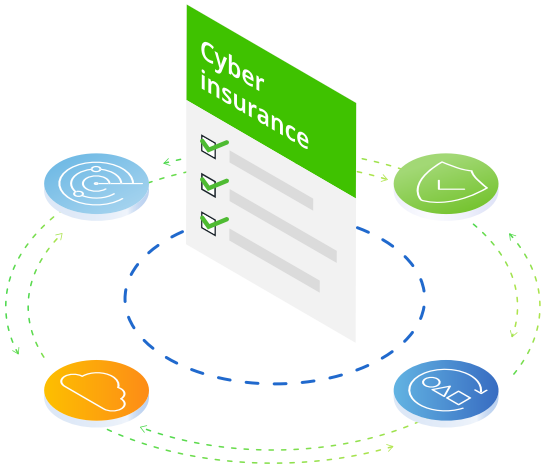
COHESITY

TIP SHEET

5 essential cyber insurance questions

What to know with ransomware soaring



It's no secret that ransomware is rampant, affecting all industries, both private and public sector. While many businesses already have cyber insurance, interest has spiked more broadly given the considerable chance of attack.

Key Challenges

- Coverage limitations and exclusions
- Difficulty in quantifying risks
- Lack of standardization
- Confusion about coverage
- Low adoption rates

What is cyber insurance?

Cyber insurance is an insurance policy that provides financial protection against losses resulting from cyberattacks, data breaches, and other cyber-related incidents. It may cover costs related to lost income, legal fees, data recovery fees, and the cost of hiring a public relations firm to help with damage control to a company's brand. Cyber insurance policies typically include coverage for both first-party (direct) losses (such as lost revenue or data recovery costs) and third-party losses (such as legal costs and settlement payments).

However, insurance companies have now realized that the prevalence of ransomware, and its focus on backup systems, has significantly increased their liability. For this reason, the ability to gain cyber insurance, or maintain it, has changed.

Read on for the five essential cyber insurance questions—and which key features these insurance companies may require in backup and recovery systems for applicants to qualify.

1. What are typical qualifying considerations for cyber insurance?

- **Data security measures**: Insurance companies will often review a business's data security measures, such as password policies, data backup procedures, and incident response plans, to determine eligibility for coverage.
- **Data breach history**: Insurance companies will typically ask about a business's history of data breaches and its efforts to prevent them, as well as the types of data the business collects and stores.
- **Revenue size**: Some insurance companies may have minimum or maximum revenue requirements for businesses they will insure.
- **Geographical location**: Some insurance companies may only provide coverage to businesses located in certain countries or regions.
- **Type of business**: Some insurance companies specialize in providing coverage for certain industries, such as healthcare or finance, and may have specific qualifications for those industries.

It's important to note that these, and other qualifications, can vary by insurance company and by policy, so it's essential to review the terms and conditions of all policies carefully. It's also a good idea to work with a trusted insurance broker who has experience with cyber insurance to help find the right coverage for your business.

2. What internal security controls are needed to qualify for cyber insurance?

Internal security controls are essential for reducing the risk of a cyberattack and improving the chances of a successful recovery in the event of a breach. Here are some internal controls insurance companies may look for when evaluating a business's eligibility for insurance:

- **Robust access control policies**: Implementing strong passwords and two-factor authentication, and regularly monitoring access logs, can help prevent unauthorized access to sensitive data.
- **Strong data encryption:** Encrypting data both in transit and at rest can protect sensitive information from theft or unauthorized access.
- **Regular software updates and patches**: Keeping software up-to-date with the latest security patches can help prevent vulnerabilities from being exploited by cybercriminals.
- **Comprehensive incident response plan**: Having a comprehensive incident response plan in place—including a data recovery plan, whether for a cyberattack or disaster recovery—can help ensure a timely and effective response in the event of a breach or data loss.
- **Ongoing employee training**: Providing regular security training for employees can help them recognize phishing scams and other cyber threats, and understand best practices for maintaining the security of sensitive data.
- **Vulnerability assessments and penetration testing**: Regularly conducting vulnerability assessments and penetration testing can help identify and address potential security weaknesses before attackers can exploit them.

Having these security controls in place—and regularly reviewing and updating them—can demonstrate to insurance companies that a business is making cybersecurity a priority and is trying to reduce the risk of a breach.

