

Cyber Liability Insurance

As technology becomes increasingly important for successful business operations, the value of a strong cyber liability insurance policy continues to grow. The continued rise in the amount of information stored and transferred electronically has resulted in a remarkable increase in the potential exposures facing businesses.

In an age where a stolen laptop or data breach can instantly compromise the personal data of thousands of customers, protecting your business from cyber liability is just as important as some of the more traditional exposures businesses account for in their commercial general liability policies.

Claims Scenario: Outsourcing Gone Wrong

The company: A national construction company that outsources some of its cyber security protections

The challenge: A construction firm partnered with a third-party cloud service provider in order to store customer information. While this service helped the company save on server costs, the third-party firm suffered a data breach.

As a result, the construction firm had to notify 10,000 of its customers and was forced to pay nearly \$200,000 in incident investigation costs. The incident was made worse by the fact that the firm did not have a document retention procedure, which complicated the incident response process.

Cyber liability insurance in action: Following a data breach or other cyber event, the right policy can help organizations recoup a number of key costs. Specifically, cyber liability policies often cover investigation and forensics expenses—expenses that can easily bankrupt smaller firms who forgo coverage.

What's more, when third parties are involved, managing litigation concerns can be a challenge. By using cyber liability insurance, organizations have access to legal professionals well-versed in cyber lawsuits and response.

Claims Scenario: Pardon the Interruption

The company: An online retail store that relies heavily on e-commerce

The challenge: A small-sized, online retailer partnered with a data centre to host its website and store its data. This is not uncommon, as many small businesses don't have the IT infrastructure to host products, process payments and fulfil orders on-site.

Unfortunately, the data centre was targeted in a distributed denial-of-service (DDoS) attack. As a result of this attack, the retailer's website went down for several days. While functionality was eventually restored, business interruption costs from lost sales and website downtime was over \$165,000.

Cyber liability insurance in action: DDoS attacks are one of many weapons cyber criminals use to infiltrate and disrupt businesses. These attacks can impact any organization that owns a website, regardless of where it's hosted.

Cyber liability insurance is one of the only protections organizations have against costly DDoS attacks and similar disruptions. This is because cyber policies offer business interruption loss reimbursement. Following a disruption caused by a cyber event, policies kick in and help organizations recover from any financial losses.

Learn More About Cyber Liability Insurance

When cyber attacks like data breaches and hacks occur, they can result in devastating damage. Businesses have to deal with business disruptions, lost revenue and litigation. It is important to remember that no organization is immune to the impact of cyber crime. As a result, cyber liability insurance has become an essential component to any risk management program.

Cyber exposures aren't going away and, in fact, continue to escalate. Businesses need to be prepared in the event that a cyber attack strikes. To learn more about cyber liability insurance, contact Nottingham Insurance today.

Benefits of Cyber Liability Insurance

- **Data breach coverage**—In the event of a breach, organizations are required by law to notify affected parties. This can add to overall data breach costs, particularly as they relate to security fixes, identity theft protection for those impacted by the breach and protection from possible legal action. Cyber liability policies include coverage for these exposures, thus safeguarding your data from cyber criminals.
- **Business interruption loss reimbursement**—A cyber attack can lead to an IT failure that disrupts business operations, costing your organization both time and money. Cyber liability policies may cover your loss of income during these interruptions. What's more, increased costs to your business operations in the aftermath of a cyber attack may also be covered.
- **Cyber extortion defence**—Ransomware and similar malicious software are designed to steal and withhold key data from organizations until a steep fee is paid. As these types of attacks increase in frequency and severity, it's critical that organizations seek cyber liability insurance, which can help recoup losses related to cyber extortion.
- **Legal support**—In the wake of a cyber incident, businesses often seek legal assistance. This assistance can be costly. Cyber liability insurance can help businesses afford proper legal work following a cyber attack.