5 Ways to Counter Soaring Cyber Liability Insurance Costs

844.638.7328 | SALES@SECNAP.COM | SECNAP.COM

SECNAP
NETWORK SECURITY

What is Cyber Liability Insurance?

This type of coverage assists organizations with the costs of a data breach or malicious software attack. Depending on your plan, expenses covered may include ransomware extortion payments, negotiators, forensic consultation, customer notification, credit monitoring, legal fees, and fines.

You may be wondering if you 'really' need to pay for cyber liability insurance. The right answer is likely 'Yes!' but it depends on your risk appetite. Typically organizations who undergo an attack will outspend what they would have if they actually had coverage. Also with cyber breaches becoming increasingly common, small to medium businesses can face costs that can often take them out of business.

There are two types of cyber liability coverage:

First-Party: covers anything pertaining to your organization

Third-Party: protect businesses that offer professional services to other companies that can be compromised by cyber attacks

Coverage Cost

Let's talk about how much of an investment this would be and where you can save on costs without putting your business at risk. Here is a list of main factors that are often considered when calculating cyber liability insurance premiums:

- Annual Revenue & Employee Count
- Organization Size and Industry
- Amount of Sensitive Data Being Housed such as PII
- Strength of Security Measures
- Required Regulatory Compliance Measures
- Previous history of breaches or insurance claims
- Coverage limits

Top 4 Loopholes Baked into Cyber Insurance Policies

Phishing Maybe Considered Negligence – If your organization is compromised and it is discovered to be due to a successful phishing email, some insurance policies will not cover this. Insurance providers can claim that the organization allowed it to happen due to improper internal risk management and negligence, better known as human error.

Lack of Routine Patching & Maintenance – Your cyber insurance policy may not protect you if your systems are not routinely updated and patched. We recommend performing external and internal security assessments to ensure your most critical issues are addressed in a timely manner.

Incident Only Coverage – Some insurance provider policies may only cover you for the losses incurred during the actual breach, and not cover any financial loss that occurred after the cyber attack.

Incomplete Coverage Due to Changes – If policies are not reviewed in parallel with those changes, there is a chance that coverage may not apply to those environments.

Insurance Landscape

In recent years, cyber liability insurance, which is wholly separate from general business liability insurance, has become a key line item in most organizations' security budgets. While organizations purchasing cyber policies have always had to be cognizant of loopholes and "gotchas," in general, cyber insurance is a sound purchase that helps mitigate the often-staggering costs of a cyberattack. However, as businesses reevaluate their security budgets and coverage options for 2022, they're encountering some nasty surprises.

Cyber liability insurance premiums have spiked as much as 300%. Insurance carriers have begun "sub-limiting" ransomware and cyber extortion incidents and applying co-insurance provisions. This means that policies will cover only fixed amounts for all covered events — and insureds will be made to shoulder more of the risks.

Insurers are also tightening underwriting guidelines and imposing coverage limits on sectors that have been heavily targeted by cybercrime over the past year, including education, healthcare, the public sector, construction, manufacturing, and managed service providers (MSPs). Another way insurers are addressing these issues is by sending detailed questionnaires regarding cybersecurity posture to their customers before the insurer will renew a policy or issue a new policy. The answers to the questions affect the size of the premium the insurer will charge.

Major Contributor to Rising Cyber Insurance Premiums

Why are cyber insurance rates rising so quickly? There are multiple contributing factors, but ransomware is by far the largest. 2021 has been the most prolific year for ransomware on record, and in Q3, ransomware attacks skyrocketed by 148% compared with the same period in 2020.

In addition to happening more frequently, ransomware attacks are becoming far more sophisticated. Recently, the Conti ransomware crime group began launching highly coordinated attacks that involve multiple steps, likely executed by multiple threat actors. The attack begins when an unpatched Microsoft Exchange server is compromised. The compromised servers are used to send phishing emails, which contain links to websites with malicious macro-enabled Excel (.XLS) files, providing threat actors with an initial foothold in the network. Access is then handed over to a different threat actor, who moves laterally through the network, escalating privileges along the way. Finally, this actor hands over access to the Conti ransomware group, which destroys backups and deploys the ransomware payload.

In an effort to strong-arm organizations into paying up, cybercriminals are engaging in double-extortion techniques, which involve not only encrypting data but also exfiltrating it. If the victim refuses to pay the ransom, the cybercriminal will put the data up for sale on the Dark Web.

All this added complexity and added risk caused total ransomware recovery costs to reach $1.85 million this year, more than double the 2020 average of $761,106.

Premiums have spiked as much as

300%

Making Ransom Payments Could Be Illegal

In addition to fearing massive financial losses, cyber insurance firms are concerned about running afoul of the U.S. Department of the Treasury. Last year, the Treasury's Office of Foreign Assets Control (OFAC) advised organizations that facilitating ransomware payments may be illegal under anti money-laundering (AML) statutes. OFAC's logic is that ransom payments may be funneling to foreign threat actors that the office has already sanctioned, and who intend to use the money to fund further attacks against U.S. interests.