3. What are some key elements of a good backup and recovery policy when it comes to applying for cyber insurance?

With the growing threat of cyberattacks and the increasing need for businesses to protect against them, insurance companies are becoming increasingly focused on security measures, including backup and recovery. In addition to strong internal security controls, they may require applicants to demonstrate that they have the following modern backup and recovery capabilities in place to qualify:

- **Multiple backup copies**: Keeping multiple backup copies in different locations can help protect against data loss in the event of a disaster whether cyber, natural, or man-made.
- **Immutable backup snapshots**: Cybercriminals have become sophisticated and now target the backups themselves. Having immutable backup snapshots that cannot be modified contrasts with traditional systems where backups can be updated or deleted. Software-based, native immutable backup snapshots provide a secure copy of the data that can be used to restore systems in case of data loss or corruption. They're also useful for forensic investigation, regulatory compliance, and ensuring the integrity of the data before recovery.
- **Strong access controls**: Using role-based access controls (RBAC) and multifactor access (MFA) helps ensure only authorized users have access to sensitive information. The goal of strong access controls is to prevent the unauthorized access, modification, or theft of this valuable data, which is why modern systems provide quorum controls in addition to MFA. Quorum provides an extra layer of security, ensuring that multiple users are involved in the decision process, to reduce the risk of unauthorized access or misuse.

- **Air gapped or isolated backup copies**: According to a Gartner strategic planning assumption, by 2025, at least 75% of IT organizations will face one or more attacks.[1] This is why some insurance companies are now looking for air gapped backups. Storing backup copies in a separate network via air gapped or isolated location—such as in a cyber vault—can help ensure backup data is available for recovery after an attack.
- **Backup integrity scanning**: Checking the integrity of backup data ensures that the data being restored is complete and accurate, and free of malware. This is a complementary capability to security solutions that scan production data and endpoints. Scanning backups ensures that as new malware is identified, it is not introduced back into the organization during a recovery process. Cyber insurance policies may ask about the ability to test the integrity of the backups to be free of malware. Modern systems with integrations from cybersecurity providers like Tenable help IT identify vulnerabilities, so they don't get reintroduced into production environments during a recovery.
- **Instant mass restore**: Utilizing capabilities like instant mass restore allows for rapid restoration of multiple systems simultaneously, thus reducing time and minimizing the impact on resources. The speed and scalability of instant mass restore allows organizations to quickly return to normal operations. Some cyber insurance applications request estimated recovery times for a successful restore from backups.
- **Tested recovery processes**: Regularly testing the recovery process can help ensure that backups can be successfully restored in the event of a data loss—and reduce the risk of data loss due to human error. Some insurance organizations are asking for assurance that a successful restoration of servers and data has occurred within the last six months.

Having these backup and recovery capabilities in your solution can demonstrate to insurance companies that a business is taking proactive steps to protect against data loss and minimize downtime in the event of a cyberattack. This can help increase the chances of a successful recovery and may improve the ability to purchase cyber insurance and its terms and conditions.

4. What role does cyber insurance play in a data protection strategy?

Cyber insurance is one part of a comprehensive approach to protecting your business against cyber threats. Here are some additional steps to enhance your cybersecurity posture:

- Implement strong passwords and two-factor authentication. Use different passwords for your backup system than those you use for other administrator credentials.
- Regularly update software and apply security patches.
- Regularly back up important data and store it offsite in a cyber vault, perhaps in the cloud.
- Train employees to recognize phishing scams and to follow best practices for security.
- Conduct regular security assessments, including vulnerability scans and penetration testing.
- Develop and regularly update all incident response plans.
- Stay up to date and informed about the latest cyber threats and trends, and understand the regulations that apply to your business or industry.

[1] Minimize Risk by Better Knowing and Managing Your Data, Michael Hoeck, Gartner, December 2022

5. Is cyber insurance necessary for my business?

Whether cyber insurance is necessary for your business depends on several factors, including the size of your business, the types of data you collect and store, and the potential impact of a data breach or cyberattack.

If your business stores sensitive customer information, handles financial transactions, or relies on technology for daily operations, it's particularly vulnerable to cyber threats. In such cases, cyber insurance can provide critical protection against financial losses, reputational damage, and legal liability in the event of a breach.

Large enterprises, and even small businesses, can benefit from cyber insurance, as the cost of a breach could be substantial and possibly devastating for a business, regardless of its size. By purchasing cyber insurance, you can transfer some financial risk associated with cyberattacks to the insurance company.

Summary

Cyberattack costs in 2023 are expected to reach $8 trillion USD worldwide according to Cybersecurity Ventures. A multilayered security approach is critical to combating ransomware, and cyberattacks more broadly. Cyber insurance, a modern data management and security platform, internal security measures, and personnel training may all play a role in helping to protect your organization's data and recovering it after an attack.

By taking the steps outlined here, and having a comprehensive cybersecurity strategy in place, you can better protect your business against cyberattacks and ensure that you're prepared in the event of a breach.

Cyber insurance can be a wise investment for businesses of any size seeking to protect against the financial consequences of a cyberattack or data breach.

Learn more at Cohesity

COHESITY

Cohesity.com | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110

9100069-001-EN 2-2023