CFOLC TOOLS LIBRARY

Four Tips for Selecting Cybersecurity Insurance

As organizations embrace digital transformation, they should include a cyber insurance strategy within their risk management program to ensure coverage against ransomware, data breaches and other cyber-attacks.

Insurance companies often struggle to assess their customers' cybersecurity risks. For traditional commercial policies, insurance firms use actuarial models based on historic data going back decades or, in some cases, even centuries. These models enable insurance firms to forecast risk and provide coverage based on highly calculated premiums.

Cyber insurance is a challenge. The expanding threat landscape, coupled with ever-changing technology, makes it too unpredictable and complex for traditional insurance models.

The complexities of cybersecurity risk policies

Organizations must consider a host of dynamic factors -- each with their own risk profile -- when selecting an insurance provider. The cybersecurity insurance space is inundated with varying types of coverage and cyber liability products. An insurance plan may protect a technology provider during a service or product failure, for example, but the same coverage might not cover a service failure caused by a separate cyber event.

Organizations must understand this distinction and ensure they have cyber coverage, combined with technology errors and omissions coverage. This guarantees product failures are covered whether or not they were the result of a cyber event.

As organizations embrace digital transformation, they should include a cyber insurance strategy within their risk management program to ensure coverage against ransomware, data breaches and other cyber-attacks.

The cyber insurance market is complex and confusing. Buyers shouldn't assume they're fully covered by add-ons or bundles through their general liability coverage. This coverage is often only relevant for certain types of incidents or only provides relief in scenarios unrelated to the user's business activities.

How to choose the best policy

Given the complexities of cyber insurance, what steps can buyers and security teams take to ensure they're getting the best coverage for the best price? Here are four steps for success.

1. Improve your cyber hygiene and evaluate your architecture

Assess your company's attack surface using attack surface discovery and evaluation tools or services. Create a list of hygiene risks that should be ameliorated through patching, configuration and other means of remediation. As businesses rapidly transform and adopt new technologies, organizations must reevaluate their architectures. Implement adaptive and context-driven trust models, wherever data and

resources are located, to enable the removal of implicit trust and limit the impact of a potential attack. Good security hygiene and zero-trust architectural principles are steps in the right direction.

2. Understand your third-party risk

In today's interconnected world, risk extends beyond traditional technology perimeters. A third-party risk management program is critical to understand supply chain risks and collect the relevant signals to inform organizations about their attack surface, security hygiene, insurance coverages, and data protection and privacy practices. Continuously evaluate supply chain partners to ensure supplier security and privacy capabilities are up to date, and determine if the data a supplier processes should be limited, as well as whether suppliers should be changed.

When assessing suppliers, it's important not to forget about insurers. They're part of the value chain and a tempting target for criminals. If threat actors can compromise an insurance company, they may be able to access the policy data and associated policy limits on the firm's clients. A supplier risk assessment should look closely at the insurer's own security hygiene, governance, policies and controls.

3. Choose your provider with care

Many of the large and traditional insurance incumbents still use manual, questionnaire-based approaches to measure the risk of an organization. These point-in-time assessments are ineffective for a variety of reasons, one being that the individual tasked with filling out the questionnaire often doesn't know the answers to the questions. Much of the innovation in this space is coming from eager new entrants to the cyber insurance market who embrace data-driven technologies. These disruptors can be much more consultative with enterprises, helping mitigate risks before and during the policy term and enabling them to tailor policies that meet clients' needs.

It's important brokers and insurers understand their clients' business. Insurers should ask questions and get down to the nitty-gritty of what a client's business does and what its risks are to ensure the coverages in its policy are aligned with its risks and incident response plan.

4. Automate where possible

To ensure efficiency and efficacy throughout the entire process -- from attack surface monitoring and third-party risk management to partnering with insurers -- automate as much as possible. Ideally, an organization should be able to operationalize and collaborate around its security posture and supply chain risk data at a moment's notice. Technology can help organizations achieve this goal -- from being able to automatically evaluate configurations and controls in a cloud environment and understand the risks in a supply chain to understanding how an organization looks from an attack surface perspective.

Cybercriminals and ransomware are here to stay, and threat actors continue to look for novel ways to disrupt, exfiltrate data and monetize their operations. Businesses that alter their perspective on cybersecurity, move to technologies that enable the continuous evaluation of risk and partner with the right insurers will be better prepared to protect themselves from worst-case scenarios.

(Source: CFOLC)