MCX

CMAA
Construction Management Association of America

Member Communication Experience

Contractors in the Cybersecurity Crosshairs

Written by: Nick Fortuna for Constructor Magazine

The list includes one of the biggest construction companies in France, a prominent North American homebuilder, and a group of Asian-based construction engineering companies. If your business isn't among them, be thankful because those companies were among the 93 construction firms to have suffered a publicly documented ransomware attack in 2020 or 2021, according to a recent report from NordLocker.

Last year, hackers launched thousands of ransomware attacks per day, resulting in more than $20 billion in losses for businesses, according to NordLocker, which provides encryption software integrated with cloud storage. Successful attacks often go unreported because businesses are embarrassed to have been hacked.

Nevertheless, NordLocker analyzed 1,200 ransomware cases that were made public by hackers in 2020 and 2021 and found that the construction industry was the No. 1 target. Manufacturing ranked second with 86 companies hacked, followed by finance (69), health care (64), and education (63).

Construction firms are attractive targets for several reasons, including the large amounts of money typically involved in high-profile projects, according to Kyle P. Murphy, assistant vice president and claims counsel at IAT Insurance Group. His company issues performance and payment bonds to construction companies.

While large construction firms may have robust IT teams in place, smaller companies often lack the resources to ward off attacks, making them especially vulnerable, Murphy says.

“We view cyberattacks as a potential risk to us, so we're educating ourselves, our underwriters, and the companies we do business with to be aware and alert, and to understand that these types of attacks are out there, and they could affect your business,” he says.

Once primarily a paper-and-pencil business, construction firms now have project management systems that are accessible by a wide range of stakeholders, including employees in the office and on jobsites, subcontractors, and vendors. Superintendents are managing tasks in the field using mobile devices and laptops, and office workers are responding to emails and sharing documents from their cubicles.

For a ransomware attack to succeed, all it takes is for one employee to slip up, and since some construction workers may not be computer savvy, that's likely to happen eventually unless you have the proper training in place, Murphy says.

Hackers often send phishing emails to employees, posing as company executives, clients, or other trusted individuals. When the employee opens an attachment or clicks on a link, the user's computer may automatically download malware, giving hackers access to a company's computer network. Another strategy frequently used by hackers is to guess an employee's username and password to gain entry into the system, Murphy says.

Once hackers infiltrate a computer system, the results for businesses can be disastrous, according to Brianne Stewart, construction technology manager for Milwaukee Tool. Ransomware attacks may freeze computers, encrypting all of their files and rendering them useless, unless a company pays the ransom, typically in Bitcoin or another cryptocurrency that's difficult for authorities to trace.

Hackers know that construction companies may be more likely to pay the ransom because they have a low tolerance for business interruption and may face penalties for delivering a project late, Stewart says.

In other cases, hackers may use a subcontractor's logo and invoice template to create a fake bill and submit it to the general contractor. Hackers often will ask construction companies to pay those bills in a new way, such as an ACH payment or wire transfer, claiming that the old way for handling transactions no longer works.

Unusual requests such as these should set off alarm bells for employees, but since the fake emails come from seemingly legitimate accounts, workers may believe them to be authentic and fall for the scam, Stewart says.

"It's important to make it clear to employees that there's no penalty for slowing down and asking questions in these situations," she says. "A lot of phishing scams depend on a sense of urgency from leadership. But if you emphasize in your training that it's important to pick up the phone and double check that something is accurate, you'll reduce the risk of a successful breach."

Corporate blackmail is another way hackers capitalize on network breaches, Murphy says. They may threaten to release sensitive or embarrassing information about a company or its employees, such as HR files or even bidding information that would put the company at a competitive disadvantage if disclosed, he says.

To combat these threats, Jeff Olejnik, principal of the CyberTech division of Wipfli LLP, came up with eight essential cybersecurity strategies for construction companies. His division of Wipfli, a leading accounting and business services firm, often simulates cyberattacks to test clients' susceptibility to hackers, either by sending out phishing emails or attempting to guess employees' passwords.

"When we're hired to do the hack and we show the board of directors exactly how we got into their system, that's powerful, and it usually inspires them to take action," Olejnik says.

For companies to avoid ransomware attacks, C-suite executives must create a workplace culture that takes these threats seriously and acknowledges the potential damage to the company, Olejnik says. Instead of rattling off stats about cybersecurity that are hard to grasp, they should reference specific examples of how ransomware attacks have seriously harmed businesses and their workers, putting a human face on the issue, he adds.

