Construction contractors must remain vigilant to minimize cybersecurity risks

James J. Giszczak | Monday, November 6, 2017

It took only one day for the "WannaCry" ransomware program to infect hundreds of thousands of computers across at least 74 countries. WannaCry seized computers, encrypted data, locked users out, and threatened to delete all records unless a ransom was paid. Another major cyberattack occurred at the end of June, a ransomware known as "NotPetya," which affected more than 2,000 individuals and corporations worldwide. Most recently, Equifax, one of the three major consumer credit reporting agencies, was the target of a cyberattack that potentially compromised sensitive information of 143 million American consumers. These types of attacks are not limited to Fortune 500 companies. Organizations of all sizes and in all industries can be affected, and construction companies risk significant loss if faced with a cyber attack.

The classic example of a cyber attack is one that exposes the personal information of customers (e.g., credit card and bank information). However, any business with systems connected to the internet is a potential victim, not just businesses that maintain large databases of customer information. The introduction of multi-user platforms accessed by different individuals both within and outside of a construction company poses an additional threat as access points and credentials are more difficult to control.

Construction companies maintain many types of information that would be attractive to cyber-criminals, including:

- **Employee information.** Company systems often house massive amounts of employee personal data (e.g., Social Security numbers, payroll information, financial accounts, benefit elections and information).
- **Construction data.** This includes project plans and specifications, as well as other confidential or proprietary data of owners, designers, or suppliers. Security information may be included within the construction plans, which, if stolen, could be used later for a more traditional type of attack on the project owner's physical assets.
- **Owner or other party data.** If a contractor's computer system is not secure, then all of the parties involved in the project become more vulnerable. A primary example is the Target breach in December

2013. In the Target breach, a cyber attack on a third party HVAC contractor resulted in the theft over 40 million credit cards and private data from approximately 70 million customers. The breach was traced back to an email containing malware that was sent to one of the HVAC contractor's employees.

- **Valuable company data.** Company computer systems likely contain various types of intellectual property, trade secrets, company financial information, and other confidential company data.

Construction companies may have brushed off the threat of cyber attacks in the past because they believed that they did not have any information worth stealing. However, it does not matter how valuable the company data is to a third party. It only matters how valuable the company data is to the company itself. Ransomware attacks operate as a type of internet blackmail, holding company files hostage until a ransom is paid. This type of attack poses a significant problem for construction companies that rely on constant access to digital files and the ability to coordinate with employees, owners, designers, architects, and other contractors on a project.

Information is constantly being exchanged on the jobsite and a single ransomware attack can shut down a project for several days. A ransomware attack on a construction project can have severe financial implications and can have a tremendous impact on the contractor's ability to timely achieve substantial completion. Bottom line, a ransomware attack puts a contractor's anticipated profit at serious risk.

How contractors can defend against cyber attacks

There are some useful steps that contractors should take to help defend against cyber attacks, as well as appropriate measures that should be taken if and when an attack occurs. These include:

- **Secure your systems.** Construction companies should remain vigilant about updating their software, systems, and network security. This includes maintaining updated antivirus software on all computers. The updates continually released by most software providers often include updated security features that help defend against attacks. The Target data breach mentioned above could have likely been prevented had the HVAC contractor used an up-to-date anti-malware program. At the time of the Target breach, all major versions of anti-malware software detected the particular malware used to initiate the breach, but the HVAC contractor used a free version of anti-malware software that offered inferior protection.
- **Educate your personnel.** Company employees must know and understand the company's security practices and be aware of potential threats, including ransomware. Cyber criminals use many different tools to trick their targets, including phishing emails.
- **Create a plan.** Every construction company should have a security incident response plan in the event of an attack. The plan should include the creation of protocols to be taken once an attack has been identified, including addressing technology that has been affected, guidelines regarding internal communications, client relations, and legal reporting obligations, among other things. How the situation is handled in the immediate aftermath of an attack can be crucial in limiting the company's legal and financial exposure.

These tips are by no means exhaustive and all companies should develop a comprehensive plan for defending and responding to cyber attacks.

Construction companies must take the threat of cyber attacks seriously. An attack could create project delays and also cause contractors to incur massive costs for investigation, remediation, legal defense, or recovery of files held hostage. Being aware of the potential risk is the first step toward preventing or effectively responding to an attack. The risks posed by ransomware and other cyber attacks can be minimized by focusing on prevention and advanced planning.

For questions or information on data privacy and cybersecurity in the construction industry, please contact one of the attorneys below.

James J. Giszczak