ARTICLE

RICHARD R. VOLACK

For More Information Please Contact

Richard R. Volack
rvolack@pecklaw.com
212.382.0909

A Comprehensive Cyber Security Plan Is Key to Robust Risk Management

A breach or hack of a construction company's computer systems is one of the single greatest threats facing the construction industry today. A breach can result in loss of income, loss of clients, loss of trust by the public and even the loss of the entire business.

Because it is impossible to eliminate completely every cyber threat, robust risk management of a cyber security threat is key to the health of the construction company.

A major part of cyber risk management is the drafting and implementation of a cyber security plan. Like most things in life, one size does not fit all. The plan must be tailored to the facts and circumstances of each individual company. Finding the right place to start may even be confusing and, at times, daunting. The first step is to engage the services of an attorney who knows the business, the construction industry and relevant technologies, and who is experienced with cyber security and data privacy law. The attorney can then engage a forensic computer consultant, as necessary. The attorney will work with the company's C-suite executives, IT persons and key managers to institute a cyber security plan that is right for the company.

SIX STEPS TO AN EFFECTIVE CYBER PLAN

Step One – The Evaluation of the Systems

Like any major project, before diving in, an assessment must be made of the "lay of the land." This assessment involves a thorough evaluation of where the company falls on the spectrum of readiness to fend off a cyber-attack. This in-depth evaluation will look at, among others, the following:

- the robustness of the fire walls and virus protection systems of the Company, including whether there is software in place to continually monitor the system for anomalies;
- whether dual-factor authentication (the use of not just the user name and password, but the input of another piece of information known only to the user) is in place and in use;
- whether the computer system is sectioned off into various silos so that even if a hacker gets in, he/she will not get very far;
- whether the company has in place a comprehensive back up system that periodically backs up the data in the system to another location;
- whether the company has in place a program to scan in-coming emails and their attachments to identify potential threats;

- whether the company has protocols for the use of smart phones and the access of personal email and social media sites;
- whether the company has a policy of restricting administrative access to the system to only those who absolutely need it;
- whether the company has a password policy in place (e.g., create strong passwords and change them every six months);
- whether there is a policy for implementing patches (or fixes) for existing computer programs and devices;
- whether there is a policy of encryption in transmission and at rest.

Step Two – Identifying the Major Assets

In addition to identifying whether certain protections are in place, the company must identify the information that is especially sensitive and confidential and record where such information resides on the company's systems. This includes anything from the personal information (social security number, health information, bank account number, etc.) of the company's personnel to certain plans and specifications for certain high-tech or government building projects. Once those assets are identified, the plan can implement certain extra procedures (additional cording off such information, placing the information on a hard drive that is not continually attached to the internet, etc.) to provide a higher level of protection from the breach.

Step Three – Identifying the Major Players Required in the Event of a Data Breach

Such personnel must include at least the following personnel:

- the director of the company's IT department;
- C-suite executives including the Chief Operations Manager, The Chief Information Security Officer (if applicable) and other high-ranking personnel that have a sense of the landscape of the entire company;
- the company's in-house counsel and the company's principal construction counsel (or other counsel that understands the inner-workings of the company);
- an attorney versed in cyber security and data privacy law;
- a crisis management expert and/or a public relations expert;
- the company's insurance broker—especially if it has cyber insurance; and
- others as necessary.

Step Four – Identifying Whether Cyber Insurance Is in Place

This first involves the determination of whether the construction company has a cyber insurance policy in place. If not, an insurance broker who specializes in cyber insurance for construction companies (usually the company's broker for its CGL, Builder's Risk insurance) should be contacted. The company should work with the broker to put in place a cyber policy that is right for the company. Like the cyber plan itself, there is no one size fits all. The insurance policy should be tailored to factors such as the size and geographic location of the company, the amount of sensitive information that the company has, the amount of risk the company wishes to bear, the amount of the deductible for the policy, among others.

Step Five – Writing the Plan

Once the above factors are investigated, the company can move ahead to place its plan in writing. The plan, like any other corporate policy, should have a section explaining what the plan is, why it is being implemented and what the company hopes to achieve from the plan. Once the preliminaries are set out, the written plan can proceed in three parts. The first part should identify and summarize the investigation to date (as described above) and the short and long-term goals in attempting to minimize the risk of a cyber-attack. The plan should be an evolving document that is supplemented and amended as new information comes into play.

The second part should focus on instituting a series of educational seminars for all company employees on, among other items, the use of email, the dangers of opening or clicking on links that are not safe and the warning signs of phishing for information from hackers. The seminars should also focus on common indications of a fraudulent email, such as non-traditional English (or other language), incorrect tenses, incorrect use of words, a strange email sender address and unusual requests to purchase gift cards or wire money. The seminars should aim to create a kind of "security environment" in which all employees participate. The seminars should also reinforce the idea that a "chain is only as strong as its weakest link" and that to be successful in fending off attacks, all employees must be both knowledgeable and vigilant.

The third part of the plan should focus on exactly what the construction company should do on "game day"—the day a real breach is identified. The procedures should identify items such as to whom a possible breach should be reported and, from there, the personnel that must be identified and in what order. The plan should also identify a person to be "in charge" of the entire breach handling situation. The plan should also identify the preliminary steps that the identified group should take in the event of an actual breach. Such steps include:

- who should be informed of the breach;
- when and where a meeting should take place to discuss the breach;
- a discussion of whether the cyber insurance company should be informed and, if so, what that notice would look like;

- a designated person to work with the cyber insurer to obtain an attorney that will be assigned by the carrier. The attorney will then work with the company to identify and retain a computer forensic company. This may be the same computer forensic company listed in the initial plan or it may be a new company if the company initially identified is not part of the first response team identified in the plan; and
- if the company does not have a cyber insurance policy, a cyber security and data privacy attorney must be identified and retained and then, to protect the privilege, he/she will retain a forensic computer consultant.

Step Six – The Closing

The plan should also provide for a "lessons learned" section. This section would be populated after:

- a breach had been addressed;
- a close call addressed; or
- a practice drill had identified new information and/or information missing from the initial plan.

While no plan will be perfect from the start, constant practice runs and revisions will keep the plan up-to-date and reduce (somewhat) the time and money, as well as the tension, which will be expended when a real breach occurs. Such proactive risk management will pay off in spades.

Reposted from constructionexec.com, October 2, 2019, a publication of Associated Builders and Contractors. *Copyright 2019. All rights reserved.*