CYBERSECURITY RISK & THREATS ARE A CONSTRUCTION CONCERN

When we think of cybersecurity, we don't instantly think of the construction industry as a significant target. However, similar to the industries that immediately come to mind like retail and financial services, the construction industry is actually more vulnerable to cyber threats.

Even before the COVID-19 pandemic, construction businesses were innovating digitally. Devices, information, vehicles and equipment were being connected to each other and the Internet. Construction businesses started collaborating online and integrating with cloud-based applications. This innovation accelerated during the pandemic and, with that acceleration, increased the threat landscape, leaving construction businesses internally and externally vulnerable.

Yes, Construction Risk is Real

While the most memorable data breaches involved large retailers or financial institutions, in 2021, the construction services industry was third-most attacked according to a Safety Detectives analysis of incidents caused by ransomware at 13.2% -- more than retail (7.5%) and financial institutions (4.6%).

But why are contractors such a tempting target for cybercriminals? It is because attackers like quick and easy targets, and as a whole, the construction industry

has not emphasized protecting its systems, data and privacy through its digital evolution. Construction businesses are more mobile now than ever, leaving them vulnerable to disruption and exposed to the theft of intellectual property and private data.

Examples include:

- Disrupting or delaying projects or services with a ransomware or malware attack
- Disclosing confidential bid information
- Stealing proprietary designs, blueprints, schematics or specifications

Cybercriminals can also cause property damage or harm by deleting data, altering plans or specifications, interfering with a project's security or safety systems or tampering with vehicles or equipment.

Keep an Eye on Your Supply Chain

As we have seen with the notable 2020 SolarWinds hack and 2021 Kaseya ransomware attack, critical third parties in your supply chain can be victimized and leave construction businesses at risk of being compromised or disrupted. In terms of disruption, cyberattacks on third parties could interfere with your ability to obtain fuel and key materials, negatively impacting project timelines. Third parties also could become a medium where cybercriminals can access your data or attack your networks, as was the case of both SolarWinds and Kaseya.

An example of supply chain disruption was the 2021 Colonial Pipeline ransomware attack. After being initially breached and having data stolen, the ransomware group encrypted Colonial Pipeline's data resulting in the pipeline being taken offline for five days. The shutdown of the pipeline affected consumers and airlines, as the pipeline is responsible for delivering refined oil for gasoline, jet fuel and home heating oil. It was only after Colonial paid the $5 million ransom to regain control of its systems and recover its systems from a backup that they were able to resume operations. Because of the threat of disruption and extortion, ransomware attacks like those on Colonial Pipeline are expected to increase.

According to Nick Weaver, a security researcher at UC Berkeley's International Computer Science Institute when asked about supply chain attacks:

"You're trusting every vendor whose code is on your machine, and you're trusting every vendor's vendor."

Understand Your Risk, Then Go from There

To better protect your company against cyberattacks, the best course of action is to have a cybersecurity assessment performed. Doing so will give you a point-in-time reference of where you are today with your security posture to identify any risks that can be remediated as you strengthen them. An assessment should take into account things like the inventory of your hardware and software, the topology of your network, policies and procedures, as well as any vulnerabilities that may exist within the devices that are connected to your network.

Ultimately, you want to identify every potential vulnerability or risk to your business. Most organizations that perform cybersecurity assessments should prioritize these risks and offer a remediation plan for addressing them. Armed with this information, you can then implement internal controls and protections to reduce the risk of a breach and develop an incident response plan to mitigate damages should one occur.

Four strategies for preventing cyberattacks, according to the Cybersecurity & Infrastructure Security Agency (CISA) include:

- Implement multi-factor authentication (MFA) on all your accounts if offered.
- Keep your software and hardware's firmware up to date. Turn on automatic updates, if able.
- Think before you click. Over 90% of successful cyber-attacks start with a phishing email. This includes being mindful of text messages on mobile devices.
- Use strong, complex and unique passwords for every account. Leverage password managers to generate and store them to avoid password reuse.

Stay Vigilant

Like most construction businesses, yours will likely increasingly evolve to rely on more mobile and Internet-based technologies. Be mindful that as the technologies evolve, the vulnerabilities and risk landscape do as well. Once you have completed an assessment and reduced risk by mitigating vulnerabilities and implementing controls, it's not the end of your cybersecurity journey. It should be the start of a cycle of risk assessment and remediation.

If you have concerns with your policies, data or privacy, our cyber experts can help you understand your risk areas and create a plan to mitigate your cyber risk.