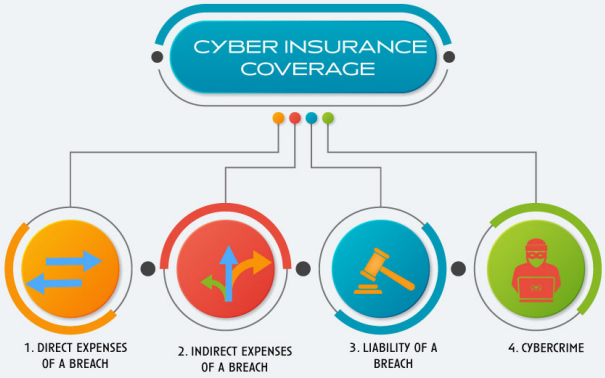
PSA
INSURANCE & FINANCIAL SERVICES

What Is Cyber Insurance and Why Is It the New "Must Have" for Businesses?



If you're like millions of business people, your usual Monday morning probably consists of starting up your computer, checking email, catching up on news and trends related to your industry, logging into systems, and getting a general lay of the land to plan out your week. If your typical routine doesn't involve technology in some way, you are definitely in the minority. Technology is now a given for most businesses—we use systems and data without even thinking about it—which is why cyber insurance is a must to protect your operation from cyber incidents.

Imagine instead of settling into your Monday morning routine, your business encounters one of these scenarios:

- Everything has grinded to a halt because key systems you use to run your business have been compromised and locked by a cybercriminal demanding a ransom before they can be unencrypted.
- Your email account has been hacked and last week it was used to send phishing emails to internal employees and external contacts.
- An employee was tricked into sending all of your employees' W2 information out to a cybercriminal.
- One of your vendors that has access to sensitive data of your clients has experienced a breach that appears to have included your data.
- Malware was discovered on your point of sale system and it appears credit card information may have been exposed.
- Several employees have had a type of malware on their systems for weeks that has been logging all keystrokes, including usernames and passwords.

These are just few of the most common scenarios, and chances are good that your operation could face some variation of these sooner or later. How can a cyber insurance policy protect you?
I'm not a big fan of using fear to motivate people into an action, but sometimes we need a little nudge. Cyber risk is abstract, and most of us haven't experienced an incident. Every scenario is different, and it's hard to predict what will happen when you experience a breach or attack. Because of this, even if you were able to predict the type of incident you are going to experience, it's hard to know exactly how to respond.

This is where cyber insurance comes in. Most policies today are broad enough to apply to many of the most common incidents. Similar to your traditional business insurance, Cyber insurance pays claims. But even more than that, it is an essential element of your cyber risk management strategy. With the right cyber policy, you'll have resources, experts, and guidance you can access right away if you find yourself in the middle of a cyber incident.

MIKE VOLK
443-798-7403
mvolk@psafinancial.com

What does a good cyber policy include?

The four essential coverage sections

Section 1. Direct Cyber Incident & Breach Response Expenses

If you experience a cyber incident, it will cost you money to respond. An essential part of any cyber insurance policy includes reimbursement for the following:

1. Data breach coach expenses (a.k.a. data privacy/cybersecurity attorney)
2. Cyber incident handling expenses
3. Cyber forensics investigation expenses
4. Public relations and crisis communication expenses
5. Victim notification, credit monitoring, and other remediation expenses

Section 2. Indirect Cyber Incident and Breach Response Expenses

A cyber incident can impact a business in many different ways beyond your initial incident response costs. Reimbursement for the following indirect costs of a cyber event are typically covered:

1. Lost income due to system disruption
2. Lost income due to system disruption of a 3rd party cloud service provider
3. Lost income due to reputation damage suffered after a cyber event
4. Extra expenses to get back up and running
5. Costs to restore data, systems, and technology

Section 3. Your liability to others for allowing a breach or incident to occur

If you fail to protect data entrusted to you by others; fail to stop the spread of a cyber-attack, post offensive/misleading or other defamatory content online; or don't comply with a law, regulation, or contractual requirement; you could face legal costs and damages.

A good cyber insurance policy should cover all defense expenses, damages, fines, and penalties resulting from the violations, failures, and non-compliance mentioned above.

Section 4. Cybercrime

Cybercrime is on the rise, and criminals are consistently thinking of new strategies and exploiting new vulnerabilities to make stealing from businesses and individuals easier. Cybercrime coverage options typically include the following but coverage may be spread across a few different policies:

1. Electronic Cybercrime—someone gains unauthorized access to a system through hacking and monetary theft
2. Social Engineering Cybercrime—an employee is tricked into making fraudulent wire funds transfer, paying fake invoices, divulging back account and payment information, etc.
3. Computing Resources Cybercrime—someone gains unauthorized access into a phone system or cloud account and fraudulently uses your resources resulting in costs.

When it comes down to it, cyber coverage is peace of mind in our turbulent, digital world. It won't solve all of your cybersecurity problems, but when all else fails, or if you failed to prepare, it gives you a paddle as you are heading up the creek. If you have questions about how to protect your organization from a cyber incident, or would like to get a cyber insurance quote, contact me at mvolk@psafinancial.com.

MIKE VOLK
443-798-7403
mvolk@psafinancial.com