



Sirtawn Systems

Start Fighting Cyber Crime with Knowledge and Action.

Our Newsletter for Issue #173 is dedicated to Cyber Insurance.

**Cyber Insurance 101
Guide for Small Businesses**

Why is Cyber Insurance Important?

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.

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.

Myths about Cyber Insurance and Cyber Security.

- 1. Cyber Insurance does not equal Cyber Security!**
- 2. Cyber Security does not equal Cyber Insurance!**
- 3. You can not have Cyber Insurance without Cyber Security!**
In fact, most Cyber Insurance Policies will not pay out if proper cybersecurity are not in place and can be proven to be effective.

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.

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.



6 Important steps to help your decision-making process:

1. **Coverage Assessment:** Ask if the policy addresses cyber-risks unique to your business.
2. **Evaluate Limits:** Check if the policy can effectively cover the financial impact of a cyber incident or a disaster.
3. **Identify Gaps:** Scrutinize the policy for gaps to ensure your business is adequately protected.
4. **Response Plan:** Analyze the effectiveness of the included incident response plan.
5. **Cost Evaluation:** Study the pricing structures of different policies to find a fine balance between affordability and coverage.
6. **Check Insurer's Reputation:** Choose an insurer who has a positive track record of processing claims.

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.



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.

TOP 5 Reasons a Cyber Insurance gets Denied:

Poor prevention practices, Third-party or contractor fault, Accidental errors and omissions, Failure to document preventative measures and/or Coverage doesn't extend beyond interruption timeframe.

To ensure your claims don't get denied:

1. **Complete the application accurately:** Provide detailed and precise information while applying for cyber insurance.
2. **Notify insurers on time:** Swiftly inform insurers to initiate & expedite the claims process.
3. **Strengthen security practices:** Continuously upgrade cybersecurity in line with industry standards.
4. **Maintain documentation of security controls:** Preserve evidence of precautions taken for claims processing.
5. **Document losses and costs:** Create detailed records of losses and costs to support claims for appropriate payouts.
6. **Seek professional advice:** Consult experts for insights on optimizing coverage and claims.

Key Considerations When Selecting the Right Cyber Insurance Coverage

In today's threat landscape, businesses that want to secure their future must have good cyber liability insurance. However, navigating the cyber insurance market on your own can be challenging, with no guarantee that you'll find the right policy for your business.

To make an informed choice, you must understand the basics, such as how first-party insurance shields you from direct losses while third-party insurance handles external claims. To ensure a safe future for your business, you must equip yourself with the right knowledge.

In Summary:

Strategize to Choose the Best Cyber Insurance

Finding the right insurance for your business can be an overwhelming task. Even if you manage to navigate the maze of jargon and diverse offerings, meeting eligibility criteria isn't a certainty.

So, here's a simple strategy for you. Start with understanding the coverage limits, identify gaps, consider the costs and validate insurers' reputations. Insurance is the key to keeping your business safe. Make the right choice.

The Role of Cyber Insurance in Proactive Risk Management

Wondering how to future-proof your business? Start by learning the why, who and how of cyber liability insurance. Discover why all businesses need cyber insurance to shield themselves against cyberthreats.

Consider taking the help of an IT service provider to fortify your business against digital threats and maximize your chances of a payout.

Our Assessment Offer



This monthly publication provided courtesy of Barry Brown, President of Sirtawn Systems.

FIGHTING CYBERCRIMINALS ON YOUR OWN CAN BE TIRING WHEN YOU HAVE A BUSINESS TO RUN.

CONTACT US TODAY

FIND OUT WHAT IT'S LIKE TO HAVE OUR CYBERSECURITY EXPERTS IN YOUR CORNER.

We are offering a FREE Network Security Audit with no obligation. You will receive a "Cyber Security Audit" outlining our findings following the audit. Again ... **NO Obligation....**

Sirtawn Systems

Your Cyber Security Experts

Phone: (905) 947-1636

Website: www.sirtawn.com

Email: sirtawnsystems@gmail.com