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

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 in ltrate 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 les and rendering them useless, unless a company pays the ransom, typically in Bitcoin or another cryptocurrency that's dif cult 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 networ3.2 (cu501 Tm[305500sr10 0 0 10 MurphEEMC)68 (10)3005im1 TC3

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 1 Typical vulnerability assessmentsift cards

About the Article