McGowanPRO

Professional Liability Insurance

Protecting Your Business: A Cyber Insurance Overview

Forty-three percent of cybersecurity data breaches involve small businesses. The idea that only large companies are at risk of cyberattacks has been popular in the past, but only because they are most often reported on in the news. Instead, investigations such as Verizon's Data Breach Investigations Report have found that small businesses are just as at risk (if not more so). Cybercriminals will find weaknesses in any organization, contributing to a nearly $7 billion loss of revenue in the United States every year.

With more of our lives becoming increasingly digital, everyone within an organization is vulnerable to cyberattacks. To combat this, businesses of all sizes should consider investing in cyber insurance. From covering the costs of lawsuits and cyber extortion to offsetting the costs of a data breach, cyber insurance protects businesses against external threats.

This Ebook will share a comprehensive cyber insurance overview, highlighting why businesses should invest in cyber protection and how to decide on the right insurance for their needs.

What is most at risk?

One of the top targets of cyber criminals is personal information, as it gives criminals an easy way into an organization's digital infrastructure that is difficult to detect.

Common private information at risk includes:

- SSN (Social Security Numbers)
- Credit Card Numbers
- Bank Account Numbers
- Personal Names
- Home Addresses

The reality is that businesses hold much of this information within their databases, either for their employees or clients. It is crucial to understand that this information can be exposed or easily accessed, necessitating steps to mitigate a business's security weak spots and potential liability. The key to that is cyber insurance.

What exactly is cyber insurance?

Also referred to as cyber risk insurance or cybersecurity insurance, cyber insurance offers coverage for everything from malware to denial-of-service (DDoS) attacks.

As an insurance product specifically designed to help businesses address the potentially company-ending effects of cybercrime, each instance of cyber insurance has to be personalized to help a company mitigate its specific risks.

Cyber insurance is no different from protecting against incidents such as natural disasters or physical risks. Cybercrime is often a question of if, not when, and insurance coverage is there to protect against that eventuality. Small businesses do not always have the resources to combat a breach and recuperate their losses, whereas cybersecurity insurance ensures these attacks do not permanently cripple a business.

What should your cyber insurance policy cover?

Cyber insurance plans cover a wide range of cyber risks while often offering coverage for business income losses or even physical damage to hardware. Each plan can (and should) be personalized to an individual business's needs and its current security outlook.

When preparing a cyber insurance overview, businesses should ensure policies include the following:

- Lost device coverage
- Assistance during a ransomware attack
- Computer forensics
- Global cyber attacks
- Theft of personal information
- Data breaches for third parties, such as vendors
- Terrorism

Businesses must also consider whether their insurance will provide coverage beyond pre-existing insurance. They need to be confident that their provider will defend them in the case of a lawsuit or regulatory investigation and offer a hotline available at any time during the day and year.

The difference between first-party and third-party coverage

Businesses must also be knowledgeable about first-party and third-party coverage when building a cyber insurance overview. The difference is the type of protection they provide.

First-party coverage protects data. This includes customer's and employee's information. With first-party coverage, protection is primarily focused on a business' costs. This could include legal counsel, replacing or recovering lost or stolen data, business interruption income losses, crisis management, etc.

Third-party coverage instead protects a business from a third-party vendor seeking to bring claims against it. Perhaps a business needs to pay out consumers affected by a data breach, or it needs coverage for losses from trademark infringement.

Together, the two types of coverage safeguard a business against a sudden data breach and the often crippling costs associated with it. Small businesses are vulnerable not just to being targeted but also to the operating expenses of legal counsel, settlements, accounting costs, and far more. With the right insurance, these businesses can rest easy knowing that if a cyberattack were to occur, its effects would be massively reduced.

Is cyber insurance alone enough?

While having comprehensive cyber insurance coverage goes a long way to address the potential damages of a breach, businesses still need to invest in an overall plan to manage their cyber security.

This is for two reasons. The first is that, as with insurance, prevention is the best way to protect a business. Cyberattacks are more common for companies that haven't fully trained their staff to be aware of potential data breaches, such as increasingly subtle phishing schemes. Having a cyber awareness plan and mandatory training can significantly mitigate the risk of a damaging attack.

The second reason is that cyber risk insurers will investigate a company's cybersecurity readiness. Better coverage is often dependent on a solid security posture. The more a company can prove that its enterprise security is well-equipped before securing insurance, the more likely it is that an insurer can be confident in an organization's security posture.

Businesses of all sizes should take the time to invest in training, cyber security readiness plans, and risk assessments to shore up any weaknesses in their defenses. It'll help protect their business while securing the best insurance available.

Which cyber insurance should a business choose?

Companies that have taken the time to prepare their organization and prepare their cyber insurance overview now need the best insurance available.

McGowanPRO Information Security and Privacy Insurance provides a variety of industry-leading coverages, protecting businesses from emerging data security and privacy concerns.

Its coverage includes:

- **Information Security & Privacy Liability:** Covering theft, unauthorized access, destruction of data, or unauthorized disclosure of non-public information (personal or third-party). It also covers a business that fails to comply with state breach notice laws, privacy policies, and government-mandated theft protection programs.
- **Privacy Notification Costs:** Coverage for costs associated with compliance with a breach notice law and the costs of hiring an expert to investigate a security breach.
- **Regulatory Defense and Penalties:** Covering the costs of defending a regulatory proceeding resulting from privacy law violations.
- **Website Content Media Liability:** Covering the display of electronic content on a business' website. Offline media coverage may also be available.

In the event of a cyberattack, your company will need support. Contact us today to learn about McGowanPRO's industry-leading coverage options.

McGowanPRO
Professional Liability Insurance

Contact us:

l Squared Insurance Agency LLC

2430 Camelot Ct SE

Grand Rapids MI 49546

Info@L2Ins.com

L2InsuranceAgency.com