Navigating Cyber-security Challenges in the Construction Industry

The construction industry is continuously moving towards digitisation, adopting advanced technology such as artificial intelligence, the Internet of Things (IoT) and Building Information Modelling software. These innovations help to automate tasks, reduce waste and improve efficiency, productivity and safety.

However, this shift also brings significant cyber-security risks. As construction companies increasingly rely on digital tools and store large amounts of sensitive data, cyber-criminals view them as attractive targets. As a result, construction businesses must take action to protect sensitive information from data breaches and other cyber-security incidents that can create financial hardship and reputational damage.

This article outlines why cyber-criminals target the construction industry, discusses examples of common types of cyber-attacks and why they are utilised, and provides cyber-security best practices. It also examines the role of cyber-insurance in mitigating cyber-risks.

Why Cyber-criminals Target the Construction Industry

There are several reasons why the construction industry is an appealing target for cyber-criminals, including:

- **High-value transactions**—Construction projects often involve significant financial transactions, making them attractive targets for ransomware, phishing attacks and financial fraud. The high value of these transactions can incentivise cyber-criminals to attempt fraudulent payments or extortion.
- **An abundance of sensitive data**—Construction companies manage sensitive data like blueprints, architectural designs, bids, contracts, and employee and client information. This data is valuable to cyber-criminals, who can exploit it for financial gain through data breaches or sell it on the dark web.
- **Complex supply chains**—With multiple stakeholders and subcontractors involved in construction industry supply chains, each with potentially varying levels of cyber-security maturity, the odds of network vulnerabilities increase. Malicious actors may target these weak links in the supply chain, as they may serve as potential access points for cyber-attacks.
- **Outdated cyber-security measures**—Many construction firms rely on legacy systems or outdated software that does not provide adequate protection against modern cyber-threats. These weaknesses present attractive opportunities for intrusion by hackers, who often seek out older systems that have known vulnerabilities and are easier to exploit.
- **Increasing adoption of digital technologies**—The digital attack surface has expanded with the construction industry's increasing use of digital technologies (eg IoT, remote project

management, cloud storage). Even though they improve efficiency, these technologies have created more chances for malicious actors to infiltrate networks, especially if cyber-security practices aren't keeping pace.

Common Cyber-attacks and Why They Are Utilised

There are many types of cyber-attacks; the following are commonly used against the construction industry for various reasons:

- **Ransomware attacks** occur when cyber-criminals gain access to a business's computer system, encrypt the files and demand a payment in exchange for providing a decryption key. This attack can be effective against construction companies because projects often have strict deadlines, making business interruptions extremely costly and prompting targets to pay the ransom quickly in an attempt to avoid further losses.
- **Phishing attacks** involve malicious actors tricking users into providing sensitive information (eg passwords) through fraudulent emails, text, calls, websites or links. Construction firms often employ temporary staff and subcontractors who may not be familiar with a company's internal communications. This makes phishing attacks especially effective, as cyber-criminals can exploit this unfamiliarity and trick targets into revealing sensitive information or clicking on malicious links.
- **Business email compromise (BEC)** occurs when a malicious actor impersonates a legitimate individual (eg a CEO) or hacks into that person's email account and fraudulently requests money or sensitive information. BEC scams are used against construction companies because large amounts of money and sensitive data often move between project stakeholders, so these requests may not raise a red flag and can go unnoticed.
- **Supply chain attacks** happen when a cyber-criminal infiltrates a business's supply chain. Construction companies often rely on multiple subcontractors and third-party vendors, which increases the potential for cyber-criminals to target less secure partners. Once a third-party vendor's system is breached, attackers can gain entry into the main company's network, compromising sensitive data.
- **Distributed denial-of-service (DDoS) attacks** are when cyber-criminals overload a business's network with traffic, disrupting standard operations or causing a network outage, leading to costly project delays. The cyber-criminals can then leverage the interruption to extort a ransom from construction companies in exchange for ending the DDoS attack.

Cyber-security Best Practices for the Construction Industry

Although cyber-threats are numerous and evolving, there are several measures construction businesses can take to safeguard computer systems and networks:

- **Employee training and awareness programmes** allow employees to educate their workers on cyber-threats. They also allow discussion on combatting cyber-risks by following the organisation's cyber-security policies and procedures.
- **Multifactor authentication** can add additional layers of protection through authenticators, such as one-time passcodes or time-sensitive links, before a user can access a company's network or system.
- **Regular software updates and patch management** can ensure software programs are best positioned to defend against the latest cyber-threats.
- **Network segmentation** divides a network into smaller parts so that if it is infiltrated, there will be security barriers to prevent lateral movement across the network.

- **Access controls** limit who can view or access sensitive information and the situations when they may do so.
- **Data encryption** transforms data into an unreadable, encoded format so malicious actors cannot decipher it without the correct key.
- **Data backup and recovery systems** allow businesses to quickly recuperate after cyber-attacks (eg ransomware or DDoS attacks) because their data is stored in another place (eg external hard drives or a cloud) and can be quickly reloaded onto systems to minimise downtime.
- **Vendor and supply chain management** ensures companies select and work with vendors with strong cyber-security practices. By carefully vetting partners, construction companies can reduce the risk of supply chain attacks.
- **Incident response planning and testing** allow construction firms to proactively build their cyber-defences by having policies and procedures to respond to cyber-attacks and test their systems to find and repair weaknesses.

The Role of Cyber-insurance in Mitigating Risk

Even with a robust cyber-security defence, no system is immune to attacks. Cyber-insurance helps mitigate exposure to cyber-related losses, filling gaps that may be left by other policies (eg commercial property insurance, general liability insurance), which typically do not cover cyber-related events. It is specifically designed to cover business interruption and other financial losses that result from cyber-security incidents, such as data breaches and ransomware attacks.

Many cyber-insurance policies provide access to a vendor panel that includes legal advisors, public relations firms, IT specialists and other experts who are experienced in managing cyber-incidents. This can help businesses respond quickly and effectively to mitigate the impact of a cyber-attack on operations, reputation and finances. Since cyber-insurance policies vary in cover, limits and exclusions, it is advisable to consult a licensed insurance professional for assistance in selecting a policy that best suits a construction business’s needs.

Conclusion

Cyber-attacks are a serious threat to the construction industry. Cyber-criminals can utilise many methods to steal data or disrupt computer networks for financial gain. Strong cyber-security practices with the proper cyber-insurance policy are essential to address these risks. By being proactive, organisations can mitigate exposures and safeguard their finances and reputations.

Contact us today for more information.