Provided by SCS Agency Inc

Contingent Business Interruption Insurance for Cyber Events

In today's evolving risk landscape, organizations of all sizes and sectors face a wide range of cyberthreats. Amid advancing attack techniques and growing hacker sophistication, cyber events can arise from various avenues and cause considerable damage, often resulting in prolonged operational disruptions and associated losses. With this in mind, it's crucial for organizations to secure adequate cyber business interruption (BI) insurance.

This coverage, which is available through the purchase of standalone cyber insurance, can offer financial protection for expenses stemming from an organization experiencing technology failures and related business disruptions due to covered losses (e.g., data breaches, social engineering scams and ransomware attacks). This type of policy may help reimburse operating costs such as lost income, employees' wages and extra expenses.

When securing this coverage, organizations that rely heavily on third parties to conduct digital operations should also ensure their policies include contingent business interruption (CBI) insurance. Such coverage can help pay for operational disruptions due to covered losses that impact essential business partners. Specifically, cyber CBI insurance can reimburse expenses arising from third-party cyber events that lead to digital supply chain disruptions, such as software provider shutdowns or cloud vendor outages.

This article provides more information on cyber CBI coverage and outlines its key benefits.

Cyber CBI Insurance Explained

While cyber BI coverage offers financial protection for operational losses related to disruptive cyber events that directly impact an organization, cyber CBI coverage helps pay for losses due to disruptions in an organization's digital supply chain, including third-party IT providers, vendors and suppliers. The main distinction between the two is that cyber BI insurance applies to losses affecting an organization's internal systems, whereas cyber CBI insurance covers losses involving third-party technology failures.

For instance, if cybercriminals target an organization's internal network in a ransomware attack and temporarily prevent access to this technology, cyber BI insurance may help recoup operating costs incurred during the disruption. On the other hand, if cybercriminals target an organization's cloud vendor in a ransomware attack and the event leads to a system outage that restricts the organization from accessing critical data or using its company website for an extended period, cyber CBI insurance could kick in to help pay for similar operational losses.

Although specific coverage offerings vary between insurers, cyber CBI insurance generally carries the following exclusions and limitations:

- **Certain cyber events and third parties**—Cyber CBI policies often limit coverage to specific cyber events and third parties (e.g., data breaches and software providers only). This means that, in most cases, some cyber events and third parties are excluded from coverage. For example, operational losses stemming from disruptions among third parties responsible for providing basic elements of digital infrastructure (e.g., internet service providers and electrical suppliers) are generally excluded.

- **Technology failures not caused by cyberattacks**—When providing cyber CBI coverage, insurers usually separate third-party technology failures into two categories: security failures and system failures. This coverage often applies to operational losses stemming from disruptions due to security failures, such as cyberattacks, but excludes protection for system failures, such as those caused by human error or technical issues. However, some insurers may offer minimal coverage for system failures, typically restricted by sublimits.
- **Waiting periods**—Cyber CBI insurance comes with a waiting period, which refers to the amount of time that must pass once a loss occurs before coverage can be triggered. The waiting period for such coverage is generally between six and 12 hours. Organizations have to cover operating costs related to third-party cyber events that they incur before this period lapses.
- **Retention and deductible requirements**—Organizations may face out-of-pocket costs through the retention structure listed in their cyber CBI policies. Some policies substitute the waiting period for the retention requirement, while others may include an additional dollar retention requirement for post-waiting period losses. These policies may also include a deductible, which is the amount organizations must pay before their coverage officially kicks in.

Key Coverage Benefits

Cyber CBI insurance can assist organizations in several ways. Some key coverage benefits include:

- **Financial stability**—Cyber CBI insurance can help organizations prevent costly and disruptive third-party cyber events from wreaking havoc on their finances. As cyberattacks continue to rise in cost and frequency and prompt significant operational losses, maintaining financial stability amid these events is crucial.
- **Protection for growing digital supply chain threats**—As organizations become more dependent on third-party IT providers, vendors and suppliers to conduct critical operations, they face greater digital supply chain exposures. Recent high-profile cyberattacks such as SolarWinds, Kaseya and Colonial Pipeline demonstrate the severity of these risks. According to research from IT company Uptime Institute, 80% of organizations have experienced technology outages since 2020, with 70% of operational downtime caused by third parties. Given that many of these disruptions are beyond organizations' control, cyber CBI insurance is vital to safeguard against operational losses from evolving digital supply chain threats.
- **Peace of mind**—Cyber CBI insurance can help ease any stress regarding the risks and potential costs of third-party cyber events. In conjunction with adopting adequate supply chain risk management protocols, strong cybersecurity policies and in-depth business continuity measures, purchasing this coverage can provide ultimate peace of mind by equipping organizations with the resources needed to navigate even the most difficult third-party cyber events.

Conclusion

Cyber CBI insurance can make all the difference in helping organizations stay resilient during disruptive cyber events due to digital supply chain exposures. By reviewing the protection this coverage provides and considering its key benefits, organizations can tailor their cyber CBI insurance to their specific needs.

Contact us today for more insurance solutions.