



Cybersecurity Insurance Buyer's Guide:

5 Tips to Consider When Buying Cybersecurity Insurance

Understanding your risks and what's required of the business by policy issuers is paramount.

Most people aren't aware of what to look for when buying a cyber insurance policy. Since it is still a novel concept, you first need to determine your cyber risk, your risk tolerance and the costs of things that don't have a clear monetary value (e.g., injury to your business's reputation). What's more, some insurance companies are still not fully certain as to how to underwrite cyber-insurance policies.

To assist you in overcoming these challenges, we have assembled a list of our top five tips for buying the best cyber insurance policy for your business.

- 1. Determine Your Cyber Risk**
- 2. Examine the Policy Terms Carefully**
- 3. Be Certain It's Right For Your Needs**
- 4. Ensure You're Clear About Exactly What Comes with Your Policy**
- 5. Know What Your Responsibilities Are**

1. Determine Your Cyber Risk

When you are considering the purchase of cyber insurance, you should begin by making an assessment of your cyber risk. The nature of these risks will be critical to identifying the right type of insurance for you.

For instance, think about whether or not you use the cloud to keep payment information, personal data, or other important sensitive information (as opposed to less sensitive data like inventory or sales figures). Does your company make secure transactions, like wire transfers? These considerations should be taken into account as you evaluate your business's cyber risk and search for the best policy plan.

2. Examine the Policy Terms Carefully

Don't skip the fine print. It's important to carefully read through the terms of any cyber insurance policy before you sign. Make sure you understand all the provisions and ask questions if needed. Bear in mind that different policies might have different definitions of certain situations (for example, what constitutes a "security event" can vary).

A thorough examination of the policy's terms will also help you ensure that the policy matches your company's risk level.

3. Be Certain It's Right For Your Needs

Cyber insurance policies are not a "one-size-fits-all" proposition. The policy will only serve your organization well if it is an appropriate fit. This means you must devote some time and effort to understanding what the cyber insurance policy offers and how its coverage can help your company mitigate its particular risk factors.

Almost every organization could benefit from a cyber policy known as "Business Interruption Coverage." Typically, you should expect a waiting period prior to this coverage starting. As soon as it does, it is good for

Cybersecurity Insurance Buyer's Guide

covering losses due to downtime your business may experience as the result of a cyber-attack or incident covered by the policy.

“Contingent Business Interruption Coverage” is also a useful policy, as it is designed to help with financial losses that may be incurred if a partner that you do business with can't offer their usual services as a result of a cyber incident.

4. Ensure You're Clear About Exactly What Comes with Your Policy

It's possible that your existing insurance portfolio offers coverage for some cyber- attacks and incidents, which is why it is critical that you know exactly what your policy covers.

Were you aware that cyber insurance frequently includes access to experts such as cybersecurity consultants and lawyers who can offer their assistance if you encounter a cyber incident? Boasting significant expertise in cyber-related matters, these experts will guide you on legal issues, privacy concerns, regulations, security, and other issues. This access to experienced professionals is particularly important for smaller companies that may not have the necessary resources to address a cyber incident.

5. Know What Your Responsibilities Are

Finally, make sure you know precisely what your responsibilities are under the cyber insurance policy you choose. For instance, do you know who to notify if there is a breach in security? What if you only just discovered that someone has been infiltrating your system for a long period of time - what do you do? (In that case, a retroactive cyber policy would be useful.)

Being fully aware of what you must do in the event of a cyber incident can affect whether or not the insurance plan ultimately covers you. In the cyber world, we call it an “Incident Response Plan.”

To discuss your cyber security needs, contact us at 774.204.0700 or info@towerwall.com

Read Next

MDR Buyer's Guide: 7 Things to Consider When Choosing Managed Detection and Response



- What is MDR
- What to look for when you shop for MDR services.
- Finding the Right MDR Solution for You

[Read Now](#)

towerwall



Cybersecurity Insurance Buyer's Guide

Above all, do some serious thinking before making a purchase to ensure you get it right. The probability that you will need to rely on a cyber insurance policy increases every day. Your cyber insurance plan's requirements around providing notice of a claim and getting the insurance company's consent prior to responding to a cyber incident should be factored into your business's comprehensive incident response protocol.

Additionally, put together a team of experts who have knowledge of cybersecurity to make the initial cyber insurance application. If you do that and take the advice above to heart, you will have greater success in buying the right cyber insurance policy for your business.

Finally make sure your company is following all the cyber insurance requirements such as ransomware protection, documented cyber programs, and user awareness training, to name a few. Otherwise, your policy could be null and void.

Ready to take the next steps on Cyber Insurance?

Leverage our expertise to make sure you are
fully protected when you need it the most.

Call us today at 774.204.0700

Email us at info@towerwall.com

The front line of cybersecurity.™

For over 20 years, Towerwall, a woman-owned business, has helped scores of companies safeguard their data and leverage their investment in IT. Our experience in all facets of information security coupled with serving in the CIO/CISO/ISO roles provides a unique understanding of the security challenges organizations face daily.