ARTICLE

RICHARD R. VOLACK

For More Information Please Contact

Richard R. Volack
rvolack@pecklaw.com
212.382.0909

What Do Hackers Want From Construction Companies? More Than You Can Imagine

For many years now, we have seen hackers break into, hold for ransom, and destroy the IT systems of well-known finance, health care, and retail giants. During that same time, the construction industry, along with many other industries, may have felt a certain false sense of security that hackers were not (or at least seemingly not) targeting them. In the last few years, however, the landscape has changed. To hackers—now with greater skill, knowledge, and computing power—the construction industry is another data-rich target, but one with far less protection than other industries. Contractors, in particular, have a right to be concerned.

What's Risk?

There are countless articles and interviews given by construction company personnel that essentially say the same things: What does my construction company even have that the hackers could want? Why would the hackers target our company? It turns out that, among other things, the high rate of turnover of personnel, the constant exchange of money, the collection of countless gigabytes of data, especially personally identifiable information ("PII"), and the access and exposure to highly technical building and infrastructure systems are just some of the many unique traits that define the modern construction industry.

The average hacker is most concerned with using the information already prevalent on construction industry IT systems to grab the most money he or she can in the smallest amount of time. This often occurs by what is now being called "invoice manipulation." The most common scheme unfolds like this: A hacker breaks into a construction company's IT system and waits and observes the e-mail traffic in and out of the system. The hacker focuses, especially, on the accounting personnel, and looks for a way to insert himself or herself into the middle of a routine transaction. One scheme the hackers use is to take over the e-mail (often by spoofing or cloaking your e-mail to make it look like an e-mail that a user would recognize) of a higher-level person in the construction company and then e-mail the owner or another entity that may owe the construction company money. The e-mail or its fake invoice attachment is simple and straightforward—we have changed our banking information, please use this new routing number when wiring our monthly payment for the enclosed invoice. There are variants of this where the hackers wait for an established pattern of payment from a contractor to a subcontractor or supplier and again insert themselves in the middle, hoping to head off a monthly construction, service, or rental payment.

In the schemes above, the hackers are hoping to intercept money in some way so that it ends up in the hacker's off-shore bank accounts. Other hackers go about obtaining the money a little more indirectly by using some form of malware to infect a construction company's computer system shutting it down completely until the company pays a certain ransom in bit coin to unlock the system. This is commonly known as Ransomware. Due, in part, to the consequences of not having use of the company's computer system for many days, the ransoms requested by hackers recently have risen into the multiple millions.

Other variants of the indirect method include using spoofing to entice lower level and/or untrained accounting or human resource personnel into e-mailing PII, social security, or bank account information to hackers posing as their respective bosses or other high-level executives of the company. In other scenarios, hackers break into the construction company's IT system and obtain copies of highly confidential plans and specifications for certain classified military installations. Armed with the stolen information, hackers will often sell the information to the highest bidder on an underground and secretive part of the World Wide Web known as the "Dark Web."

Still other hackers break into construction companies' systems to either use the companies' computing power to mine for bit coin or to simply observe the exchange of information, hoping that he/she will come across other pieces of valuable information that could be exchanged for money.

Still other hackers are not interested in financial gain at all. Some hackers break into the construction company's systems solely to cause panic and mayhem or to make a point. A good example of this is a radical animal rights group breaking into the IT systems of a construction company that is in the process of building a vivarium 1 or to protest the clearing of a rain forest. Other hackers, working on behalf of terrorist organizations or nation-states, may hack into a construction company's systems to retaliate for certain political positions the construction company espouses or the relationship a construction company has with certain world leaders.

What Should You Do?

The above scenarios are not meant to scare, but simply to inform. They should serve as the impetus to put in place a robust risk management program to attempt to harden the company's IT systems and to attempt to stave off a cyber-attack. Such risk management programs include, among other items, the following:

- Obtaining and purchasing cyber insurance that will help cover and manage the risks and consequences of a cyber attack.
- A robust training program for all the construction company's employees to practice safe computing and to learn how to identify spoofing or other "phishing" schemes—those designed to obtain personal information or password or other log on information or learn to identify malicious links to malware.
- The performance of an overall security analysis on the company's systems to identify weak and vulnerable spots.
- The implementation of the most up- to-date versions of anti-virus and anti-malware software on the market, especially software that monitors for anomalies on the system and that alerts you to such anomalies immediately.
- The implementation of multi-factor authentication, in which, in addition to the required username and password at log on, the user must input another piece of information that only the user knows, such as a constantly changing pin number or group of letters.
- Assembling a team consisting of a good security consultant and an attorney that specializes in cyber security and data privacy to work with the company's in-house legal and technical personnel.

States Law Imposing Duty of Care

If the risks of losing important or confidential information or having certain important payments interrupted or the loss of use of your entire IT system were not enough incentive, several states have recently introduced very strict data privacy/ cyber security laws that require businesses, construction companies included, to use "reasonable" means to protect the PII of the business' clients, and customers. One such act, the California Consumer Privacy Act of 2018, AB375, Title 1.81.5 (the "CCPA"), which is set to go into effect this year, now greatly expands the definition of personal information that must be protected by the business. The CCPA mandates that the construction company employ at least reasonable means to protect such data. Some of the reasonable means to comply with the CCPA are listed above. The CCPA also appears to provide citizens a cause of action against those companies who fail to take reasonable efforts to protect the personal information of the consumers that do business with the construction company.

Another good example of state government attempting to force companies to use "reasonable" means to keep the personal information of their employees and customers safe from hackers is the New York State SHIELD ACT, "Stop Hacks and Improve Electronic Data Security Act" (SHIELD ACT), N.Y. Gen Bus. Law§ 899-bb. Similar to the CCPA, the SHIELD ACT greatly expands the definition of what is now considered personal information. Although the SHIELD Act does not provide a private right of action, it does, like the CCPA, provide for civil enforcement by the State Attorney General and for the imposition of civil penalties for a violation of the Act.

New York and California are just two of a host of states that either have passed similar cyber security and data privacy regulations or are in the process of passing them. Thus, if diversion of money or assets or the loss of use of your computer systems were not a big incentive to act, now construction companies in a growing number of states may face hefty fines for their failure to enact certain basic security measures, similar to those outlined above in this article. If construction companies have learned anything from the last few years—it is that gone are the days when the company can, like the proverbial ostrich, stick its head in the sand and say I had no idea hackers found my IT systems (and the information contained therein) so enticing.

The theoretical has now become the reality for the construction industry and it only gets worse from here.

Published in *Under Construction* Volume 21, Number 3, Spring 2020.