Why Do Contractors Need Cyber Insurance?

Today, general contracting involves multiple stakeholders collaborating in a digital environment.

Contractors generally have access to sensitive client data and systems for the duration of each project. They also frequently oversee the project's software and technical equipment.

The construction industry uses technological advancements to streamline operations and serve clients more effectively. But while these technologies can increase efficiency, they can also create new weaknesses for cyber criminals to exploit.

Vulnerable systems make attractive targets for hackers looking to steal data and disrupt operations. Contractors must strengthen their security measures and adopt cyber security policies to protect their clients' data in the face of emerging, always evolving digital threats.

Cyber Risks and Exposures for Contractors

Here are some key reasons contractors should invest in Cyber Insurance:

1). Cyber Attackers Target Construction

Construction continues to be one of the economic sectors running the highest risk of a cyber attack. In Q1 2023, the KELA Cyber Threat Intelligence Report named construction as one of the most commonly targeted industries.

The construction sector faces an average of 226 incidents a year, according to cyber security company ReliaQuest. A majority (59%) of construction and design professionals responding to a Dodge Construction Network survey reported experiencing a cyber security threat since the fall of 2021. Seventy percent of those respondents are general contractors.

Ransomware is one urgent threat. Of 35 industries the software firm Nordlocker analyzed between January 2022 and January 2023, the construction industry suffered the most ransomware attacks.

Cyber attackers also frequently use social engineering schemes—for example, posing in emails as legitimate vendors or contractors—to target construction businesses.

2). Contractors Bear 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, cyber criminals could steal such proprietary corporate assets as contracts, confidential bids, designs, intellectual property, or valuable client data.

Cyber Risks and Exposures for Contractors - (continued)

3). Reputational Damage Can Be Irreversible

Without adequate security measures and Cyber Liability Insurance coverage in place, contractors' clients may feel their assets and information aren't protected, and refuse to do business with the company.

A single successful cyber attack could cause contractors to suffer irreversible reputational harm, destroying current and possible future partnerships.

Real-World Cyber Threat Examples for Contractors

1. In early 2023, 71% of construction and property businesses reported they had experienced recent ransomware attacks—a 129% increase in two years—leading to lost business and revenue.

2. In October 2023, Johnson Controls International, a major manufacturer of physical security equipment and automation systems, was hit with a ransomware attack. The attack may have compromised data belonging to the Department of Homeland Security, for whom Johnson Controls is a contractor, including building floor plans. Johnson had to shut down much of its IT infrastructure, including customer-facing systems. The costs of responding to and remediating the attack reached $27 million.

3. Also in October 2023, Simpson Manufacturing Company—a major, California-based producer of building materials, including anchors, connectors, and new construction and retrofitting materials—was forced to take some of its IT systems offline in response to an unspecified cyber attack. Simpson operates seven laboratories for testing new designs and materials, and holds more than 2,000 patents and trademarks.

4. In 2023, Andrade Gutierrez, a major construction conglomerate in Brazil, suffered a data breach in which hackers stole approximately 3 terabytes of emails and sensitive company information, including names, email addresses, passports, payment information, tax ID numbers, and health insurance details of more than 10,600 past and present employees. Hackers also stole blueprints and 3D projections of critical infrastructure projects.

5. In August 2023, the Newtron Group, a leading commercial and residential construction company in Louisiana, suffered a data breach compromising the sensitive personal information of nearly 40,000 individuals.

6. In August 2022, Sunland Asphalt and Construction suffered a data breach in which a hacker gained access to the confidential information of 7,884 individuals.

7. In 2022, one of a U.S. property management and construction company's own third-party vendors caused a data breach, acting under the company's guise to successfully extort both it and its clients. The vendor could use the company's systems due to poor access management and weak cyber security controls.

How Cyber Insurance Can Help Mitigate Risks

Contractors' reliance on technology is necessary, but does create cyber susceptibilities that can disrupt critical workflows and lead to massive business losses. Investing in Cyber Liability 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