SANDBERG PHOENIX

CONSTRUCTION BLOG

Cyber Crime and Terrorism Threatens the Construction Industry: Contractors Need to be Prepared

AUTHOR: ROSS A. BODEN

If you believe cyber criminals target only large contractors, think again. Cyber criminals attack contractors of all sizes, and in fact, construction firms with less than 250 employees face the highest rate of cyber attacks. Furthermore, the potential exposure includes not only the contractor's own data but also any data to which the contractor has access. This is why it is imperative for *all* contractors to improve cybersecurity preparedness. Hackers need only one weak link for a massive security breach.

A prime example is the infamous data breach at Target in 2013. An HVAC contractor had access to Target's networks for the purpose of installing smart thermostats in Target stores. Hackers penetrated Target's network through the HVAC contractor and stole data from approximately 40 million customers. The breach cost more than $200 million, an insurmountable liability for most contractors.

Common Cybersecurity Threats to Know About

Implementing sound cybersecurity policies requires a basic understanding of common security threats. Hackers constantly change methods, but there are common cyber scams that every construction professional should know about:

Ransomware: This is a form of malware that prevents access to computer systems, e-mail, and data until a ransom is paid. The ransom is typically low enough ($1,000 to $25,000) to make it cheaper than the business interruption, negative publicity, and repair costs. Hackers usually demand the ransom to be paid in cryptocurrency (such as Bitcoin), which is difficult to trace. Even if the ransom is paid, hackers may destroy the data or attack again until the security breach is cured.

Phishing: These scams often try duping employees (or customers) into revealing sensitive information or diverting payments. Like all cyber scams, it is continually more sophisticated and difficult to detect. A classic example is an e-mail from a customer, a reputable source, or a superior with an urgent request to provide sensitive information, click on a malicious link, open an infected attachment, or visit a fake website to enter login credentials for a sensitive account.

Denial of Service: This attack comes in many different forms which are designed to disrupt or flood the targeted server, website, or network until it crashes. These attacks generally do not include a theft or loss of significant information or data, but they are costly and disruptive.

Spyware: This is a form of malware designed to monitor the target's device activity or gather information on the target's device. It can monitor keystrokes, clicks, and internet activity. It is a common way to steal usernames and passwords.

Sabotage, Manipulation, or Terrorism: In the construction industry, a few possible examples could include sabotaging designs, manipulating structural calculations, or taking control of a crane remotely.

Cybersecurity Practice Tips

A robust cybersecurity plan has many layers. While it is highly recommended that construction leaders educate themselves as much as possible and remain actively involved in the implementation, this is not a do-it-yourself task. Engage a professional team to explain the options, requirements, costs, and risks involved. The plan should be a collaborative effort of cyber security consultants, insurers, software vendors, attorneys, and other professional advisors. Synthesizing their different perspectives will achieve better results. Common components of cybersecurity protection include:

- Training employees and controlling access
- Installing firewalls, antivirus, and data encryption software
- Requiring privileged account security on all devices and cloud access
- Backing up data with daily updates
- Advanced threat detection
- Requiring complex passwords
- Regularly updating security systems, software, and passwords
- Developing specific procedures for reporting and responding to attacks
- Designating a response team and point person
- Cyber insurance

- Having your attorneys draft favorable contract provisions to reduce potential exposure with vendors and other contractors

Cyber Insurance Is Highly Recommended

Purchasing cyber insurance is a crucial part of being prepared. Cyber insurance policies and coverages vary significantly, and many general liability and property insurance policies do not provide coverage for losses or liabilities caused by cyber crimes. Contractors should discuss coverage options and limits with their insurance agents and cybersecurity advisors.

Contact a qualified attorney if you need help interpreting the policy, and be sure to know what your policy covers. If you need help determining recommended coverages, discuss your cybersecurity advisors and attorney.

Responding to Attacks

When an attack hits, follow your cybersecurity response plan. Presumably, your response plan will include notifying your cybersecurity professionals, attorneys, employees who need to know, insurers, and law enforcement. If included in your cyber insurance policy, the insurer will hire forensic experts, crisis management teams, public relations advisors, and attorneys to assist in the aftermath. Importantly, always consult with your attorney *before* contacting your insurer. Your attorney can help secure coverage and guard against making statements detrimental to your insurance coverage.

It is highly advisable to speak with your attorney *promptly* after an attack. There are deadlines to report certain scams and data breaches to government agencies, and your attorney can advise on applicable requirements. Cybersecurity threats will never be eliminated, but well-prepared contractors may reduce the negative consequences.