Understanding Cyber Threats

IN CONSTRUCTION

4 Ways to Protect Your Business from Attack

DWIGHT ANDRUS

INTRODUCTION

Everyone is familiar with the data breaches that have hit major financial companies in recent years, exposing millions of customers' personal data to internet scammers and identity thieves. These banks and firms are understandably irresistible to hackers in search of a payday. But as those targets increase their defenses, internet criminals have widened their focus, developing new ways to attack a variety of businesses – including construction. In fact, the last few years have seen such **a spike in cyber attacks against construction companies that the industry ranks first in ransomware attacks[1], costing companies across the world more than $2 billion.[2]** But why construction — and why now?

There are several aspects of the construction industry that make it more vulnerable to online threats. One obvious factor is simply a widespread lack of preparedness. As other industries have been forced to strengthen their online security – either following attacks or due to new regulations — many criminals have moved on to softer targets and different tactics.

Construction firms do have valuable data, including confidential and proprietary information stored digitally and accessed remotely. This kind of sensitive information (e.g., bid data, intellectual property, and financial reports) can be stolen via cyber actors who then extort the business for hefty sums. Adding to this risk is the proliferation of technology in the industry, in the form of mobile devices like phones and tablets, as well as new project management software and tracking programs. These tools have helped construction companies increase their efficiency, while also offering cyber criminals even more ways to gain access to their data. Throw in third-parties and contractors who also access parts of your system and the threat grows exponentially.

All these factors are why cyber losses have continued to climb in the construction industry since 2010, but most dramatically since 2020. This rise has been part of an overall increase in attacks against businesses: according to the FBI, **cyber attacks rose by 400% in 2020 alone.[3]**

While companies often choose not to publicly disclose that they were attacked, the costs can prove devastating. As a high-volume, low-margin business highly tied to deadlines and contract specifications, any strain on cash flow can impact operations and lead to major financial penalties or losses.[4]

How are Criminals Getting In?

Cyber crime continues to evolve in response to new vulnerabilities and security protocols. While some attacks have grown more sophisticated, the majority rely on human fallibility. At a recent industry conference, cybersecurity expert David Anderson noted that 80% of data breaches involve compromised passwords.

> **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.[5]**

[1] Nordlocker Report 2021 Analysis of top industries hit by ransomware

[2,5] Dive Brief: Summary of comments by cybersecurity expert David Anderson during an educational session at the July 2021 Construction Financial Management Association conference.

[3] Advisen data/©Zywave, "Cyber Losses in Construction Are on the Rise."

[4] AON: Cyber Vulnerability In The Construction Sector

Email communication is one of the easiest ways for malicious actors to gain access to a company's internal data. It starts with individual passwords, which are rarely set to the maximum parameters for security (length, uniqueness, two-factor authentication). That means fraudsters can often simply guess weak passwords, but they can also easily obtain them from published hacks of other websites, because people often use the same passwords for business and personal activities.

Beyond password compromise, cyber attackers have developed several ways of tricking people using business email accounts. Email spoofing and phishing are both designed to get recipients to click on a link or download a file which then installs malware or other malicious programs. **Some savvy scammers may create fake email accounts that appear to belong to a company executive in order to access sensitive information or send money.** Once a cyber criminal has successfully compromised a single computer or email account, he or she can use it to more convincingly target other company accounts.

Ransomware is a particularly nasty form of malware that allows criminals to hack into a company's network, take administrative control, and then lock the system from the inside and often delete any system backups that may exist. Then, they demand payment (usually in Bitcoin) from the business to get their data back. According to Anderson, they may even request a second payment for not posting the company's data publicly.[6] While ransomware is less common than other data breaches, these attacks continue to grow and pose a serious threat to all construction firms.

What can Construction Businesses do to Protect Themselves from the Growing Cyber Threat?

There's quite a bit that companies can do to safeguard their data, or at least make it harder for thieves to access it. The first step is a risk assessment to identify vulnerabilities and weak points in various defenses. An outside security firm can assist with this process and help ensure necessary measures are implemented throughout company operations. They can also help develop a plan for regular testing, system upgrades and other routine security requirements.

When choosing a security firm, it's important to check their credentials, years of experience, contractual terms, insurance carried, and more — before you engage with them.[7]

One major focus of any effort to improve company security should be training employees. Practicing good cyber hygiene and best practices is the responsibility of every person on staff, whether full- or part-time. Workers need to be able to recognize potential phishing attacks or spoofed domains in emails. They also need clear instructions for what to do if they suspect a breach has occured. Businesses should also consider requiring stronger passwords that are regularly updated (or even multi-factor authentication).

As construction businesses evaluate their risk for cyber attack, they should also review the security protocols for any third-parties that they work with. Are there agreed-upon policies or requirements included in legal contracts that cover each company's responsibility for cyber security? There should be.

[6] Ibid
[7] Jennifer A. Beckage, Esq. and Daniel J. Parziale, Esq., "Why The Construction Industry Is Being Impacted By Cyberattacks, And What To Do About It," AGC'S 2021 Surety Bonding And Construction Risk Management Conference.

In the spirit of "better safe than sorry," companies need to have a plan for how to respond when they are attacked or suspect a breach has occurred. It should detail roles and responsibilities, emergency procedures, and steps to be taken to restore the system with all company data as quickly as possible. Having a secure, remotely stored system backup is one of the easiest ways to protect your data and avoid paying ransom demands.[8]

The steps above can help companies lower their risk of cyber crime, but one way to mitigate the potential threat is through specialized insurance coverage.

At Dwight Andrus Insurance, we help our clients secure the right kind and level of coverage for their unique needs. Contact us today to learn how we can help protect your construction business from the growing cyber threat.

Cyber Crime and Business Insurance

Traditional business policies that cover crime, property, liability, kidnap, ransom, etc., may provide some limited coverage in case of cyber attack. However, as the threat grows, many policies are narrowing their scope to exclude cyber risk-related costs. That's why a comprehensive, stand-alone cyber insurance policy may be needed to fully protect businesses.[9]

Protecting businesses from the risks of cyber attack is no simple matter. And the costs incurred following a breach can add up quickly. There's the company's liability to those affected. This may include damages/fines, settlements, attorney fees, etc., depending on the nature of the incident. Then there are the costs of responding to the breach, like notifying affected individuals, credit/identity theft monitoring, and PR assistance. Add to that the cost of a) making the extortion payment to retrieve data, or b) paying to restore data in another manner — plus the operational downtime until systems are restored. Of course, there can be other unexpected costs such as forensic experts or other services.

Cyber attack insurance policies can provide coverage for **different types of attacks/risks:**

- Data breach expenses
- Cyber extortion or ransomware
- Fraudulent wire transfer
- Business interruption

Don't wait...

The threat of cyber crime is real and increasing for businesses of all sizes in the construction industry. Don't make the mistake of thinking your company won't be targeted or that you'll be somehow overlooked by the millions of malicious actors on the internet. Assume it's a matter of time before the hackers get to you, because it could be just that. Take the necessary precautions now to protect your company's data, reputation and bottom line. Contact Dwight Andrus Insurance today to learn how.

[8] Nordlocker Report 2021 Analysis of top industries hit by ransomware
[9] AON: Cyber Vulnerability In The Construction Sector