MCX

CMAA
Construction Management
Association of America

Member Communication Experience

The Construction Industry Is More Vulnerable Than Ever to Cyber Attacks

Written by: Hannah Hoeflinger, National Cyber Risk Operations Leader, and
Dan Hanson, Senior Vice President, both with Marsh McLennan Agency

Over the past decade, the construction industry has become more and more reliant on technology, in particular to help manage a widely distributed workforce. Using laptops, tablets, and smartphones as a digital network, along with Wi-Fi use at field offices, home offices, and elsewhere have potentially opened the door to more cyber attacks.

According to a Travelers Companies survey, 87% of construction business decision-makers are reliant on technology functioning properly so their business can operate. That same survey shows that 40% of construction industry business leaders believe their business is becoming somewhat riskier with each year. However, 20% say they are not knowledgeable about the cyber issues that could have a negative impact on their companies. And only 30% have a written business continuity plan to help them survive and recover from a cyber-attack.

In recent years, cloud-based email breaches alone have cost U.S. businesses more than $2 billion. The average cost of a data breach in 2020 was $150 million. How many businesses can continue in the face of a loss that large?

Ransomware attacks have increased. Recent victims of ransomware attacks in construction have ranged from an Asia-based group of construction engineering companies that consult on projects worth an estimated $20 billion annually to small, family-owned enterprises, such as a roofing company in Texas, according to NordLocker, an encryption software firm.

Most of these occur because of human error, not because the technology failed. Cyber-criminals have become increasingly sophisticated, responding quickly to preventive and protective measures.

Construction companies hold a lot of valuable information that hackers would love to get their hands on. A data breach could mean losing customers, destruction of a reputation, liability for lost data, and even financial ruin. Most companies cannot afford to take that chance. Given all of that, it's baffling why a Rival Security study reports that 84% of companies lack adequate IT security.

WHY ARE CONSTRUCTION COMPANIES AT RISK?

Construction is now the number one industry for ransomware attacks, according to the NordLocker analysis. Construction companies are appealing targets for cyber criminals. They are vulnerable to losing funds, information, or even having the smart technology in the buildings they're involved with hacked and held for ransom.

Construction relies on Internet of Things devices for asset tracking, worksite security, machine control, wearable technology, and more. This interconnected approach - along with surveillance devices like IP cameras and GPS-connected drones, and a lack of industry cyber defense - has resulted in a serious rise in successful cyber attacks. Construction companies also rely on associations with third parties - such as subcontractors - making them even more vulnerable.

HOW ARE CYBER CRIMINALS GAINING ACCESS?

Favored approaches include denial of service attacks, which disrupt operations and crash the server or network. These attacks can also enable hackers to install malware or ransomware they can use to copy or lock data, change security settings, connect a company to a malicious network, consume resources, and even remotely control systems. Hackers can gain access by exploiting third-party vulnerabilities such as weak passwords, unsecured hardware, apps, or connected cloud services.

Phishing presents a major threat, according to the Verizon Data Breach Study, which reports that 93% of data breaches occur through phishing campaigns. Legitimate-looking emails are sent to company employees who unwittingly install malicious software on their devices or provide personal information, like passwords. Other threats include fake websites and email addresses, which scammers use to get into your network, and social engineering, where cyber criminals build trust through fake ads or other means and use that trust to extract valuable personal data or logins.

THE HARD REALITY: CYBER COVERAGE IS HARD TO GET AND COSTS MORE

More and more contractors are being hit by cyber criminals. The amount of capital involved and the ability to threaten the safety of the project are attractive reasons for cyber criminals to target the industry. More claims activity has resulted in insurance premium increases, but these have so far been relatively modest. However, rate increases through the balance of 2022 and into 2023 are inevitable.

Policyholders are also spending more on deductibles, uninsured losses, safety programs, equipment and safety training, and a host of other related expenses. Another growing expense is for analytical tools, which can help leaders make intelligent risk management decisions and are critical to discovering where risk management problems may be lurking.

There are obvious costs associated with inadequate risk management, but there is also the potential of indirect costs from downtime, recruiting, and training.

Shopping for the lowest possible premium is a go-to strategy for trying to lower expenses. However, the only significant way to lower costs is to lower the frequency and severity of claims. That's why investing in risk management can often pay enormous dividends.

CONTRACTORS NEED TO BE PROACTIVE AND VIGILANT - AND SO DO THEIR EMPLOYEES

Every construction firm needs to identify vulnerabilities and locate security weaknesses as soon as possible. Develop written plans to protect against cyber attacks as well as detailed guides to how the company will respond when it happens. Train every employee, vendor, supplier - every entity or person associated with every project - and make certain training is repeated and updated. Everyone needs to understand how to spot potential problems and how to respond to cyber threats.

Work with qualified experts who have the knowledge and tools to help identify and manage risk - including cyber insurance and cyber best practices, and develop training for the most important protections, such as multi-factor authentication, password management, getting rid of end-of-life software, and more. Finally, remember that no company is invulnerable. Be forewarned and prepared.

About the Authors

Hannah Hoeflinger is national cyber risk operations leader for Marsh McLennan Agency. She can be reached at Hannah.Hoeflinger@MarshMMA.com.

Dan Hanson is senior vice president for management liability with the Marsh McLennan Agency. He can be reached at dan.hanson@marshmma.com.

About the Article

Republished from Construction Executive, a publication of Associated Builders and Contractors. Copyright 2021. All rights reserved. Associated Builders and Contractors is a national construction industry trade association representing more than 21,000 members. Based on the merit shop philosophy, ABC helps its members develop people, win work, and deliver work safely, ethically, and profitably for the betterment of the communities in which they work.

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.