Tips for Protecting Your Construction Business from Cyber Attacks

Cybersecurity should be of utmost importance to the construction marketplace. Today, mobile platforms are very much integrated into how construction professionals perform jobs. At the same time, more and more connected technologies are present in the workplace and at the jobsite.

For construction, this technology is also becoming more integrated into heavy equipment as well, and this can impact the construction industry in a number of different ways, according to Matt Barrett, cybersecurity and privacy applications group leader, NIST's Information Technology Laboratory.

"The simple act of charging your mobile phone using a nearby USB port could cause the equipment you are using to malfunction," he explains. "If that happens at the wrong time, perhaps you have a safety issue, even loss of life. An equipment malfunction could also cause an interruption of construction activity and schedule. When you've got multiple trades dependent on the master schedule, there can be significant financial impacts from a simple and seemingly harmless act."

With this in mind, he suggests it is really important to educate project teams on the possibilities so they know what to do and what not to do.

How Cybersecurity Impacts the Jobsite

For construction companies interested in learning more about how cybersecurity impacts the job there are a couple key steps that should be followed:

1. Address concerns.
2. Create a strategy for success for the business and workers.

In general, cybersecurity has become more complex, as malware attacks have continued to skyrocket, with ransomware leading the charge.

Scott Schober, president and CEO of Berkeley Varitronics Systems, explains that cybersecurity concerns have only increased and they will only continue. He attributes this is due to a number of factors.

He says, "Companies remain too complacent when it comes to routine data backup, which is the most effective counter to any ransomware demand. User behavior has not changed fast enough to keep pace with the onslaught of attacks. I witness cyber-complacency daily in organizations that feel it won't happen to them, a dangerous stance that leads to lack of preparedness in security situations."

Preventing Cybersecurity Attacks

He points to the example of Turner Construction, which was the victim of a focused spear phishing attack that could've been easily prevented.

"When an employee unknowingly sent employee tax information to a hacker, confidential information including name, social security number, bank account information and login credentials were shared with criminals," he explains.

He offers the following advice:

1. Cyber awareness training for all employees.
2. Teaching good cyber-hygiene throughout an organization. This means training management as well as the office personnel all the way to the workers at the jobsite.
3. A third party can assist help train and test the staff.

Looking beyond the growing malware attacks that are impacting companies across the country, cybersecurity in general has become more complex and they are becoming more sophisticated in their approaches.

Barrett of NIST explains that cybersecurity requires many groups of people to know their part in cybersecurity and to perform their part well.

"Users need to understand how to use technology the right way, and be aware of how technology might be misused," he says. "Executives need to understand how to allocate money and time to cybersecurity."

Often, putting good practices and training in place first begins with creating a strategy for cybersecurity within the construction company.

A Strategy for Success

The first step to addressing cybersecurity concerns is to create a policy for how cybersecurity will be addressed within the company.

Schober says it is important for organizations to be proactive and diligent in the face of growing cyber crime. This means putting basic controls and protocols, which include:

- Create a regular backup plan for all data stored offsite. Any cost effective cloud storage provider is a good start.
- Use only name brand security software on every computer, tablet and laptop that is automatically updated to combat the latest threats.
- Update all operating system regularly and never use unsupported outdated software.
- Verify all firewalls have the latest security patches installed.
- All mobile devices on your network should have both hardware and software encryption with a long and strong password or PIN required for access.

- Verify the Wi-Fi network within the company and at the job site is secure, encrypted and has a long and strong password. Set up MAC filtering to only accept pre-approved employee devices.

While putting good controls and protocols in place is the first step, Schober also suggests quarterly training sessions where companies can improve the cybersecurity culture to demonstrate that everyone is an integral part of the security. This will help all employees so that 'thinking cyber' becomes part of everyone's daily job requirements.

"By raising awareness, employees will realize the importance of slowing down to question anything that seems a bit off," he says. "They will also come to understand that they will be rewarded for reporting something and not chastised by management for being overly cautious."

It is also important for construction companies to create a clear policy about what technologies are allowed or not allowed in the workplace.

Barrett of NIST suggests asking this key question: Is it acceptable for your employees to use their own device (laptop, tablet, phone, etc.) to interact with corporate mail servers, wireless networks, and computers? Perhaps, even more importantly, do your employees know the answer to this question? 

Enlisting the Help of Cybersecurity Experts

When it comes time to implementing new solutions and training operators out at the construction jobsite, there are a number of tools and organizations available to help. For instance, the National Cybersecurity Center of Excellence develops and publishes technical solutions so companies can copy and implement those solutions. While it requires some customization, it will help address cybersecurity.

There are also organizations that specialize in cybersecurity training for people who are not cybersecurity experts. This basic level of awareness is critical for operators to avoid some of the adverse scenarios.

"For instance, there are services that send your employees email that mimic phishing attacks," explains Barret of NIST. "You can get reports on how many employees clicked on the links,

which might have infected your computers with malware in a legitimate phishing attack. You can then talk with those employees about how to handle the situation better next time."

Construction companies can also consider the Cybersecurity Framework from NIST as a way to understand their current cybersecurity, define what they want their cybersecurity to be, and determine how to get to that target state. It also offers an easy-to-understand approach for those who are not cybersecurity experts and bridges to more technical methodologies known by cybersecurity practitioners.

Going Forward

While cybersecurity concerns are complex today, this is only going to continue to grow in the near future. This is because technology continues to evolve and impact organizations at every level.

Wes Smith, president, AEC Cloud, points to a new, emerging trend: "Blockchain and decentralized trust-enabled systems are coming. Likely rearing their head via consortiums, Internet of Things and artificial intelligence."

As all this happens and evolves, it is important to remember that every company that is connected to the Internet is a potential target for hackers.

In construction, many jobsites are remotely accessible with building information modeling, but this also opens the doors for hackers to launch targeted cyber attacks. Further, there are many wireless sensors and advanced telematics that can inadvertently act as a conduit for attacks. Once a hacker gains access, they can move laterally throughout the network, affecting other connected machines and devices.

Schober of Berkeley Varitronics Systems concludes, "Workers using their own smartphones, tablets and laptops at work must take into account the possibility of their own devices acting as carriers for malware invading their company's network."

Take the time now to invest in cybersecurity training and prevention methods to ensure your jobsite will remain a safe and secure place in the future.

Source: http://www.conexpoconagg.com/news/february-2018/tips-for-protecting-your-construction-business-fro/?utm_term=Tips%20for%20Protecting%20Your%20Construction%20Business%20from%20Cyber-Attacks&utm_campaign=Today%5Cu2019s%20Construction%20%2526%20Tech%20Trends&utm_content=email&utm_source=Act-On%20Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-Today%5Cu2019s%20Construction%20%2526%20Tech%20Trends-_-Tips%20for%20Protecting%20Your%20Construction%20Business%20from%20Cyber-Attacks