Preparing for Cyberattacks in Construction

Is your business at risk of cyberattacks? This question could be rattling around in your brain after the recent cyberattacks around the world. Threats are everywhere and could be just around the corner if the correct precautions are not taken. “Who would’ve thought 10 to 15 years ago that a supplier would have to file a lien because of cybersecurity,” said Connie Baker, CBA, director of operations with NACM’s Secured Transaction Services (STS).

“Cyberattacks can impact the upfront costs of a contract, and a breach could slow payments and add additional costs,” Baker said. Nearly two-thirds of all cyberattacks are focused on small- and medium-sized businesses, according to IBM, cited a *San Francisco Chronicle* article. “Of those small businesses that do get hacked, about 60% are forced to close six months after an attack,” noted the article.

So where does the construction industry fit within the cyber criminal network? “Unlike highly regulated industries such as finance or health care, many construction firms do not have a cybersecurity protocol in place, thus making them more susceptible to cybercrimes,” said an article with the *Legal Intelligencer.* People and businesses not familiar with the construction industry may think this makes sense, since the sector deals with tangible items and not information like a bank does, but “it is exactly this line of thinking that provides a window for hackers to strike,” added the *Intelligencer.* Construction firms can still have highly sensitive information on their networks such as employee records and blueprints for government buildings.

Subcontractors and suppliers should be concerned if the contractor they are working with gets attacked, but “the level of concern depends on the type of information provided to the contractor during the bidding and/or contracting process,” said Randy Lindley, Esq., partner with Bell Nunnally & Martin in Dallas. “Subcontractors and suppliers may have shared confidential pricing information, banking information, and even proprietary information about construction processes or techniques with the contractor who gets hacked. All of this information is valuable and worthy of protection,” he added.

Some fallouts of being involved in a cyberattack include a drop in business, damage to the company’s reputation and the aforementioned added costs. “Added costs could mean closing down for smaller contractors and suppliers,” said Baker. Payments from the contractor are also affected. “If the attack cripples the contractor's ability to conduct business, this would jeopardize payments being received from the contractor. If confidential information about the project is made public, then this could jeopardize the business relationships of the contractor with other parties in the construction chain,” explained Lindley.

There are certain steps that can be taken to mitigate the risk of a cyberattack. According to Lindley, they include: dedicating one computer for the company's purchasing, banking and confidential financial business and restricting access to confidential data to key employees. Unfortunately, if it is too late and the hack has already happened, businesses must record when the breach was discovered and alert the proper internal department and authorities, if necessary, said Lindley.

– Michael Miller, editorial associate