Viewpoint Blog

Why Cybersecurity Matters in Construction — Part 2 of 2

Learn the Best Practices to Thwart Common Cyberattacks and What to Look For in Future Threats

In part one of this two-part blog series, we looked at a real-world example of a data security breach at a construction company, the steps that company took to get through the attack, and what it did to protect itself moving forward. Now, we'll share some construction cybersecurity best practices and insider tips on what to be on the lookout for.

A recent report by IBM Ponemon found that 74% of organizations do not have a security response plan ready in the case of a cybersecurity attack. This puts companies at a significantly higher risk of falling victim to cyber criminals. The construction industry is #3 on Safety Detective's list of industries that are currently suffering from the most ransomware attacks. In our recent webinar, *Cybersecurity in Construction*, Mike Dooley, Viewpoint's information security officer, sat down and discussed security best practices that every organization should consider.

Best Practices for Construction Cybersecurity

Having a plan ready for a potential cyber security threat can lower the probability of a successful attack.

Many organizations that have cyber insurance think they are fully protected from a cyberattack. However, this is not the case. Construction organizations need to be doing everything they possibly

can to lower the probability of a successful attack.

By planning ahead and investing in proper security, costly business mistakes can be avoided. Here are four things your organization can do right now to slam the door on cyber criminals:

1. Stop Taking the Bait: All it takes is the click of a wrong link or attachment for ransomware to be downloaded to a computer. Make sure to triple check all emails for strange email addresses, URLs or requests. If anything seems fishy, send it to your IT department to have checked.

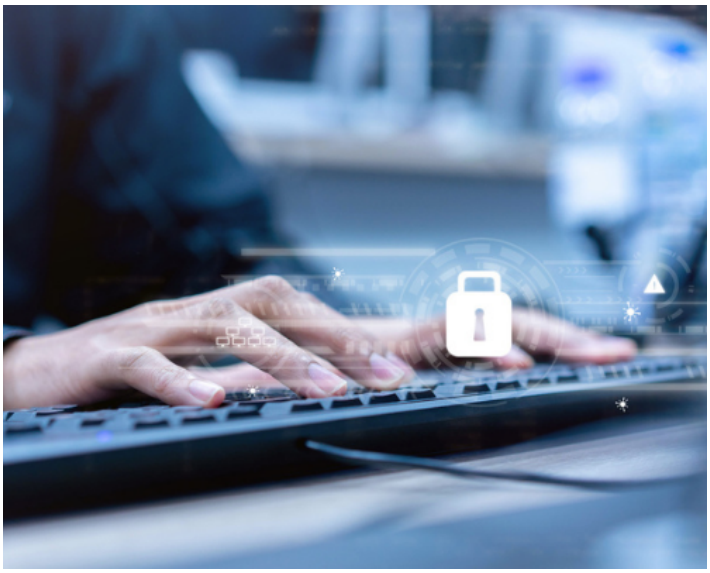
2. Continuous Training: Build and train a company that is constantly thinking about data security. Employees should be looking out for threats as they open every email, visit every website or perform any action on their computing device. Hosting training sessions and showing employees exactly what they should be looking for is a great step towards avoiding cyberattacks.

3. Passphrases Not Passwords: Breaking employee passwords is one of the most common ways for cyber criminals to access company data. To increase security, it is recommended that employees use an entire phrase when creating a password. Including spaces between a minimum of four words is a great start but to make it even more complicated, try adding in characters, numbers and case-sensitive words. By lengthening and complicating this form of security, hackers will have a much more difficult time getting through

4. Multi-Factor Authentication: MFA on high value assets is a must! Enabling this feature on all assets is ideal, but at the least, make sure all high-security logins require employees to verify their identity in more than one way.

When a cybersecurity attack occurs, time is of the essence. Cyber criminals are known for attacking companies more than once, especially when the company was easy to exploit the first time around. Any company that does not have a plan in place is only making the hacker's job that much easier. Remember that something is always better than nothing.

What's Next for Ransomware?



There are multiple topics your organization should be aware of in 2021.

There are many avenues that criminals have to breach personal and business data, from phishing schemes to wire transfer and invoicing fraud to malware on computing devices. Yet ransomware is one of the most commonly used tactics against businesses. Here are five ransomware topics to be aware of as you make your way through 2021.

1. Life and Death Matter: Ransomware attacks are becoming more and more frequent. As attackers begin to make their way into more industries, including health systems, lives are being put at risk. Even in the construction industry, cyberattacks pose a risk to employee wellbeing. Make sure your company is doing their part in preventing these attacks.

2. Pivot to Extortion: While this is nothing new, cyber criminals have multiple ways of getting what they want. It is one thing to lock down infrastructure, it is a whole other situation when they threaten to expose all confidential information. Your organization should have multiple plans in place for dealing with various types of attacks and threats.

3. Ransomware Response Plan: Organizations can no longer afford to be unprepared. Customers are taking cybersecurity more seriously after witnessing the severity of recent attacks. As other organizations prepare to fight back against cyberattacks, your organization should be doing the same.

4. Ransomware Legislation: With the new presidential administration comes new legislation. A new law is currently in the works for making the payments of cyber ransoms illegal. With this looming on the 2021 horizon, it is now more important than ever for organizations to do everything they can to prevent cyber attacks. In addition, organizations need to have a game plan ready that does not include paying the ransom.

5. Next Generation of Security Professionals: With a shortage of qualified professionals, cybersecurity has a highly competitive job market. This is the perfect opportunity for college graduates and interns to capitalize on. As an organization who may be looking into hiring a security professional to assist in cybersecurity, be ready to offer a competitive wage and filter through a

large number of candidates to find the right fit.

To hear more about how your organization can better prepare for a cybersecurity attack, watch the *Cybersecurity in Construction* webinar here:

Viewpoint is committed to ensuring our software is protected against cyberattacks. To learn more, click here.

Posted By

Kati Viscaino

Kati is an Associate Manager of Customer Advocacy at Trimble Viewpoint, enthusiastic about all things marketing and construction.