THE CONSTRUCTION INDUSTRY
Planning for Cyber Risk

There's a common misconception that construction firms do not pose much of a cyber risk. This only makes them more attractive to cyber criminals because their lack of defences leave them easily exploitable. ATC Insurance Solutions is here to help you better understand the threat landscape of the construction industry.

POTENTIAL EXPOSURES / RISKS

- **Funds Transfer Fraud:** Imagine paying a large invoice from a supplier, only to realise that it was fraudulent and the money is now irretrievable. Fake invoices are becoming increasingly more difficult to spot as cyber criminals use innovative methods to trick their suspects.
- **Human Error**: Humans make mistakes. According to a study by IBM, human error is the main cause of 95% of cyber incidents. This could be as simple as clicking on a malicious link or opening a bad email attachment which could lead to a malware infection or criminals stealing data. Cyber security training is key to protect against this.
- **Business Interruption**: Delays to projects as a result of a cyber event including systems being inaccessible or vital documents being lost can be incredibly costly for a firm as well as cause reputational damage. It's important to have a Business Continuity Plan/Disaster Recovery Plan in place in case of a cyber incident.
- **Third Party Liability**: Construction projects require collaboration of businesses within the industry. The use of third-party suppliers and subcontractors as standard increases cyber risk. This is because they often have access to systems or share or maintain data critical to operations. According to a recent report by CBInsights, 44% of all data breaches are caused by a third party and only 15% of these vendors informed impacted parties of the breach. The potential impact of this is very real to the construction industry.
- **Data Breach**: Even though construction firms aren't always data rich in terms of Personally Identifiable Information (PII), they do hold and use their client's confidential information, including but not limited to blueprints and architectural designs which are costly to recreate.
- **Underinvestment:** Typically, because they aren't aware of the risk, construction firms underinvest in IT and more specifically IT security. This can lead to lack of even the most basic defences that can eradicate the majority of cyberattacks. Criminals target these businesses as 'low hanging fruit', including firms who are running legacy/unsupported systems.
- **Mobile Device Dependency**: As advancements in technology have facilitated the ability to work from anywhere, construction workers are taking advantage of working on-the-go from site to site. The increased use of portable devices to ensure constant connectivity exposes critical systems to cyber risk. Multiple access points to the company's network increases the number of vulnerability points. Coupled with underinvestment in IT security as mentioned, this environment is ideal for cyber criminals to gain access.

HOW ATC CAN HELP

- 24 Hour incident response hotline – access to cyber security experts in a time of crisis
- Claims managed in Australia by Australians
- Free commercial grade antivirus for up to 10 devices
- Operator error covered
- Funds Transfer Fraud cover available
- No excess in respect of remediation costs
- No sub-limits in standard wording
- Public Relations Costs covered
- Cyber Extortion Covered

Contact

Jenny Arkell
Senior Underwriter - Cyber
E: jennya@atcis.com.au
P: 03 9258 1777

FOR MORE INFORMATION

ATC Insurance Solutions Pty Ltd
Level 4, 451 Little Bourke Street
Melbourne VIC 3000

Tel: 03 9258 1777
Email: cyber@atcis.com.au
Web: **www.atcis.com.au**

MELBOURNE • SYDNEY • BRISBANE