Cybersecurity in the Construction Industry:

Know Your Risks and Take Steps to Protect Your Company

Jonathan W. Massell

Shareholder

Maynard Nexsen

Raleigh, NC

(919) 573-7447

jmassell@maynardnexsen.com

The digital age has enabled the construction industry to utilize new technologies to increase efficiencies and become more streamlined. Electronic communications, online banking, automated systems and digital storage of key information are now standard aspects of even the most low-tech companies in the construction industry. It is easy to take these systems for granted. But have you ever wondered what you would do if you were completely shut out of your company emails, operating system and electronic databases? Could you operate without these systems and data? What could happen if this data falls into the wrong hands? How much would you pay to regain access to your systems and data?

Unfortunately, many companies in the construction industry find themselves completely unprepared when they fall victim to a cyber-attack and are forced to address these hard questions. In recent years, the construction industry has been one of the most heavily targeted industries for cyber-attacks. In fact, as of 2021 studies indicated that it was the third most targeted industry. This high volume of cyber-attacks is symptomatic of the fact that the construction industry lags behind many other industries in terms of cybersecurity and privacy protections.

There are several reasons why the industry is so vulnerable. First, to date, the construction industry has avoided the strict data privacy and security regulations that industries such as healthcare and banking have faced. Absent increased regulation, the industry has not been forced to address its vulnerabilities. Although technology has become an integral part of daily business for almost all construction companies, many companies have obsolete computers and operating systems with inadequate firewalls and protections to ward off sophisticated hackers. Additionally, the nature of the construction industry often involves intermeshed digital and communication systems across multiple offices, jobsites and individuals that creates a labyrinth of doorways that can give bad actors access to the entire system.

These vulnerabilities make many construction companies easy targets, and cyber criminals have been quick to capitalize. Among others, the biggest cybersecurity risks facing construction companies are ransomware, data theft and fraudulent wire transfers. Each risk is discussed in turn.

Ransomware

The most common delivery source for ransomware to infect an operating system is via phishing emails that seek to induce the reader to download malware. While some phishing emails are easily detected through their broken English and unusual instructions, others are more subtle, and easy to fall prey to. Cyber criminals will often send phishing emails from email addresses that at first glance appear legitimate and recognizable. An ostensibly legitimate email containing concise instructions to click a link to download updated project documents or information is often

all that it takes to catch somebody off guard. Once downloaded, the ransomware enables the cybercriminal to steal data or lock a business out of its operating systems (including payroll) until a hefty ransom is paid. Not only does the lack of access to email and operating systems cause substantial business disruptions, but it often entails the theft of sensitive confidential information of the company, its employees and its vendors. In addition to reputational harm, this can create substantial liability risks for the victimized company if damages flow down to its vendors and customers. The reason that ransomware is becoming increasingly prevalent is that it pays. Often, the only way for a company to regain access to its systems and data and resume operations is to pony up and pay the ransom. Unfortunately, even if the company pays the ransom, this is no guaranty that it will get everything back that was taken. In fact, the percentage of cases where the payment of the ransom does not result in regaining access to data has seen a significant increase.

Data Theft

Whether acquired through ransomware or other hacking mechanisms, data theft is a serious issue. There is a big market on the dark web for banking information and sensitive personal information of customers, vendors, and employees, including social security numbers and credit card information. If a company has inadequate safeguards to protect the sensitive information it has been entrusted with, there can be serious potential liability implications and risks of reputational harm. Additionally, some construction entities deal with sensitive and confidential intellectual property such as blue prints, designs, patents and bid information. Sophisticated hackers recognize the value of such information, and there is no limit to what they will do to extort their victims.

Fraudulent Wire Transfers

As construction companies become increasingly reliant on online banking and wire transfers, they become susceptible to wire fraud. Once a hacker has found a back door into a company's email and operating systems, the hacker may set up fake email accounts that mimic those of the construction company's employees as well as banks, customers, and vendors that the company regularly deals with. The hackers can learn who the key players are in financial transactions, and will often insert personal details and information into their communications in order to catch somebody with their guard down. When the hacker knows that a large wire transfer is imminent, they may send revised wiring instructions to the company individual responsible for initiating the wire transfer. If the individual is fooled and transfers the funds into the new account, there is often very little that can be done to recover these funds once the transfer is complete.

What Can Construction Companies do to Protect Themselves?

1. **Meet with an attorney** who focuses on cybersecurity and privacy issues or a professional cybersecurity consultant to help understand your risks and come up with a game plan to protect your company. The vast majority of the time, companies have no idea just how vulnerable they are. It's best to get ahead of bad actors rather than learning of your vulnerabilities the hard way after your data has been compromised. If a data breach is bad enough, there may not be a second chance.
2. **Create an incident response plan,** a plan of action for what your company will do if it falls victim to a cyber-attack. You need to be ready to take immediate action to mitigate damages. Determine which individuals in your company will be responsible for taking key actions, and have a point person designated to lead the charge. Immediate action items may include notifying your insurer (if you have cyber liability coverage), notifying law enforcement, notifying vendors whose data may be compromised or who may suffer business interruptions, and ensuring that employees do not take any additional actions that may be detrimental to mitigation efforts. A cybersecurity consultant can help you create an appropriate plan that is tailored to the specific needs of your company.
3. **Educate all of your team members** about cybersecurity risks. A key source of infiltration is email links. Make sure that your personnel understand this risk and other vulnerabilities by conducting periodic training and workshops. It is likely not enough to just train your employees. You should periodically evaluate whether the lessons are sticking by sending mock phishing emails to see how well your employees perform. Any failures

will serve as valuable teaching tools. Finally, make sure that your employees know who the point person is at your company to contact in the event of a cybersecurity breach, and that they also understand what NOT TO DO, such as engaging in self-help efforts to fix the issue on their end by deleting data or sending additional information that can further compromise security.

4. **Implement procedures** to help prevent fraudulent wire transfers and make sure that the employees who handle wire transfers diligently stick to these processes. Once procedures are in place, re-evaluate them on a regular basis to ensure they keep up with new tactics that are utilized by cyber criminals. As AI technology continues to advance, it can be expected that cyber criminals will increasingly become more sophisticated and convincing in their efforts. It only takes one slip up to create potentially huge losses.
5. **Consider cyber liability insurance.** If you suffer a data breach, your coverage may help you cover the costs of hiring attorneys, forensic IT consultants, and other crisis management costs that you may incur. Insurance may cover losses from fraudulent wire transfers (if your company followed certain procedures to avoid the incident) and may also assist in negotiating and paying a ransom. Importantly, if you do opt to obtain cyber liability insurance, ensure that your cyber breach response plan includes designating an individual at your company to provide immediate notice to your insurer in order to ensure that coverage is not jeopardized.

Though the above list is not complete, these are some key considerations for what construction companies can do to help protect themselves. Though it is easy to continue business as usual and keep cybersecurity risks out of sight and out of mind, prudent companies will take proactive steps to help mitigate their risks, especially given the frequent changes in technology and legal requirements which further add to the risk profile. By spending a little now to address and manage risk before a problem emerges, this will not only potentially help your company save a ton later, but can also help drive both top line and bottom line growth for your company.

About the Author

Jonathan is an attorney in Maynard Nexsen's Raleigh, NC office and practices in the areas of Construction Law and Business Litigation. He represents owners, contractors, subcontractors, and suppliers in contract drafting and negotiations. He represents clients in a wide array of construction issues, including contractual disputes, defects, delays, and lien and bond claims. He also represents clients in land use and zoning matters, both at the early development and planning stage and in litigation.