Small Business Insights

The Importance of Cyber Insurance for Small Businesses

Provided by: BHC Insurance

The Importance of Cyber Insurance for Small Businesses

Businesses across industry lines have become more reliant on technology to conduct their operations. However, any digital presence—no matter how small—presents a cybersecurity risk. Whether a business utilizes e-commerce, stores sensitive data or sends emails, it could be vulnerable to cyberattacks.

These incidents can result in large-scale financial losses, regulatory fines and reputational damage. While such consequences can impact organizations of any size, small businesses may find them particularly devastating due to their limited funds and response resources. That's why it's imperative for these businesses to secure cyber insurance.

This coverage can serve as a critical lifeline to small businesses during a cyberattack by helping pay for costs related to data recovery, legal defense, breach notification requirements and public relations efforts. This article provides more information on the value of cyber insurance for small businesses.

Why Small Businesses Should Consider Cyber Insurance

Although every company can benefit from cyber insurance, there are several reasons why this coverage is particularly important for small businesses.

Cyber economy researcher Cybersecurity Ventures reported that 60% of small businesses close their doors for good within six months of experiencing a cyberattack. Fortunately, cyber insurance can make all the difference in keeping small businesses afloat following cyberattacks.

BHC INSURANCE

Here are some key points to consider:

- **Small businesses are top targets for cybercriminals.** Many small businesses assume that cyberattacks are more likely to impact larger companies. Yet, according to international IT services and consulting firm Accenture, 43% of all cyberattacks target small businesses. Threat actors may initially compromise small businesses' software with the end goal of infiltrating larger businesses through supply chain attacks.
- **Small businesses often neglect cybersecurity.** Compared to larger organizations, small businesses typically have lower cybersecurity budgets and related resources. These businesses may also have fewer IT staff and lack the technical expertise to implement and manage effective security measures, leaving them susceptible to cyberattacks.
- **Small businesses aren't training their employees.** Many cyberattacks stem from human error, such as employees accidentally opening email attachments containing malware. Despite this, only 34% of small businesses provide cybersecurity training for their staff, according to IT company Orion Network Solutions. Reduced cybersecurity awareness among their employees could expose small businesses to cyberthreats.
- **Cyberattacks are getting more sophisticated.** Phishing scams and similar incidents are becoming difficult to detect now that artificial intelligence (AI) tools allow cybercriminals to seamlessly mimic a company's tone, language and style. Consequently, the number of small businesses encountering advanced cyberattacks may increase as AI evolves, especially if they lack the expertise to protect against them.
- **Cyberattacks can pose severe financial consequences.** The lost revenue, operational disruptions and legal consequences of cyberattacks can take small businesses months, or even years, to recover from. Even if these businesses manage to recoup the financial losses from an attack, their reputation may be harder to repair.

How Cyber Insurance Can Help

Cyber insurance can help financially protect small businesses from the potentially devastating consequences of cyberattacks by covering a range of first- and third-party expenses. It may also include access to IT forensics, legal experts, public relations advisors, brand consultants and other specialists typically unavailable to small businesses, expediting their recovery capabilities.

Overall, cyber insurance can prove vital in minimizing downtime, restoring data, and limiting financial and reputational harm stemming from cyberattacks. Moreover, securing this coverage demonstrates an organization's dedication to safeguarding essential data, which may boost stakeholder trust.