

Cyber Liability Insurance: What Is Covered, Costs, and Key Considerations

What Is Cyber Liability Insurance?

Cyber liability insurance is a specialized form of insurance that covers organizations for financial losses resulting from cyber incidents including data breaches, network damage, and business interruptions caused by cyber-attacks or malfunctions. This type of insurance is crucial for companies that depend heavily on digital operations and must protect the personal information of customers.

Unlike traditional business insurance policies, which often exclude cyber risks, cyber liability insurance offers coverage for expenses related to recovery from cyberattacks, legal fees, and related settlements. It's tailored to help organizations mitigate the financial impact of cyber threats and ensure business continuity in the face of digital disruptions.

What Businesses Need Cyber Liability Insurance?

Any organization that handles sensitive personal data, operates online services, or relies on computer systems for its core business functionality should consider acquiring cyber liability insurance. Industries like healthcare, retail, finance, and education, which store large amounts of confidential information, are particularly vulnerable to cyber threats.

Small and medium-sized enterprises (SMEs) often mistakenly assume they are too insignificant to be targeted. This misconception can leave them vulnerable to detrimental cyber-attacks. In reality, cyber-attacks often target smaller businesses, and organizations of all sizes can benefit from cyber liability protection.



Cyber Liability Insurance vs Data Breach Coverage: What Is the Difference?

Cyber liability insurance is an overarching policy covering a range of incidents including data breaches, cybercrimes, and system damages. It covers the immediate responses required after a cybercrime and also accommodates the potential lawsuits and legal claims resulting from the incident. This type of insurance is comprehensive.

Data breach coverage is typically a component or an endorsement within a cyber liability insurance policy, specifically focused on the privacy and security breaches involving personal data. This coverage includes costs related to customer notifications, credit monitoring services, and public relations efforts necessary after a data breach incident. It is more narrowly scoped around data-centric incidents, and especially important for organizations that need to comply with data protection regulations.

What Does Cyber Liability Insurance Cover?

Cyber liability insurance policies typically include the following elements:

- **Privacy liability coverage:** Protects organizations from claims due to violations of privacy law or breaches involving sensitive customer information. This can include settlements, legal fees, and other related expenses. This coverage extends to situations such as improper disposal of data, unauthorized access, and failures in ensuring data privacy.
- **Network security coverage:** Addresses losses originating from security failures like unauthorized access, malware attacks, and Denial-of-Service (DoS) attacks. This includes costs for restoring data, repairing system damages, and business disruptions. It might also cover costs related to forensic investigations to determine the cause and scope of a breach.
- **Business network interruption coverage:** Aids in minimizing financial losses when operations are halted due to cyber incidents. This typically includes compensation for income lost during downtime and potentially extra expenses incurred while restoring operations. It can extend to include costs associated with managing the incident, such as hiring expert consultants.
- **Error and omissions (E&O) coverage:** Targets losses stemming from inadvertent omissions or errors in provided services that result in a breach or data loss. It supports handling legal claims alleging negligence. This is particularly important for organizations that provide IT and consulting services, where such mistakes can have significant financial and reputational repercussions.

What Is NOT Covered by Cyber Liability Insurance?

It's also important to understand the limits of a cyber liability insurance policy. Typically, these policies don't cover the following:

- **Resulting loss of future revenue:** Losses stemming from diminished customer trust or altered market conditions following a cyber event. Organizations cannot claim for speculative future profits or rely on insurance to mitigate reputational damage.
- **Property damage:** Generally, cyber liability insurance does not extend to damage to physical facilities or hardware that might occur due to a cyber incident, as most policies focus strictly on digital assets and operations.
- **Loss or theft of intellectual property:** Intellectual property can constitute a substantial portion of a company's value, but most insurance policies don't cover losses resulting from stolen IP.



How Much Does Cyber Liability Insurance Cost?

The cost of cyber liability insurance depends on several factors, including the size of the business, industry, and the amount of sensitive information handled. According to Insureon, on average, small businesses pay about \$145 per month, or approximately \$1,740 annually, for a cyber insurance policy.