"The tone needs to be set at the top of the organization," Olejnik says. "Your IT team shouldn't have to do the convincing. Cybersecurity is a critical business risk that must be managed, and your IT professional usually won't be able to move the needle in terms of company culture. If it's not coming from the C-suite, then your cybersecurity program is going to fail."

HERE ARE OLEJNIK'S EIGHT CYBERSECURITY BEST PRACTICES FOR CONSTRUCTION COMPANIES:

1. Implement multifactor authentication for remote access and cloud-based services. Many people use simple, easy-to-guess passwords or rely on the same passwords for multiple accounts across their professional and personal lives, making it easier for hackers to compromise those accounts.

Having a second method of authentication, or multifactor authentication, reduces this risk significantly. One popular method is receiving a text message with a code on your mobile device that allows you to log into your email account on your laptop.

2. Train employees regularly. Human error or negligence contributes to about 90% of data breaches, making employees the weakest link in a company's security profile. Employees may get tricked into sharing login information through social engineering, they may send wire transfers or buy gift cards based on fake emails, or they may leave unencrypted laptops in a car that gets stolen.

Companies invest a lot of money in IT tools and technology, but without proper training for employees, companies face an elevated risk. Training should be updated and repeated frequently, and it should emphasize "out-of-band" verification processes before making changes to payment instructions, wire transfers, W2 requests, and bid information.

3. Perform regular vulnerability assessments and penetration testing to identify weaknesses. These tests can reveal a company's vulnerabilities and help executives identify which employees are most likely to fall for a phishing scam and therefore need more extensive training.

4. Implement real-time detection and response. This practice helps companies identify indicators of a breach early. It includes advanced endpoint protection to look for applications that are behaving like ransomware and to identify unusual behavior.

As an example, Olejnik points to a client that experienced suspicious activity with its Office 365 accounts. One employee's account was logged into from Hungary shortly after a login from Wisconsin, but the threat was identified quickly, and the employee was told to reset his password.

5. Ensure proper vulnerability management. Software vulnerabilities are discovered frequently, so companies should keep their software current and apply security patches. Otherwise, those vulnerabilities may be exploited.

6. Test your backup and recovery plans. Companies should be able to restore their data in the event of a ransomware attack, which means backing up your systems at least daily, if not hourly. It's also important to test your backup capabilities to ensure that they work properly.

For example, if you back up your data to Microsoft Azure, take that data in Azure, rebuild it on another server, and then verify from a user perspective that you're able to access it and that it's functional.

7. Block traffic to and from countries in which you don't conduct business. Blocking IP addresses from countries known to launch cyberattacks, including Russia, Iran, and North Korea, is often referred to as "geo-IP filtering" and is an effective way to prevent attacks from hostile foreign actors.

8. Get appropriate levels of cyber coverage. Once easily affordable, premiums are going up, even if your business hasn't experienced a loss, due to the sheer number of cyberattacks launched daily.

Insurance companies are getting tired of writing out big checks to cover losses, so when cyberattacks occur, insurers look for inconsistencies between what was disclosed on the insurance application and what was in place on-site so that they can avoid paying claims. Some insurers are now requiring controls such as multifactor authentication and endpoint detection and response as a condition of coverage.

Talk with your insurance agent so you understand your coverage and any potential gaps in that coverage. Raise specific examples that may be relevant to your business, such as whether the policy covers ransom payments, provides ongoing monitoring if customers' data is affected, or covers costs related to business interruption.

Construction firms that implement all of these measures will greatly diminish their risk of catastrophic losses from cyberattacks, Olejnik says.

"There's no silver bullet," he says. "Cybersecurity has to be a layered approach."

About the Article

Written by Nick Fortuna and republished from Constructor Magazine, a publication of Associated General Contractors of America. The Associated General Contractors of America works to ensure the continued success of the commercial construction industry by advocating for federal, state, and local measures that support the industry; providing opportunities for firms to learn about ways to become more accomplished; and connecting them with the resources and individuals they need to be successful businesses and corporate citizens.

Any views and opinions expressed in this article may or may not reflect the views and opinions of the Construction Management Association of America (CMAA). By publishing this piece, CMAA is not expressing endorsement of the individual, the article, or their association, organization, or company.