CONSTRUCTION
INSIGHTS

LloydSadd

NAVACORD®

Ransomware Attacks in the Construction Industry

As the construction industry continues to increase its use of technology, the risks of cyberattacks also rise.

Furthermore, certain aspects of the construction industry make it vulnerable to attacks, such as the older systems still in use and the prevalence of inadequate cybersecurity systems. Even with robust prevention systems in place, businesses are susceptible to malicious cyber events. One particular area of concern is ransomware, which is malware that infiltrates a computer system through phishing emails, compromised credentials, malicious URLs, removable devices or other vulnerabilities. Once on a victim's device or network, this malicious software encrypts data and threatens to block access to it or publicly release it unless a ransom is paid to the cybercriminal. According to an analysis of ransomware cases between January 2022 and January 2023 by encryption software company Nordlocker, construction was the most targeted industry.

Ransomware Targets

Numerous types of ransomware threats could impact the construction industry, including:

- **Cloud vulnerabilities**—Cloud software and application can be susceptible to targeted cyberattacks. Individual devices or cloud accounts could be infiltrated through known weaknesses.
- **Targeted software supply chains and managed service providers**—Cybercriminals may target software supply chains and managed service providers to gain access to several organizations in one attack.
- **Interrupted industrial processes**—It's been reported that ransomware groups may have written malicious code to stop critical industrial and infrastructure processes.
- **Specifically timed attacks**—Cybercriminals may look to carry out ransomware attacks on weekends, holidays or other times when fewer IT personnel are available or working to stop it.

Ransomware Prevention

Being proactive and implementing extensive cybersecurity and risk management practices can help mitigate the risk of becoming a victim of a ransomware attack. Strategies to consider include installing updates and patches, providing comprehensive employee training, cautiously opening email attachments and using preventive software. Making sure to back up important data on separate devices can also help lessen a ransomware attack's impact.

If you have questions specific to your business, or would like additional information, please reach out to your Lloyd Sadd Advisor.

™®Local Touch. National Strength. Navacord and Navacord logo are Trademarks of Navacord. The information contained herein is general in nature and general insurance description only. The information is not intended to be insurance advice; nor does it amend, modify or supplement any insurance policy. Consult your actual policy or your broker for details regarding terms, conditions, coverage, exclusions, products, services and programs which may be available to you.

LET US HELP YOU MANAGE YOUR RISK

Edmonton: 1.800.665.5243
Calgary: 1.866.845.8330
Kelowna: 1.800.665.5243

lloydsadd.com
info@lloydsadd.com

Local Touch. National Strength.™