Cyber risks in the construction industry: Are you prepared?

From business disruption to data theft, the ramifications of cybercrimes can be far-reaching for construction companies.

When you think of industries with exposures to cyber risks, does construction make the list? Although security breaches of healthcare, retail and government organizations have grabbed headlines, the construction industry can also be a target for cyberattacks.

In fact, cybercrime damages across all industries are on the rise and are projected to reach $6 trillion worldwide on an annual basis by 2021. [1] Large contractors, as well as mid-sized and smaller subcontractors, may be at significant risk. Contractors may believe it can't – or won't – happen to them.[2] This complacent approach to cybersecurity could expose a company to risks, as preventive measures to thwart cybercriminals may not be implemented.

Cybersecurity risks in construction can come from multiple sources

Most contractors operate multiple job sites at any given time. Company staff, subcontractors and other vendors typically enter and exit work trailers on the project site throughout the day. Securing these job sites can be challenging and may offer entry to bad actors, especially since workers likely have varying degrees of cybersecurity training.

Some of the more common cyber risks include:

- **Social engineering:** With so many different workers on a job site at any given time, each with a laptop or cellphone in hand, phishing attempts are a common way to steal user data and possibly access company systems. With phishing, hackers send fraudulent emails that appear to be from a reputable company in order to get recipients to send personal information, such as passwords and credit card numbers.

- **Ransomware attacks:** Malicious software that infiltrates a company's computer system and disabling it until monetary demands are met, ransomware attacks may impact the timeliness of deliveries, delay work and impact the targeted company's successful progress on a project.

- **Wire fraud:** Construction companies may pay vendors and subcontractors on-site. This creates a widespread accounting process and multiple access points to IT systems. High staff turnover is often one of the biggest drivers of fraud against the company.[3]

- **Hacking:** Cybercriminals may access a contractor‘s proprietary information through subcontractors’ systems. Even if a construction company might not store a large number of customer records in its system, attacks involving intellectual property, building plans and bidding records can have a long-term impact. In particular, building plans can be used post-construction to provide access to these properties, creating further security risks after the project is completed.

In the short term, a cyberattack can disrupt a construction company’s daily business operations. However, there are often long-term consequences to consider. Reports of malicious activity and project delays can potentially tarnish a company’s reputation. The ramifications of these incidents can also extend beyond the targeted company, as it’s possible that the attack could eventually spill over to firms that are linked financially.[4]

Taking preventive measures can help

Many construction companies have historically had training programs that focus on establishing a safety culture. As cybercrimes become more prevalent, there are several steps a company can take to address the risk and help implement more robust cybersecurity measures:

- Work with the insurer’s risk engineering team or a cybersecurity consultant to implement employee training that educates staff on how to prevent common cyberattacks, including social engineering events. Building awareness is one of the best ways to help prevent loss.

- Ensure that your subcontractors and vendors provide cybersecurity training for all staff. Require these business entities to carry a cybersecurity insurance policy providing for additional protection in the event of a cyberattack. In the Information Security and Cyber Risk Management survey from Zurich North America and Advisen Ltd., it was noted that 72 percent of large companies and 41 percent of middle market companies have included cyber insurance requirements in their requests for proposals and contracts.[5]

- Create a disaster recovery plan. Cyber resilience is key to long-term success. Construction companies must understand how to identify cyber risk and continue business operations despite the adverse outcomes of a cyber event.

1. Morgan, Steve. “2017 Cybercrime Report: Cybercrime damages will cost the world $6 trillion annually by 2021.” Cybersecurity Ventures for the Herjavec Group.16 October 2017.
2. Slowey, Kim. “A future 'hot target' for attackers: How construction companies can improve cybersecurity.” .ConstructionDive. 11 August 2016.
3. “Three Quarters of Construction Companies Affected by Fraud in the Past Year.” Business Wire. 23 November 2015.
4. “The Cost of Malicious Cyber Activity to the U.S. Economy.” The Council of Economic Advisers. 16 February 2018.
5. “Information Security and Cyber Risk Management.” Zurich North America and Advisen Ltd. October 2018.

Karen Reutter is the Head of Construction for Zurich North America Commercial Insurance