In a revised advisory published in early November 2021, the U.S. government's Financial Crimes Enforcement Network (FinCEN) reiterated the importance of due diligence and compliance obligations required by OFAC. The revised advisory reminds insurers and financial institutions of their reporting duties under laws administered by FinCEN, OFAC, and the Department of Justice, and lists a number of "financial red flag indicators of ransomware and associated payments." It also sternly warns that "FinCEN will not hesitate to take action against entities and individuals engaged in money transmission or other MSB activities if they fail to register with FinCEN or comply with their other AML obligations."

How Organizations Can Lower Premiums

To lower their cyber liability insurance premiums, organizations need to take proactive steps to reduce their risks. Here are five, based on the questions insurers ask during the underwriting process.

1. Comprehensive password security policy + MFA

Earlier this year, the White House issued an Executive Order on improving the nation's cybersecurity. The EO was heavy on password security measures, including the use of multi-factor authentication (MFA) — which is something cyber insurers will ask about. Compromised passwords are responsible for over 80% of successful data breaches, and about 75% of ransomware attacks.

For extra protection, organizations should invest in a Dark Web monitoring service. These services scan cybercrime forums for exposed PII and login credentials and notify organizations if their data appears.

2. Limit data collection, and encrypt collected data

Cyber insurance underwriters frequently ask potential insureds whether they collect personal identifying information (PII) and how much PII they have on hand. They'll also inquire about data loss prevention (DLP) measures. Organizations must limit the amount of PII they collect and store, encrypt all PII at rest and in transit, and take additional measures to prevent data loss. In addition to lowering cyber premiums, these best practices help businesses comply with data privacy regulations, such as the GDPR and CCPA.

3. Perform regular penetration testing & vulnerability scanning

A good rule of thumb is that vulnerability scans should be performed quarterly, and penetration tests annually, as well as whenever the organization makes a major change to their data environment, such as switching cloud providers, adding an additional public cloud, or adopting a remote workforce.

4. Conduct employee cybersecurity awareness training

Insurers expect organizations to educate their employees about cybersecurity awareness and best practices, especially regarding password security and avoiding social engineering schemes. This training will be a continuous learning process throughout the employee's time with the organization. For example, regular phishing simulations train employees to recognize malicious emails.

5. Invest in a Managed SIEM solution

Insurers will ask many questions about security log monitoring, including the organization's audit logging policies, anomaly review practices, how frequently logs are audited, and which log analysis solutions the organization uses.

Security information and event management (SIEM) solutions aggregate log and event data generated by organizational assets, such as security software and appliances, network infrastructure devices, and applications. The SIEM analyzes this data, identifies anomalous activity, and generates an alert.

SIEMs simplify compliance, help organizations monitor and secure modern distributed data environments, and demonstrate to underwriters that the organization frequently audits its logs. However, be aware that SIEMs must be monitored by a human staff 24/7 so that identified threats can be responded to immediately. Many organizations invest in SIEMs only to find that they lack the in-house resources to properly monitor their SIEM and respond to incidents.

While premium savings will vary greatly based on an organization's location, industry, cyberattack history, and other practices, implementing these best practices has benefits beyond lower cyber liability insurance premiums. They'll reduce the risk of breaches, ransomware, and other cyberattacks. Preventing an attack in the first place is much better than waiting for one to happen, then hoping that a cyber insurance policy will come close to covering the costs.

For more detail on how to secure your organization against ransomware attacks, download SECNAP's free whitepaper, 8 Proactive Strategies for Ransomware Risk Reduction.

Not Having Insurance, or Relying on Insurance too Heavily

Cyber insurance policies, just like health, auto, and homeowners' policies, have coverage limitations and loopholes. For example, cyber policies generally do not cover breaches due to "employee negligence." This may sound reasonable, but some policies consider an employee clicking on a phishing link to be "negligence," and phishing attacks account for over 80% of security incidents.

Additionally, no policy can cover all of an organization's losses after a cyberattack, especially indirect losses, such as the damage to the company's reputation. Nearly 40% of the average total cost of a data breach is due to lost business and includes customer turnover, lost revenue due to system downtime, and increased costs of acquiring new customers in the wake of a damaged company reputation.

About SECNAP Network Security

Since 2001, SECNAP Network Security has been combining human intelligence with innovative technology to protect organizations of all sizes against cyber threats, including data breaches, ransomware, phishing, and advanced persistent threats (APTs). Our proprietary, patented and patent pending CloudJacketX managed security-as-a-service platform addresses common pain points faced by IT teams, such as alert fatigue, challenges with meeting regulatory compliance requirements, lack of resources, and hidden vulnerabilities.

SECNAP's proactive cybersecurity approach combines ongoing network security assessments with managed detection and response (MDR) services, an advanced SIEM solution, and a patented intrusion detection and prevention system (IDS/IPS) to provide multiple layers of detection and protection, which are monitored 24/7 by our U.S.-based security operations centers (SOCs). SECNAP utilizes proprietary security technologies that were developed in-house.

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations

GSA Advantage!