data breach.

If you fear losses due to theft of your intellectual property, you'll have to look towards a specifically tailored intellectual property insurance policy. Additionally, allegations that the policy holder's patents infringe upon those of a third party will also not be afforded coverage. If an agent of a foreign power causes the breach, the coverage can be denied under the acts of war exclusion. Additionally, the cost to improve your security and technology systems after an attack will not be included in most policies (make sure to read our guides on how to respond to cyber-attacks and how to recover from a cyber-attack).

When considering whether you'll be covered for cyber-related exposures it's crucial to understand the concept of "Silent Cyber". Many traditional insurance policies, most notably general liability insurance (CGL), weren't designed with cyber risks in mind. This means that they don't have precise language either implicitly including or excluding cyber exposures. However, in practice this means that CGL policies generally won't cover cyber liability, and if they do the coverage will be minimal at best.

It's also important to note that social engineering attacks can be considered a special case. Social engineering refers to attacks that rely on psychological manipulation to gain access to sensitive information or funds. Victims following instructions from fraudulent emails or calls is not considered a computer system breach. Therefore, a special policy social engineering extension needs to be added to the cyber insurance.

Wrap Up...

In the world we live in today there is unequivocal evidence that no matter what size or type of organization you are you need cyber insurance. Like all insurance the lower the organization's risk to cyber-crime the lower the premiums! Therefore, arm your organization with the best of the best protections and security stacks. This is an investment worth having.

Contact ICM CYBER to discuss your cyber-security needs:

Solutions@icmcyber.com

888.713.2718