This average cost can provide a benchmark; however, premiums can vary widely. For example, 38% of small businesses pay less than \$100 per month, while 33% pay between \$100 and \$200 monthly.

Factors influencing the cost of cyber liability insurance include:

1. **Policy limits and deductibles:** Higher policy limits usually mean higher premiums. Policies typically have per-occurrence limits ranging from \$1 million to \$5 million, and the aggregate limit is the maximum payable over the policy's term. The average deductible for such policies is around \$2,500.
2. **Industry risks:** Organizations in sectors with higher cyber risks, such as IT consulting or cybersecurity, often face higher premiums. These industries may need third-party coverage due to their responsibility for clients' data security.



3. **Coverage type:** The type of cyber insurance purchased also impacts the cost. First-party cyber liability insurance covers the insured's own losses, while third-party insurance covers legal costs if a client holds the business liable for a cyber incident.
4. **Business size and data volume:** The number of employees and the volume of sensitive data managed by the business play crucial roles in determining the premium.
5. **Claims history:** A history of past insurance claims can affect the cost of new policies, with businesses that have filed more claims typically facing higher premiums.

Given the variability, it's recommended to consult with a licensed insurance agent to tailor the policy to the company's needs and obtain the best possible terms.

Key Considerations for Cyber Liability Insurance Policy

When evaluating policies, organizations should consider the following:

Conduct a Technology and Cybersecurity Risk Audit

Comprehensive technology and cybersecurity audits help identify vulnerabilities in the IT infrastructure, assess the effectiveness of existing security measures, and highlight areas needing improvement. Understanding these risks enables organizations to tailor their cyber insurance coverage to their needs.

Additionally, an audit can provide data that can be used to negotiate better terms with insurers, as demonstrating a strong cybersecurity posture can lead to lower premium rates. Audits should be conducted regularly as part of an organization's risk management strategy to ensure coverage remains aligned with current threats and business practices.

Implement Cyber Security Best Practices

Implementing industry best practices in cybersecurity is essential for businesses wanting to strengthen their defenses and manage their cyber liability. Using secure authentication, regularly updating software, and training employees about cyber threats can help mitigate the risk of breaches and cyber attacks.

Following these practices helps protect the organization from cyber incidents and positions it favorably when acquiring cyber liability insurance. Insurers often look for adherence to these standards as indicators of diligent risk management, potentially leading to more favorable insurance terms.

Request Quotes from Multiple Insurance Providers

To secure the best terms and coverage, organizations should obtain quotes from various cyber liability insurance providers. This comparison shopping allows them to understand different offerings, coverage limits, exclusions, and premiums, enabling informed decision-making.

It's also useful to consult with an insurance broker specialized in cyber risks who can provide insights into the most suitable policies for a particular business. This helps ensure the company obtains tailored coverage that addresses all its cyber liabilities and exposures.

Understand What Is and Is Not Covered by the Policy

It is important for organizations to thoroughly understand what their cyber liability insurance policy covers and, just as importantly, what it does not. Clarity on coverage limits, deductibles, exclusions, and the claims process is essential for making insurance claims in the event of a cyber incident.

