




12 Questions to Ask Your Cyber Insurance Provider


Not all cyber insurance plans are created equal, so it's essential to ask the right questions to ensure your coverage matches your organization's needs.


We're not insurance agents, but Defendify has helped many organizations navigate the complicated and changing insurance landscape. We've compiled a list of questions to help you in the conversation with your insurance agent or provider.


-  **What is covered under this policy?**


Cyber insurance can help mitigate risks and costs of a cybersecurity incident. Policies typically cover losses associated with remediation, restoration, notification, and more.
-  **Are there losses or types of incidents that are specifically excluded or not covered?**


Like other types of insurance policies, cyber insurance may exclude coverage for certain types of losses or incidents that arise from Bring Your Own Device (BYOD), acts of war, or social engineering. It is important to understand what is and is not covered.
-  **Does the policy reimburse for loss of revenue from downtime or business interruption?**


Whether it's included in your policy or requires an additional enhancement, you'll likely want to ensure you're covered for lost profits and any fixed expenses incurred during your business interruption.
-  **Is there a minimum downtime before the policy takes effect?**


Most policies have a waiting period of several hours to several days before the provider will respond. Since cyberattacks can escalate very quickly, you'll want to watch for long waiting periods and decide what length of time is acceptable.
-  **What are the minimum controls or security requirements?**


Insurers may require minimum security requirements to obtain coverage and will often require a thorough risk assessment before issuing a policy. These minimum controls may include enabling multi-factor authentication, conducting employee security awareness training, using encryption, having policies and plans, scanning for and patching vulnerabilities, and more.
-  **If we implement additional security measures, can we reduce our premium?**


It may be worth the investment in additional security controls if you demonstrate that you can reduce your risk. As a result, your insurer may be willing to reduce your premium.
-  **How will our premiums be affected if we have a security incident?**

Some providers may increase premiums, especially if minimal or no attempts are made to remediate the security gaps that lead to a breach. Depending on the size and scope of your incident, this answer may shape whether or not you file a claim.
-  **Are there any notification requirements in the event of an incident?**

It is essential to check what your obligations are before an incident occurs. Not correctly following their procedures could potentially result in a claim not being paid. It's like seeing an out-of-network doctor and your health plan not covering the bill.
-  **Is there retroactive coverage for unknown attacks that stemmed from before the policy's effective date?**

An attacker may have gained a foothold several weeks or months before they are uncovered. If initial access or other parts of the attack occurred prior to the date you obtained your policy, you might not be covered.
-  **What are our ongoing requirements to maintain coverage?**

Many providers require a regular audit or review of the security measures you reported when you applied for coverage. Understand the expectations around maintaining your current security program to help ensure your policy and insurer will respond if needed.
-  **Are there any geographical limits?**

With the digital transformation over the last few years, companies have hired outside their traditional geographical area. There may be restrictions if you conduct business internationally or use cloud-based data storage providers with servers in another country.
-  **Can the coverage be modified?**

The cyber landscape changes constantly. You may want to be able to adapt and adjust your policy to reflect your risks. The other side of this is whether the cyber insurance provider can modify, reduce or eliminate coverage due to the changes in the threat actor tactics.