CYBERSECURITY INSURANCE FOR ENTERPRISE

Cybersecurity insurance

protects companies from damages or liability resulting from data breaches and malware attacks. And business is booming—especially in the enterprise sector.

A 2020 Advisen survey of corporate risk managers showed that 78% had purchased some type of cyber insurance coverage.

Why the surge of interest in these policies? Ransomware.

Ransomware attacks doubled in frequency in 2021 over the previous year. Recent studies show that attackers—often well-funded nation-states or organized crime syndicates—are increasingly targeting enterprises.

Worse, it's not just about paying a ransom to release data any longer.

72%

of data breaches targeted large companies

(Verizon Data Breach Investigations Report 2020)

The number of ransomware attacks nearly doubled in the first half of 2021

(Cognyte, 2022)

$1.85 million

—Average overall cost of remediating a ransomware attack in 2021

(ENISA Threat Landscape 2021)

$1,589

—Average cost of a cyber liability policy in 2021 for $1 million in coverage, with a $10,000 deductible.

(Verizon Data Breach Investigations Report 2020)

Enterprises are often victims of double extortion tactics, where a hefty payment is demanded to decrypt locked down data and prevent its publication or sale. Criminals may also threaten DDoS attacks on a target's public-facing websites to disrupt business if the ransom isn't paid immediately.

And in 2021, the FBI warned about bad actors targeting publicly-held companies before a major event such as an IPO or merger. The gangs search for non-public information, then threaten to release any documents that could be financially damaging.

The increase in the severity and number of attacks has enterprises worldwide looking to mitigate their risk and potential financial exposure.

Insurance underwriters are looking to mitigate their own risk as they face a surge in payouts for a growing number of large claims.

Premiums have increased anywhere from 25-80% over the last two years, according to insurance provider AdvisorSmith. Insurers have also reduced coverage limits, tightened their terms and conditions for coverage, and are imposing more requirements on firms seeking coverage.

Increasingly, they are adding exclusions to clarify what cyber events are covered. Some offer ransomware coverage as a costly add-on to another policy or require a separate policy entirely.

Do you need cybersecurity insurance?

Before 2018, data breaches were the biggest cyber threat, so companies holding personally identifiable data, sensitive financial data and proprietary intellectual property were most advised to seek cybersecurity insurance.

With the rise in ransomware, as well as an increase in targeted attacks and advanced persistent threats, enterprises across all industries are targets.

How to evaluate policies

Policies differ widely, so enterprises should work with a knowledgeable broker or agent and examine the fine print closely. The coverage amounts and sub-limits for ransom payments are important, but how the terms define a covered event is equally important. Make sure it effectively covers ransomware, including coverage for extortion demands and payments, and look closely at how extortion is defined. A small nuance in wording can make the difference between coverage granted, and coverage denied.

The policy should include two main types of coverage: first party and third party.

First-party coverage is for damages to your business caused by the cyber incident. Examples include: Costs for legal counsel to determine your notification and regulatory obligations, forensic services to investigate the incident, recovery of lost or stolen data, recovery of your network and systems, customer notification and call center services, fines and penalties related to the cyber incident, cost of crisis management or public relations, and lost income due to business interruption.

Third-party coverage is for claims against your company by others related to the cyber incident. Examples include payments to customers affected by the incident, costs for litigation and responding to regulatory inquiries, and claims and settlement expenses relating to disputes or lawsuits.

Cyber insurance coverage can and should do more than pay claims; good service is vital in helping you respond to the incident. Most ransomware attacks happen after hours and on weekends, so look for a 24-hotline for reporting the incident. Insurers should also have experts who can assist you with legal advice, mount an effective response, negotiate with attackers, and recover your data and systems.

Qualifying for coverage

Having cybersecurity insurance to protect you against losses doesn't mean you can let your guard down. The opposite is true: underwriters won't grant coverage unless you have good cybersecurity measures in place.

At a minimum, you can expect to complete a questionnaire, but some insurers will require an assessment by a cybersecurity firm, possibly including penetration testing to probe your defenses. They may also require that you provide regular, in-depth cybersecurity awareness training across your organization. The depth of your security will impact your coverage limits, premiums, and whether you can get coverage.

Insurance underwriters all have different ideas about what constitutes effective security, but the requirements are typically some combination of the following:

- Use of an endpoint detection and response (EDR) tool that constantly scans the network for threats
- Multifactor authentication for all remote access, on privileged accounts, and for securing backups
- All PCs equipped with endpoint security software that is updated regularly
- Regular employee cybersecurity awareness training
- Regular backups using external media or secure cloud storage that an attacker cannot overwrite, even if administrative privileges are gained
- A strong password policy and secure provisioning process for access rights and permissions
- Regular patching and updates and retirement of systems that are no longer supported
- Email filtering to remove malware and block phishing attacks
- Business continuity and disaster recovery plans in place

Note: This is informational only and should not be construed as legal advice.

Check out our Enterprise grade solutions designed with your cyber risk insurance needs in mind.

LEARN MORE