

How to Outsmart Cybersecurity Threats

Written by: David Lukić, Information Privacy, Security, and Compliance Consultant, idstrong.com

FOUR STEPS TO ENSURE THE SAFETY OF YOUR COMPANY'S FINANCIAL DATA

Construction work is conceptualized by many as an active line of work, far removed from the standard 9 a.m. to 5 p.m. desk job. However, most people do not consider how much information is stored digitally. As a result, people underestimate the wealth of information that might be desirable to hackers.

Client and vendor information, financial records, and intellectual property (IP) data are all valuable and susceptible to cyberattacks. Hackers can and will target anyone, using several different methods, including phishing, social engineering, and data breaches.

Taking a proactive stance is the best way to protect your company from online attacks. What can you do to protect yourself and your colleagues?

How Can Hackers Target Your Company?

There are several methods cybercriminals use to access valuable data. Some of the most common methods are:

- » Data breaches – A data breach occurs when sensitive, protected or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. This can be done through the installation of ransomware on your computer via a phishing attack
- » Ransomware & phishing attacks – Ransomware is harmful software that can be installed on company equipment, most



often downloaded by unsuspecting employees who click on a harmful link. Why might an employee click on a harmful link? This is where social engineering and phishing come into play.

- » Social engineering – This is a form of manipulation used by cybercriminals to get employees to help release confidential information. By imitating a company email or an email address or format from a trusted source, cybercriminals can make their attempt convincing to those ignorant about the signs of a phishing attack.
- » Insider threat – The above types of fraud can come from both past and current employees through inattention or carelessness.

What Happens to Your Data?

What does a hacker do with the information they've stolen from your company? Most often, the answer is industrial

espionage. For example, in 2006, a South Korean steel and construction company fell prey to one of the largest cybersecurity attacks in recent memory, which impacted over 70 major companies across the globe.

This attack resulted in an unprecedented transfer of wealth in the form of IP and trade secrets. Credit card numbers and security codes can be used to create clone cards for making fraudulent transactions and social security numbers and home addresses can lead to identity theft or fraudulent tax returns.

Cybercriminals not only sell your data to other people, but they can also attempt to sell it back to you in the form of a ransom. They may threaten to leak client or vendor information and blueprints to competitors unless you send them an exorbitant sum of money to buy their silence.

All of this creates a lot of risk for you, your company, and your employees. However, there are several steps you can take to ensure the safety of company data.

1. EDUCATE YOUR EMPLOYEES

The most important factor in being proactive against cyberattacks is to educate your employees. Remind them to use strong passwords when using company systems and email.

One suggested method is to skip the complicated password and opt for a simpler solution. Instead of creating a convoluted password that they're tempted to write down (which increases the chances it may get stolen), encourage employees to use a phrase from their favorite show or movie that they will remember, but will be difficult for someone else to guess. The longer the password, the more secure it is.

Inform employees about phishing, ransomware, and other forms of social engineering. This can be mandated with training videos, but it's better to make the sessions interactive.

Encourage employees to take a phishing test on their own, and reward the employees who earn the top scores. Engagement leads to better retention, which improves the safety of your company's IP and other sensitive data.

2. CREATE A CYBERSECURITY PLAN

A recent risk management report suggested that company owners create a disaster relief plan and perform mock drills to gauge employee response. The report suggests designing a

cybersecurity plan that is unique to your company.

Determine your own cybersecurity goals and needs through a risk assessment. Too often, organizations are sold a plan by a vendor. However, if a breach occurs, such a plan would do little to prevent legal and technical risk.

3. BE AWARE OF EMERGING THREATS


It's important to stay current on cybersecurity trends, as well as threats affecting all different types of businesses. Northeastern University recently highlighted seven important cybersecurity trends in 2021:

- » New technology and devices
- » Increasing ransomware attacks
- » Attacks on cloud services
- » Outdated and inefficient systems
- » Remote work risks
- » Continued use of multifactor authentication
- » Increased interest in data privacy

While many of these may seem like no-brainers, it's important to dive deeper into each one if you are serious about protecting your company. Set aside time in your workday to review cybersecurity news, and in the construction industry, and pay attention to how firms are handling safety to avoid serious data breaches.

4. CONSIDER THIRD-PARTY PENETRATION TESTING

While it's important to have your own robust internal monitoring systems, it can be helpful to have an outside perspective on your cybersecurity plan. Consider hiring an outside information technology (IT) firm to perform penetration testing and a security audit to spot gaps or issues your team may have overlooked. Companies that conduct identity monitoring and provide regular credit reports and credit score checks are available, but be sure you're hiring a trustworthy source.

All companies should be concerned about cybersecurity, regardless of their goals or purpose. Act today to protect your construction company's financial data. You can do this through staff education and employing rigorous cybersecurity measures. 



About the Author

David Lukić is an information privacy, security, and compliance consultant at idstrong.com. Lukić has a passion for cybersecurity and shares his knowledge in order to make it accessible and interesting for businesses.

Visit idstrong.com.

About the Article

Republished from [Construction Business Owner](#). Construction Business Owner (CBO) is the leading business magazine for contractors and is designed to help owners of construction firms run successful businesses. Founded in 2004, CBO provides real-world business management education and knowledge that is of real value to the owners of construction companies.

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.