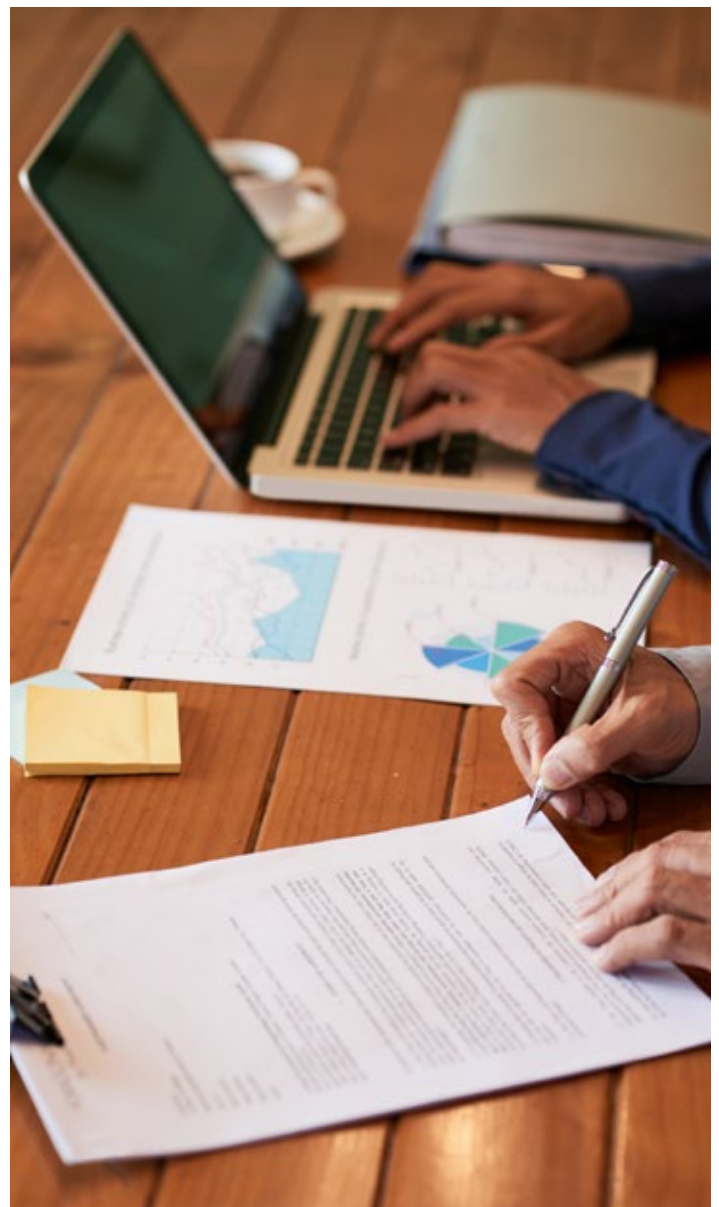
Organizations should also be aware of any responsibilities they have under the policy, such as immediate incident reporting or steps required to mitigate losses. Knowledge of these details

can help maximize the policy's benefits and navigate the aftermath of a cyber incident.

Create a Cyber Incident Response Plan

Having a comprehensive cyber incident response plan is a critical preparation alongside acquiring cyber liability insurance. This plan should outline clear steps to follow when a cyber event occurs, including initial incident containment, communication strategies, and restoration processes.

An effective response plan helps minimize the damage caused by cyber incidents and conforms to the requirements of many cyber insurance policies. Insurers often require insured parties to demonstrate how they will respond to and manage a cyber incident.



Cybersecurity Tools Cover What Insurance Doesn't

Faced with the increase in data breaches, many organizations opt to expand their cyber insurance coverage. While doing so is smart, cyber insurance does not take the place of defense tools.

Extended detection and response (XDR) is a cyber security approach that delivers holistic protection against cyber-attacks. A robust XDR solution has the following capabilities:

- ✓ Identifies hidden threats
- ✓ Tracks threats across multiple components
- ✓ Increase the efficiency of threat investigation
- ✓ Detects and responds faster to active threats
- ✓ Provides full visibility of files, networks, hosts, and users

Using an XDR solution can even help reduce your insurance premium.

The encompassing protection of an XDR solution significantly lowers the risk of a security incident, bringing a consequent reduction of legal claims.

Other benefits of an XDR include:

- ✓ Improved prevention
- ✓ Granular visibility
- ✓ Greater control over access
- ✓ Increased alert accuracy
- ✓ Effective response

[Partner Name]'s Approach to Cybersecurity

Cyber insurance is an important safety net, but it doesn't replace the need for a strong cybersecurity posture. That's why [Partner Name] partners with Cynet, a trusted leader in the industry, to provide comprehensive protection against cyber threats. Cynet's platform delivers powerful threat detection, response, and prevention, backed by top performance in MITRE ATT&CK Evaluations.