Rehmann

Are you covered?

4 Key Factors to Consider for Cyber Insurance

Every organization carries the risk of a cyber-attack. Because of this, taking proactive measures is critical for incident recovery as well as continued operations.

As the cybersecurity landscape continues to evolve, the requirements and complexities of acquiring and renewing cyber liability insurance are changing. Cyber insurance is a young industry that has experienced significant losses in recent years. Insurance companies are adapting to try to mitigate these losses by requiring more detailed documentation and setting stricter cybersecurity standards. Now, obtaining coverage puts a greater burden on organizations throughout the application and attestation process.

Be sure to consider these 4 factors to ensure you sign on for the right coverage to secure your organization.

Allow ample time to secure coverage.

Applying for cyber liability insurance is a time investment. Be prepared to complete longer, more complex attestation statements and provide extensive details for coverage.

Be proactive and allow at least 60-90 days to gather information and complete each part of the submission accurately. Be sure to build in time to put the right infrastructure or processes in place to meet heightened requirements, and to thoroughly review your submission.

Analyze your risk.

Each record held by your organization has a street value to a threat actor — every piece of a record's data has a price tag. While data record values vary by industry, the global average cost per record in 2022 was $164.

As you prepare to apply for the first time or renew an existing policy, evaluate your records to better understand and estimate your financial risk and your potential level of exposure.

These data points will help determine the coverage you should consider.

Consider the impact of downtime.

An organization's average downtime from a cyber-attack can range from 7 to 21 days.

If you can't deliver products or services — or collect revenue — imagine the severe impact that could have on your bottom line.

How much downtime can you afford? Analyze your internal operations to gain insight into what amount of downtime is acceptable to your organization. This will help you determine the coverages that may be needed and identify any required business continuity strategies. This analysis will also create the opportunity to build an effective incident response plan. Incident response plans have proven effective to reduce overall downtime, reduce costs and speed response when using an updated and regularly tested plan.

Evaluate your cyber hygiene to ensure full compliance.

Your cyber insurance provider will take a close look at your organization's stated policies for IT security, as well as for demonstrated compliance across all operations.

It's not enough to say you have a solid security framework in place. If you attest to specific measures or protections, but the insurance company finds they are not in active use, you face the risk of declined coverage, fines or other penalties, or even a lawsuit.

Verify all the information you provide and take corrective action if necessary. A credible technology partner can help you review your policies, protections, and preparedness to ensure a smooth application and renewal process — and seamless coverage when you need it most.

To ensure appropriate cyber risk coverage for your organization, consider these 4 factors and work with a credible technology partner to help you prepare accurate attestations. Your technology partner can also recommend changes or updates to your security protocol.

It's no longer a matter of "if" a cyber-attack will happen, it's a matter of "when." Make sure your organization is protected — and prepared.

616.222.9200 rehmann.com

Rehmann