

Why Do Contractors Need Cyber Insurance

Nowadays, general contracting involves promoting a collaborative digital environment between multiple stakeholders. As a result, contractors generally have access to sensitive client data and systems throughout each project. They also frequently oversee the project's technical and software equipment.

The construction industry is [leveraging emerging technologies](#) to streamline operations and provide clients with better services. However, while these technological advancements increase efficiency, they also create [new weaknesses for cybercriminals](#) to exploit. Vulnerable systems are attractive targets for hackers looking to steal data and disrupt operations.

Emerging threats prompt contractors to strengthen security measures and adopt cyber security policies to protect client data.

Cyber Risks and Exposures for Contractors

Here are some key reasons why contractors should invest in cyber insurance:

1). The Rise of Cybercrime

The FBI reported a [300% increase](#) in cybercrime because of the COVID-19 pandemic. In 2020 alone, [one in six](#) construction companies reported experiencing a ransomware attack.

According to an [industry report](#), social engineering is the leading technique cyber attackers use to target the construction sector. Overall, the estimated [cost of a breach in the industrial sector](#) is about \$5 million. These alarming statistics highlight the need for companies to invest in cyber security.

2). Third-Party Liability

Since contractors are third-party vendors to their clients, they are exposed to stakeholder breach liability when a cyber attack occurs. In addition, there is always a risk of cybercriminals stealing proprietary corporate assets, such as contracts, confidential bids, designs, and intellectual property, as contractors hold valuable client data.

In 2013, [hackers accessed a prime contractor's](#) computers, exposing a government project's plans, server location, and security system designs.

3). Reputational Damage

Contractors rely heavily on client relationships. Without adequate security measures and cyber insurance coverage, clients may feel their assets and information are not protected and refuse to do business with the company. In a successful cyber attack, contractors could suffer irreversible reputational harm that can [drive away future partnerships](#).

Real World Claims Examples for Contractors

Ransomware attacks, social engineering tactics, phishing, and data breaches are becoming increasingly common across industries. Here are some real-world examples.

- **Target Breach:** In 2013, [hackers penetrated Target's systems](#) by stealing network credentials from a third-party HVAC contractor initiated via a phishing scam. This resulted in the theft of 40 million credit and debit card information. The hacker exploited the compromised system of the air-conditioning contractor to gain access to the Target network before leapfrogging onto the company's payment system.
- **Bird Construction Ransomware Attack:** A multi-million dollar Canadian construction firm that has worked on major government projects [suffered a ransomware attack](#) in 2020. The attack resulted in the encryption of company files, and the cybercriminals demanded approximately 6 million USD in exchange for a decryption key.
- **Business Email Compromise at Solid Bridge Construction:** A Texas-based commercial project contractor [fell victim to BEC](#). The company received an email from the perpetrator, claiming to come from one of the company's subcontractors. The attacker claimed to have experienced issues with receiving check payments and requested payments to be sent to a different address. Solid Bridge Construction sent a check amounting to more than \$200,000, believing the scam.

How Cyber Insurance Can Help Mitigate Risks

Like most businesses, contractors rely on technology for their operations. While it can be an advantage, it can also create cyber susceptibilities that can disrupt critical workflows and lead to massive business losses. Investing in cyber insurance can help contractors reduce risks and mitigate these vulnerabilities. Cyber insurance can provide:

First-Party Coverage

- Expenses Related to Hiring IT Professionals
- Cost of Repairing Digital Assets
- Cost of Notifying Affected Individuals and Stakeholders

Third-Party Coverage

- Legal Expenses
- Cost Related to Breach of Contract and Negligent Protection of Data
- Regulatory Fines
- Payouts to Affected Customers