Eric Messer
Business & Risk Consultant - Construction
emesser@starrgroup.com

The STARR GROUP
Insurance & Risk Solutions

5005 Loomis Road, Greenfield, WI 53220
P: (414) 421-3800 F: (414) 421-6145

Visit us at StarrGroup.com

***THE STARR GROUP**: Performance-driven analytic risk advisors that deliver insurance, benefits, cost control, and DE-RISKING strategies to ambitious leaders looking to break-free from insurance dependency and boost performance.*

7 ways to hack a construction firm and how to prevent them

Dive Brief:

- **Cyberattacks are serious threats to the construction industry. In the last three years, cloud-based email breaches cost U.S. businesses more than $2 billion.**
- **Despite news reports of foreign hackers, 85% of the hacking activity originates within the U.S., with 56% coming from the same state and 35% from the same city as the victimized company.**
- **Company executives in all industries are increasingly concerned about system breaches, compromised email and ransomware attacks, cybersecurity expert David Anderson said during an educational session at last month's Construction Financial Management Association conference. But companies can take steps to protect themselves.**

Dive Insight:

Anderson, principal cybersecurity consultant at Minneapolis-based CliftonLarsonAllen, told the CFMA audience just how susceptible construction firms can be to this type of crime.

He said that about 80% of data breaches involve password compromises. An increase in remote working during COVID-19 helped increase opportunities for breaches. Moreover, remote access isn't being revoked. It's become the post-pandemic norm, he said.

"The number of users with remote access greatly increased," Anderson said. "Lots of hackers have moved from malware to credential stealing to get their foothold. They can look for VPN technologies and attempt to connect with your work systems using those technologies."

Besides password compromises, there are several other tactics that hackers use to infiltrate companies, Anderson said. They include:

Business email compromise. Techniques include email spoofing, where fraudsters pose as trusted email senders asking recipients to click on links enabling them to gain access to data.

Domain impersonation. Attackers purchase a domain name similar in appearance to a company's or vendors. Changing a letter "l" to a numeral "1" can fool recipients into trusting emailers.

Name dropping. Fraudsters create an email address appearing to be a CEO's personal address, then ask an employee, for instance, to buy and mail gift cards to a given address.

Unauthorized access. In another technique hackers gain unauthorized access to a company or vendor email and use the compromised legitimate mailbox to send email. "The hacker is in control of the outgoing messages being sent," Anderson said.

Password guessing. Security professionals and fraudsters alike possess tools to guess passwords. Hackers know and try common passwords like Summer2021.

"It's very easy for hackers to password guess against your users," Anderson said. "Weak passwords can be susceptible to a guessing attack."

Password guessing also occurs after websites are hacked. LinkedIn, for instance, has been hacked, users' passwords stolen and sold online. In many cases, people with LinkedIn profiles reuse LinkedIn passwords on work email systems. Anderson urges using the legitimate website, "Have I Been Pwned?" to look up accounts and learn whether those online sites have fallen victim to known data breaches.

Ransomware. In this especially insidious type of attack, fraudsters hack into a company's network, gain full administrative control, then deploy ransomware to lock the company's systems. The hackers demand ransom to unlock the system. Many criminals delete company backups in their initial system penetration.

"Another tactic is before deleting the backups, they download the backups and capture data," Anderson said.

"They reach out [to victim companies] and say, 'Pay me X amount of Bitcoin to recover your system and pay me an additional amount not to release this data to the world.'" Data can include Social Security numbers, addresses and more.

To combat these types of cyber risks, Anderson recommended these protective measures:

- Enable multi-factor authentication on as many accounts as possible.
- Harden your email spam filter.
- Create a strong password policy with long passwords.
- Train your end users.
- Keep good backups, isolated from your network.
- Consider cyber insurance.
- Evaluate security controls of third parties.

This article was written by Jeffrey Steele and posted on constructiondive.com, published on 8/11/2021.