ARTICLE

RICHARD R. VOLACK

For More Information Please Contact

Richard R. Volack
rvolack@pecklaw.com
212.382.0909

Failing to Adopt a Comprehensive Cyber Plan Can Lead to Disaster

Despite being aware of cyber risk, and even frightened by it, a shocking number of companies in the construction industry have neither a cyber insurance policy nor a basic cyber security plan to deal with a hack or breach into their computer systems. Once breached, companies with no plan in place become, essentially, a rudderless ship subject to the whims of criminal tides.

A proper cyber plan lays out at least the following:

- the criteria for when a plan would be triggered (i.e., in the event of a breach or a hack);
- which persons inside the company (in-house counsel, IT personnel, executive, project managers) and which persons outside the company (attorney with knowledge of cyber issues and ideally construction law as well; forensic computer experts, crisis management experts; and an insurance broker familiar with cyber policies) should be involved;
- the chain of command and communication in this type of situation and the distinct roles each of the above players will fulfill (Note: this is not the same as the normal corporate chain of command); and
- the various available options to address the breach situation, which will all depend upon the facts at issue—such as the type and extent of the breach and how much of what particular kind of information was lost, stolen or exfiltrated.

Breach plans and protocols do not have to be very long and complicated—but they do need to at least sketch out how the company should react (and the variables it should consider) if it finds itself in the uncharted waters of a breach.

The consequences of not having a plan in place can be catastrophic. Primarily, the failure to have a plan usually means that not only is there no formal set of protocols to follow in the event of breach, but also that no preventative measures have previously been enacted by the company. Such preventative measures include systematic training of the company's personnel to identify possible cyber threats and a penetration test of the company's computer systems to detect (and hopefully correct) any open vulnerabilities. The lack of such basic defenses and preparation can substantially increase the chances that the construction company's system will be hacked.

The failure to have a coordinated, deliberate plan will not only leave open a higher possibility of attack, it will also considerably slow down the company's response and investigation once a breach or hack occurs.

Another consequence of not having a cyber action plan in place is that the hacked company's employees may not realize that a breach coach or an attorney specializing in data privacy and cyber security should be a vital member of the team. Having the attorney on board will usually cloak the consultant's forensic investigation with the attorney work product privilege, thus potentially shielding it from those outside the construction company.

Without the education and rigors of a cyber plan, a construction company also faces a much lower chance of surviving a cyber-attack. Along with standard protocols, a construction company cyber plan will usually include purchasing cyber risk insurance. Such insurance can offset the staggeringly high costs of the consultants that will be necessary to investigate and eliminate a cyber intrusion.

Having a cyber plan in place will also speed up the investigation and response time to the breach for the following reasons:

- Having a plan in place means that when a breach occurs, the company will not waste resources and time sifting through proposals from outside attorneys, computer forensic teams, crisis managers, etc. Ideally, the retainer letters and consultant agreements for those entities would have been negotiated and put in place at an earlier time.
- Retaining attorneys and consultants beforehand allows a pre-breach education on the construction company's risk tolerance and its policies and procedures (especially its IT policies and procedures).
- Having a plan also ensures that the company has trained and put in place the right internal persons to respond to the breach, especially those from the in-house legal and IT departments, as well as those in the C-level, including the Chief Information Officer or the Chief Information Security Officer, if applicable.

It is very important to keep in mind that time is critical in breach situations. Every minute lost is one more minute the hackers are residing in and/or gaining access to the company's computers.

With a plan in place, the hacked company is like a ship with much-needed direction in the form of a map and compass (cyber plan) or at least a good captain (breach coach) to steer the ship where it needs to go and away from the pirates (hackers) that are patiently waiting to invade the company ship.

Reposted from constructionexec.com, October 4, 2019, a publication of Associated Builders and Contractors.