RICHARD R. VOLACK

For More Information Please Contact

Richard R. Volack
rvolack@pecklaw.com
212.382.0909

The Nightmare Scenario: What to Do When Systems Are Hacked

Avoid Disaster by Preparing for the Worst

In an age where everything is connected and cyber threats have become more sophisticated, it is more important than ever to know what to do in the event of a cyber security breach.

Imagine a scenario in which a construction executive returns from a planning meeting for one of the company's largest building projects. He/she is excited about starting the multi-year, multi-billion-dollar project and all the income and publicity that will come with it. Now imagine that an hour later one of the company's junior IT employees comes to the executive's door and says that the firm's IT systems were hacked and the hackers planted a Ransomware virus that completely froze all of the company's computer systems. The hackers demanded that the firm pays $50,000 in bitcoin, or they will not "unlock" the firm's computer systems and will erase all data stored on the firm's IT systems.

Unfortunately, this nightmare scenario is becoming increasingly common in the construction and development industry. Due, in part, to the constant movement of money, frequent turnover of personnel and exposure to critical infrastructure and building system information, hackers are more frequently targeting information stored on and flowing through the IT systems of constructors and developers. Below are some tips on how to handle this growing trend.

When hacked, it is imperative to remain calm and remember to think logically. Construction executives must apply the same analytic skills to this problem as they would to any other construction challenge.

For those companies that have cyber insurance in place and the practice drills and education that comes with it, dealing with the breach will be a somewhat less taxing ordeal. However, for the majority of those in the construction and development industry that have not yet purchased a cyber policy, here are some simple steps to follow:

- Involve the company's general counsel or, if the company does not have a general counsel, involve the law firm that provides the most advice and has the most knowledge of the hacked company's inner workings.

- Call an attorney who knows about both the construction and development industry and the field of cyber security and data privacy. An attorney with knowledge in these areas will get "up to speed" on the company's issues in a shorter amount of time. They will be what are known in the data privacy industry as a "breach coach." The reason to call the attorney early in the process is to cloak the entire event under the attorney client privilege—thus making it much harder for the investigation and its findings to be discovered by anyone outside the walls of the breached company.[1] The data privacy and construction counsel should then recommend a computer forensic firm to work with the hacked company's IT personnel to determine how the hackers entered the company's IT system, the extent of the data viewed or removed and how to possibly deal with the hack. Be aware, such firms can become expensive very quickly. However, at this point, forensic firms possess the knowledge and expertise for situations just like this.

- Depending on the company's size and the extent of the breach, the hacked company may want to involve a crisis management firm and/or a public relations consultant so that the company can have a say in shaping the story and how it is presented to the outside world.
- The above-described personnel should work together as a team to investigate the breach or hack, determine the extent of data reviewed or stolen, and then make decisions as to what next steps should be put in place. Next steps could involve remediating the breach, restoring data from backups, strengthening the breached company's systems, determining whether there is a legal need to notify those persons possibly affected by the breach. This determination will vary by state.

While no company on earth can absolutely avoid the above doomsday scenario, applying basis risk management techniques will help lessen the overall impact the hack would have on the company's systems. Such techniques involve purchasing cyber insurance through a reputable broker. Most of the major insurance brokers for the construction industry also now have cyber insurance options that can be explored. Many policies will cover the fees for the breach counsel, the forensic expert and the PR/crisis management expert.

Once an insurance policy is in place, construction companies should periodically bring together top-level executives, representatives of the IT department, the company's in-house counsel, data privacy counsel and its PR consultant and run though practice scenarios. Those scenarios, known as "table top exercises" will help determine what formal policies and plans to put in place for the long run. The table top exercises will help iron out any logistical and personnel issues that may arise on the day of an actual breach and provide for a smoother response to what is becoming an increasingly more common event in the construction industry.

As the common adage goes—"practice makes perfect." Executives must keep in mind that cyber security is an iterative process that must be updated weekly. It never was, and never will be, a "one and done" process. All involved should treat it accordingly.

[1] The construction executive and breach counsel should also determine whether to contact the FBI. Most regional offices of the FBI have a specialized cybercrime bureau staffed with knowledgeable agents that want to help. The motto for the FBI recently has been that you are the victim and should be treated as such. The FBI may be able to help at least determine the hackers place of origin, their motives and could possibly have information about the keys to unlock the Ransomware virus—but that is more the exception than the rule.

This article first appeared online for Construction Executive on September 25, 2019 and is linked HERE. Copyright 2019. All rights reserved.