CYBER INSURANCE 101 FOR SMALL BUSINESSES

Cybercrime is one of the biggest threats to your business today. That's right—just because you're a small business doesn't mean cybercriminals will look past your company.

Since hackers know you won't have the resources or security precautions larger enterprises would have, they might even be more interested in targeting you. Fortunately, cybersecurity tools and cyber insurance can help you deter them and safeguard your small business.

This checklist will throw light on the different types of cyber insurance coverage, debunk common misconceptions surrounding cyber insurance and more.

Contact us at (608) 755-1524

The Computer Center

What is cyber insurance?

Cyber insurance is an insurance policy that can help your business recover financially from cyber incidents such as data breaches, malware attacks, ransomware attacks and more. Complying with your policy requirements increases your chances of getting reimbursed for audits, forensics, compliance fines, lawsuits and even extortion.

3 main types of cyber insurance

There are various cyber insurance plans that providers might offer you to meet your specific business requirements. However, here are three key types of coverage every small business owner needs to be aware of:

1. Cyber theft: Cyber theft insurance protects your business from liability if sensitive customer information, such as health data, social security numbers, credit card numbers, account numbers and driver's license numbers, is compromised.

This type of cyber insurance provides first-party coverage that financially protects your company from embezzlement, scams, payroll redirection and gift card scams. You don't have to worry about lost revenue caused by operational outages as long as you have first-party coverage and meet your policy requirements.

2. Cyber liability: Data breaches and malicious software attacks can incur high costs for your business. Cyber liability insurance can protect your business against these costs. It covers all expenses related to third parties such as customer notification, credit monitoring, legal fees, fines and other costs.

Some providers even cover legal fees and expenses associated with potential damage to partners, customers or employees as a part of third-party liability.

3. Cyber extortion/ransomware: A cyberattack or threat of an attack associated with a demand for money or another response in exchange for preventing or resolving the assault is cyber extortion. Gaining access to a company's networks and exploiting vulnerabilities or valuable targets are the goals of cyber extortion attacks.

This type of insurance typically covers expenses for ransom, negotiations, forensics, system rebuilding and business interruption.

Don’t fall for these cyber insurance myths

There are many myths and misconceptions surrounding cyber insurance even though the value of cyber insurance is being recognized more and more. Knowing the real facts regarding cyber insurance is crucial if you want to maximize your chances of being accepted for coverage and receiving a payout in the event of a breach.

Let’s look at the top three myths:

Myth #1: All my small business needs is a cyber insurance plan to cover the costs of a cyber incident.

Truth: A cyber insurance policy will only cover you if you have the cybersecurity measures stipulated in the contract, so it’s highly unlikely your application will be accepted if you aren’t compliant. Also, if you get coverage and fall out of compliance later, your insurance provider can deny your claims in the event of a breach.

Myth #2: Cyber insurance is easy to get

Truth: With the rate that cybercrime is spreading and the amount it is costing organizations, insurers are understandably becoming reluctant to take on so much risk. While receiving cyber insurance coverage is not impossible, it’s tough and growing more expensive and harder to obtain.

Myth #3: If I have a cyber insurance policy, my claims will be covered if I experience an incident

Truth: If you can’t prove you’ve adhered to your policy’s terms prior to, during and after a cybersecurity event, it’s very likely that your claim will be denied. You can’t just “set it and forget it” when it comes to cyber insurance coverage.

Cottage Health and Columbia Casualty case study

Cottage Health System is a Southern California-based, nonprofit hospital network that had a NetProtect360 claims-made policy with Columbia Casualty. The company experienced a data breach involving around 32,500 private medical records in the fall of 2013.

Columbia is now suing Cottage for a declaratory judgment, claiming that the firm is not obligated to defend or compensate Cottage because they didn't abide by the terms of their policy.

Cottage committed to maintaining certain minimal risk controls as a condition of their coverage, which Columbia claims they failed to do. Columbia also claims that Cottage submitted false answers to the "Risk Control Self-Assessment" in their insurance application.

Columbia Casualty has petitioned the court, claiming that it is not legally obliged to pay a $4.1 million compensation in litigation because the hospital system failed to:

- Constantly monitor and maintain security patches on its system
- Reassess its information security exposure and enhance risk controls
- Have a system in place that can detect unauthorized access or attempts
- Access sensitive information stored on its servers
- Control and track all changes to its network to ensure it remains secure

How an IT service provider can help

Navigating the world of cyber insurance can be difficult for a small to midsize organization like yours with limited resources and budget. While partnering with an IT service provider doesn't ensure coverage or payment in the event of an incident, they can implement best-in-class cybersecurity solutions and help you adhere to your policy's requirements, maximizing your chances of qualifying for coverage and payout in the event of a breach.

Contact us for a no-obligation consultation today to find out how we can help.