WHAT EVERY BUSINESS NEEDS TO KNOW

Cyber Threats in the Construction Industry

As the construction industry continues to increase its use of technology, the risks of cyberattacks also rise. According to an analysis by encryption software company Nordlocker, the construction industry had the most cases of ransomware attacks between January 2022 and January 2023.

The construction industry's heavy reliance on computer-aided design (CAD), building information modeling (BIM), and cloud-based collaboration tools has resulted in increased security vulnerability. Without comprehensive cybersecurity strategies, an attack has the ability to shut down business operations, cause reputational damage and result in costly litigation and fines.

Contributing Factors

Lack of Cyber Regulatory Focus

The construction industry has historically not been subject to mandatory cyber regulatory requirements or scrutiny, which has had the adverse effect of deemphasizing cyber priorities.

Increased Technology Adoption

Increased use of mobile devices, digitization, and connectivity to the cloud are driving changes on the cyber risk front by expanding vulnerabilities and the potential for attacks.

Desirable Data

Large amounts of sensitive business information in the construction industry make firms lucrative targets for cybercriminals.

Third-Party Exposures

Construction companies often rely on external partners, such as subcontractors, suppliers, and service providers, which creates potential vulnerabilities.

Lower Your Risk

- Educated employees are better prepared to recognize and respond to potential cyberattacks.
- Identify and control cyber risks related to working with external organizations.
- Create and regularly test a cyber incident response plan.
- A trusted broker can help you secure sufficient coverage for cyber losses.