Holland & Knight

ALERT

Cybersecurity in the Construction Industry

What Construction Executives Should Be Doing Now to Prepare for the Inevitable

April 16, 2015

Gregory Meeder
Christopher Cwalina
Kaylee Cox

HIGHLIGHTS:

- A hacker with access to construction data could wreak havoc not only operationally but also through the physical destruction of data, servers and infrastructure as well as ultimately by threatening the safety of individuals on-site. In fact, such incidents can cause harm to an owner's design and security systems.
- Companies should begin to prepare for a cyber-event before an incident actually occurs to ensure a streamlined and coordinated response process and minimize the subsequent aftermath. Best practices include creating incident response policies and communication protocols, conducting cyber-exercises and employee training to practice scenarios, and designating third-party vendors to assist in the event of an cyberattack.
- A successful incident response team that needs to be in place before a cyberattack occurs consists of a multitude of cross-functional representatives in addition to IT and information security. Company executives need to identify who can advise on a wide range of topics such as legal implications, compliance, privacy concerns, public relations, government affairs, audit matters and ethics.

Cybersecurity is everywhere in the news today because hackers have been very successful in exploiting human weaknesses across a broad array of industries. Our construction industry appears to be tempted to brush off these early attacks, thinking that our industry is not a prime target. However, any business that is connected to the Internet is a potential victim. The construction industry also contains special vulnerabilities related to the physical makeup of our society that do not exist in other commonly recognized target industries, such as the financial or healthcare sectors. In the construction industry, ignorance can hamper a construction company's well-being and its operational security.

Construction executives should be paying attention to and learning from those who have already experienced a major cyberattack. For instance, an owner's plans, specifications and virtual construction data present an easy target. Take, for example, the virtual construction needs of a large construction project. There is almost unlimited access to a building's physical and security design. In addition, many design and construction software systems – such as BIM, Revit, Procore and Aconex – have remotely accessible controls or Internet-connected capabilities. A hacker with access to this data could wreak havoc not only operationally but also through the physical destruction of data, servers and infrastructure as well as ultimately by threatening the safety of individuals on-site.

Even if an attacker has no intentions of causing physical harm, he or she may be interested in obtaining valuable corporate data, such as intellectual property, trade secrets or any other data that could be used for competitive advantage. Furthermore, even in instances where hackers have no interest in your company's data whatsoever, they may nevertheless capitalize on human weaknesses in your system as a jumping-off point for other data systems. This is especially true for contractors, who may offer unanticipated avenues to other targets and is even more pertinent for those in the government contracting space, as they may have access to sensitive government information or capabilities.

Also, construction companies house significant amounts of sensitive employee information, making it a path of least resistance for those looking for a simpler target. They do not care where they get their information. They only care that they get it, and they are patient. A recent survey showed that cyber-attackers went undetected for an average of 243 days.

Moreover, even those construction businesses who do recognize the threat to the industry may be inclined to think that cybersecurity is solely an IT issue. However, preparing for – and responding to – a cyber-incident falls on the shoulders of many more than just IT or information security professionals. In fact, a successful incident response team consists of a multitude of cross-functional representatives in addition to IT and information security, such as legal, compliance, privacy, public relations, government affairs, audit, ethics, and business lines.

No matter how secure or resilient a company's system may be, perfect security does not exist. As many cybersecurity experts profess, "it is not a matter of if but when." Thus, against the backdrop of the inevitable, the time to prepare for a cyber-incident is not while an attack is ongoing. A critical aspect of cybersecurity is preparedness.

Below are some baseline steps members of the construction industry should be taking to ensure cyber-incident preparedness:

- **Incident Response Policies:** It is absolutely critical to have a plan in place in the event a cyber-incident does take place. While traditional incident response and disaster recovery plans may serve as a rough guide, cyber-incidents pose specific threats that will not be adequately addressed by policies directed at incidents occurring on a more tangible level (such as natural disasters). So it is imperative that a policy be created specifically for a cyber-event that takes into consideration these specific characteristics.
- **Designated Leadership:** An incident response policy is only effective if the people responsible for executing it understand their role and are able to fulfill their duties. Accordingly, there should be clearly designated roles for the varying aspects of the incident response process. In particular, there should be a pre-identified incident response team, with a single "incident command" who is in charge of the overall response process and who has real-time decision-making authority. Similarly, there should be designated points of leadership within functional departments to manage the process in their respective areas. As mentioned, the incident response team should consist of representatives from all key stakeholders within the organization, and these roles and responsibilities should be clearly defined and memorialized in the incident response policy.
- **Communication Protocols:** In order to respond in a timely and appropriate way in the event of a cyber-incident, employees must understand when and what needs to be communicated across departments. Any incident response policy should clearly articulate communication protocols and escalation procedures. Similarly, there should be clear guidelines regarding external

communications, such as requiring that all third-party inquiries be routed through the public relations department and a strict prohibition against communicating about the incident to the outside world.

» **Employee Training:** To ensure that incident response procedures are properly communicated, companies should conduct regular training with *all* employees. Training should not be limited to just those individuals directly involved in the incident response process but should be given to all employees. However, additional targeted training should be conducted with official Incident Response Team members.

» **Cyber-Exercises:** The best form of training is through execution. Simulated cyber-exercises are the most effective method to ensure (1) incident response policies and procedures are sufficient and effective and (2) such procedures are readily understood across the organization. Cyber-exercises can help to identify unknown vulnerabilities or unanticipated gaps in process that may not be readily apparent on paper. Moreover, exercises allow companies to practice their response protocols for the first time in a controlled environment rather than during a live event. In addition, regulators and consumers are increasingly expecting that companies conduct cyber-exercises as an information security best practice.

» **Third-Party Vendor Management:** A major cyber-incident will inevitably trigger a need for external assistance (e.g., outside counsel, forensic firms, credit monitoring services, etc.). Just as the time to test incident response procedures is not during an actual incident, companies likewise will not want to deal with establishing third-party relationships in the midst of a cyberattack. Companies should make these arrangements in advance so that these parties are ready to respond if and when the time comes for their assistance.

As discussed, there is no such thing as perfect security, and the construction industry equally is not immune from a cyberattack. Thus, it is imperative that companies begin to prepare for a cyber-event before an incident actually occurs to ensure a streamlined and coordinated response process and minimize the subsequent aftermath.

While the above principles serve as a baseline for cybersecurity preparedness, a sound information security and incident response program requires skilled, intensive attention and analysis. Holland & Knight's Construction Industry Practice Group as well as our Data Privacy and Security Team have the combined experience to assist companies with cybersecurity incident preparedness, including reviews and analyses of policies and procedures, conducting cyber-exercises, and providing vendor management services. For further information regarding these services, please contact the authors of this article.

Authors

Gregory Meeder
Chicago
312.928.6022
gregory.meeder@hklaw.com

Christopher Cwalina
Washington, D.C.
202.469.5230
chris.cwalina@hklaw.com

Kaylee Cox
Washington, D.C.
202.469.5185
kaylee.cox@hklaw.com

Information contained in this alert is for the general education and knowledge of our readers. It is not designed to be, and should not be used as, the sole source of information when analyzing and resolving a legal problem. Moreover, the laws of each jurisdiction are different and are constantly changing. If you have specific questions regarding a particular fact situation, we urge you to consult competent legal counsel.

The lawyers resident in all offices, unless otherwise indicated in an individual attorney biography, are not certified by the Texas Board of Legal Specialization. Attorney Advertising.