

5 Ways to Protect Your Construction Business Against Cybersecurity Threats

BY JOSHUA GLAZER

CONSTRUCTION - DEC 6 2017 - 6 MIN
READ



Admit it—you’ve clicked on a questionable link, answered an unnecessary online survey, or been too lazy to update an app. Everyone’s done it. If you’re feeling a bit queasy about these lapses in cybersecurity judgment now, imagine if one of these errors cost your construction business millions of dollars. What if responding to an illicit email put you and all your colleagues out of work?

These worst-case scenarios do happen in the real world, from high-profile breaches like those at Uber, [Equifax](#), and [Target](#) to hackers defrauding small to midsize construction companies every day. In fact, the Target breach was the result of security credentials stolen from a third-party HVAC subcontractor.

Perhaps that well-publicized cybersecurity breach has led cybercriminals to view construction firms as easy targets. But according to technology expert Ashkan Soltani—consultant at Soltani LLC and former chief technologist at the Federal Trade Commission and senior adviser at The White House—it depends on the risk profile.

“Say you’re building a bank: By virtue of operating for that client, you’ll have a higher threat or risk profile,” he says. “Every so often, you may have an expensive or high-value client, so you might need better operational security.”



Soltani says that considering risk is a little like protecting a car against theft: “Do you have a car alarm on your car? Do you have a club for the steering wheel? Perhaps if you live in a really sketchy area where car theft is high, and you have an expensive car, you’d take extra precautions. The same concept is true for businesses. Know your own risk and figure out where you need to invest.”

In 2016, Construction Dive reported a 400 percent increase in ransomware attacks on the construction industry over the previous year. And a survey by researchers at the University of Bolton in the UK found that 70 percent of respondents agreed: “People need to take BIM’s security more seriously.” Add the already rampant use of more traditional fraud against architecture, engineering and construction companies, and it becomes a matter of *when*, not *if*, your company will be threatened by a hacker.

While no security is foolproof, all construction companies can take steps right now to help thwart cybersecurity attacks. Here are five things your firm can do to protect its data and systems.

1. Don’t Let Your Receptionist Be Too Nice

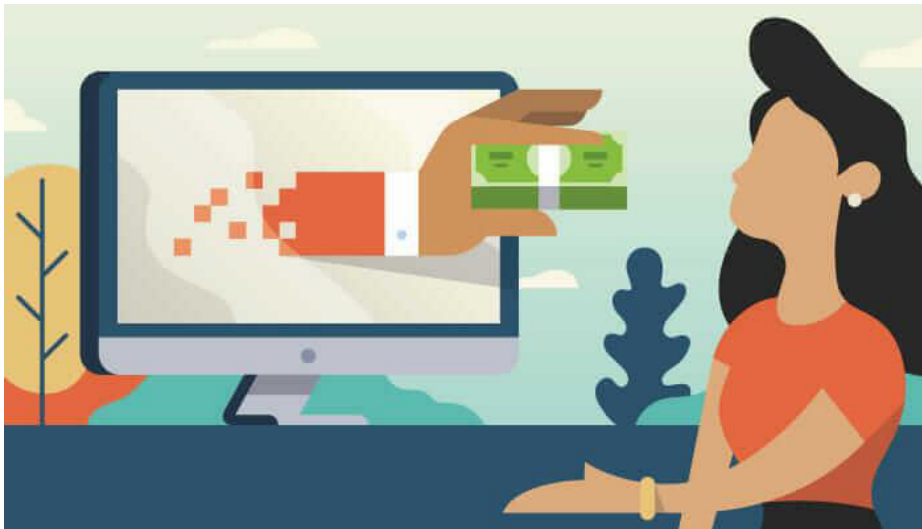
The media portrayal of a hacker is usually some vitamin-D-deprived loner using his modem to penetrate your digital systems through screens of code. The truth is, most hacks include at least a component of social engineering. Bits of banal information given out by a friendly employee on the phone can be used to trick others into allowing in nefarious code online.

“Social engineering is always the weakest link,” Soltani says. “Bad actors or hackers may go after the receptionist or junior associate. Make security a priority and provide Internet-safety training just like you provide job-site-safety training.”

2. Don’t Skimp on Your Email System

Most folks are smart enough to recognize obvious phishing scams. But what if the email comes from a colleague, a partner, or even the CEO of your company? Those attacks are called “spear phishing” and can be enabled by using discount email services that are hijacked to send fake emails from seemingly legitimate accounts.

In a notable case this year, scammers used what appeared to be a legitimate email account from contractors Adolfson & Peterson Construction to trick the Boulder Valley School District into transferring \$850,000 to a fake bank account. Think that’s bad? A similar scam in Edmonton, Canada convinced MacEwan University to transfer nearly \$12 million dollars to bank accounts supposedly belonging to Clark Builders.



The question is, which kind of email service is most secure: a private server in your office basement, a server you lease and manage from a data center off-site, or a cloud-based email system?

“A lot of people are worried about cloud email because the provider can read the email,” Soltani says, “but are you worried about Google reading your email or hackers in the Ukraine reading it? If it’s the latter, I think cloud-storage solutions with strong security features turned on—such as two-factor authentication—are the way to go. Cloud-based companies are monitoring and protecting their systems from millions of users.”

Take extra steps to protect your credentials on cloud-based source-control systems, as well.

3. Consider Hiring an In-House Security Expert

Maintaining IT personnel is expensive, and your company has tight enough margins when trying to win competitive bids. But failing to secure your data can result in losses that could bankrupt your company—and even result in criminal complaints by the FTC.

“The question is, is security enough of an issue to merit the CIO hiring a junior admin who is sole-tasked with security?” Soltani asks. “Whatever that salary is, say \$100,000 a year, is it worth it to your firm to invest in that? If the answer is yes, you hire that person and make him or her responsible for implementing solutions to address your security risk, such as patching systems or setting up VPNs for people when they’re working with client data at Wi-Fi hot spots.”

If you’re not ready to hire full-time IT staff, you need to at least work with an expert who can help you navigate rapidly changing cybersecurity threats. A 2016 report by DHG Assurance Services recommends contracting the services of an IT adviser with CISSP, CCE, CISA, CRISC, and GCIH certifications. And check out this comprehensive Start With Security best-practices guide from the Federal Trade Commission.

4. Limit the Number of Admins

Another area where companies compromise security for convenience is giving too many employees admin-level access. This can become especially problematic, as networked systems like BIM grant access to your intellectual property remotely and throughout many third-party stakeholders.

