ALLIED WORLD

APRIL 2018

The Case for Cyber Coverage in the Construction Industry

By Jason Glasgow, Vice President, Cyber Lead, Allied World

Construction may be one of the few industries today that is not data production driven. Most construction firms don't have large IT departments and the majority have little expertise in managing information security. However, access to clients' confidential information and an increased dependence on technology have exposed construction companies to a host of new threats, making the need for cybersecurity a critical risk management consideration.

It is projected that cyber crime will cost businesses approximately $6 trillion per year on average through 2021. There's a belief among construction companies that they aren't a target, which only makes the industry easier prey for attackers. And it's not just large companies that are susceptible. In 2016, nearly half of cyber hacks targeted small businesses. A recent Forrester survey revealed that more than 75 percent of respondents in the construction, engineering and infrastructure industries had experienced a cyber-incident within the last 12 months.

Like all businesses, construction companies must adopt a robust cyber security risk management strategy and take the time to understand the exposures including:

- **Access to client's confidential information –** Although your company may not store the type of personal information hackers find desirable (e.g., credit cards or financial records), you may still have access to your clients' confidential information. Compromised intellectual property such as building specifications and architectural drawings can provide a roadmap for criminals to gain access to valuable personally identifiable information (PII), including financial accounts and employee data. Just like any other company, if you have access to this type of confidential information, you're vulnerable to phishing, ransomware, and other common forms of cyber attack.
- **Business interruption exposure –** As in any industry, cyber attacks can result in costly business interruptions for construction companies. A delay in construction projects can be quite costly. This potential disruption must be built into a risk management plan. If a breach occurs, construction companies should have a contingency plan in place to make sure projects are not delayed and if so, they are back up and running as soon as possible.

A recent Forrester survey revealed that more than 75% of respondents in the construction, engineering & infrastructure industries had experienced a cyber-incident within the last 12 months.

- **Mobile dependency –** The construction industry poses a unique cyber security challenge in that it is highly decentralized. There are many stakeholders involved in construction projects that are highly dependent on mobile devices and laptops, offering multiple access points to networks and creating vulnerability if they are not all adequately trained on cyber security. Adding another layer of exposure, valuable technology such as laptops are often stored on jobsites in unsecured trailers, making this information an easy target for thieves.
- **Increased reliance on technology –** In addition to a reliance on mobile devices such as smart phones and laptops, the construction industry is increasingly adopting new technologies to improve safety and efficiency. Wearables and drones provide real-time monitoring and data collection, while virtual reality can create simulations of building designs. These technologies open a world of safety, training and efficiency opportunities, but also give malicious actors potential access to valuable information.

CONTINUED >

- **Third party liability –** As third party vendors to clients, who also use third party suppliers and subcontractors themselves, construction companies are exposed to stakeholder breach liability risk on all sides. Perhaps the most well-known example of this exposure came in the 2013 cyber attack on a large, national retailer, in which a small HVAC contractor providing services suffered a data breach. The hackers gained access to the network credentials that the contractor used to remotely access the retailer's network, resulting in a breach of credit and debit card information for tens of millions of customers in the U.S. This HVAC contractor could have been held liable for the damages customers sustained.
- **Claims Findings –** Claims arising out of breaches are as a result of various types of attacks including ransomware, phishing and social engineering where criminals send emails purporting to be employees or trusted business partners in order to get confidential information or steal money. These attacks can be from criminals with a pure profit motive, competitors attempting to steal information, or criminals seeking to create chaos for other reasons.

The bottom line? Construction companies are not exempt from the dangers of cyber crime. Our increased dependency on technology exposes all stakeholders to increased risk. Companies can mitigate this risk by developing mobile device security and cyber breach plans, and by providing adequate training for all employees on cyber security measures and responsibilities.

Recognizing that construction companies tend to be more focused on completing projects on time and within budget, some cyber policies offer proactive, value-added risk management support. This added level of support can serve as a tremendous resource, especially for companies that lack expertise in information security. Working with an insurance agent who has proven expertise in cyber security and familiarity with the unique risks posed to this industry is the best way for construction companies to ensure that they are adequately covered.

alliedworldinsurance.com