CONSTRUCTION EXECUTIVE CE

Cybersecurity for Contractors—Including How to Mitigate Cyber Attacks

By Michael Needham | Wednesday, December 13, 2023

Safety Best Practices , Cybersecurity , Safety , Risk Management , Technology

Construction companies face numerous issues in the current environment, especially with increased materials costs and labor shortages. Cyberattacks are another area these companies need to pay particular attention to, but they often fly under the radar. Construction companies make for appealing

targets for a handful of reasons:

1. Construction companies store large amounts of sensitive data, especially those that work on government contracts. This data could include bidding strategies or highly sensitive blueprints.

2. Many construction companies use software and devices that could contain vulnerabilities. This includes job-costing systems, time and entry systems and asset tracking software.

3. Construction companies frequently work with numerous vendors and subcontractors. A data breach could affect any of these partnered companies.

The first step towards protecting a company from cyberattacks is identifying possible entry points into the system that cybercriminals can use. Contractors and their employees often rely on construction project-management software to track the status of ongoing projects, which helps them have current data on the progress of projects and track costs and profits. These systems are widely run on smartphones, laptops and/or tablets since project managers are in the field. With so many devices being used, it is hard to enact total security that can protect every single entry point in the system, leaving the system vulnerable to cybercriminals. Even if a construction company has taken proactive measures, its subcontractor or client systems may not be secure. However, there are further steps that can boost cybersecurity for all parties.

IMPLEMENT ZERO-TRUST SECURITY

Zero-trust security systems ensure that every login attempt and user device is authenticated whenever employees want to access sensitive company information. Zero-trust security policies assume that each attempt to access the system is a likely threat until proven otherwise.

For a construction company employing a lot of workers, each of whom is logging in from different locations and devices, zero-trust security can be a good policy for protecting all entry points. Zero-trust security also provides an added layer of data encryption so that even if cybercriminals can pass through the authentication process, they cannot decrypt the stored data.

CHOOSE THE RIGHT SOFTWARE

Construction-management software is a significant part of a company's business and needs to be secure.

When selecting software, choose a company with a proven track record in the construction industry. Look for positive customer reviews from people who have used the product. Check if the developer offers technical assistance. Ensure they provide automatic updates for new threats.
Firewalls and antivirus software are also a must-have. Antivirus software is essential and needs to be consistently updated; A firewall can help build network security and protect the company's devices from unauthorized user access to the company's system.

FOLLOW GOVERNMENT STANDARD SECURITY REGULATIONS

One way to ensure that your company's cybersecurity plan is up to the standard is to make certain your company complies with government-standard cybersecurity regulations. Bring in a certified third party to conduct security analyses and risk assessments. This is a preventive approach that gives your company the ability to identify weak spots within the systems and create solutions before a cyberattack takes place.

CREATE AN INCIDENT RESPONSE PLAN

If a system breach occurs, your construction company must be prepared to deal with the damages. Create a clear incident response plan so that employees know what they are responsible for, what their roles are in enacting companywide damage control and who they should report to.

Conduct regular incident response testing to ensure your company and the policies are clear. You want to be as prepared as possible if a breach occurs. Regular testing clarifies which parts of the incident response plan will run smoothly and where confusion needs to be straightened out.

PURCHASE CYBER INSURANCE

Cyber insurance is a good backup layer for added protection if a cyberattack incident occurs. Most cyber insurance policies will include breach notification and take care of the costs associated with forensic investigation processes.

Other types of insurance, such as professional indemnity and directors and officers liability insurance, will likely exclude cyberattacks from their policies, so purchasing cyber insurance as an additional layer of protection can be a good idea for companies who do not want to be held liable in the event of a data breach or other successful cyberattack.

EDUCATE YOUR EMPLOYEES

Human error accounts for a high proportion of cybersecurity incidents. All employees, subcontractors and temporary workers should be thoroughly trained in cyberattack prevention. Understanding the possible threats and identifying common cyberattack tactics that target employees, such as phishing emails and malware, can add an essential intrinsic layer of security.

Training employees on good security practices–such as regularly installing software updates, creating strong passwords, utilizing multi-factor authentication on all devices and encrypting sensitive data–can prevent slip-ups that might have severe effects. IT policies should be clear to all employees so anyone can report suspicious communication, activity or login attempts to the correct colleague.

In the digital age, companies in almost every industry are susceptible to cyber threats. Mitigating that risk sometimes requires investing significant time and resources, but it can save millions of dollars in the long run.