ALS THE ALS GROUP

Managing Risk to Influence Successful Outcomes

Construction Projects at Risk Because of Cyber Exposures

Authored by
Albert L. Sica

Are Your Construction Projects at Risk Because of Cyber Exposures?

The construction industry continues to evolve rapidly, with an increasing reliance on emerging technologies for equipment control, project management and completion. As projects become more digitally connected, there are significant concerns regarding the cybersecurity of "smart" equipment such as cranes and drones, as well as Software as a Service (SaaS) and Infrastructure as a Service (IaaS) systems (BIM software) used for project planning and management. Additionally, the utilization of interconnected systems by third parties, such as general contractors and subcontractors, to share and centralize sensitive data poses further cyber risks to projects.

While these technological advancements enhance project efficiency, they also introduce new exposures to the industry. Moreover, many construction companies still do not fully understand their cyber exposures or lack the means for adequate risk mitigation, placing projects in significant jeopardy.

Here are some cyber risks that construction companies should be aware of in 2024:

Business Interruption/Project Delays: A cyber breach resulting in the loss of sensitive information, intentional shutdown of systems, or disruptions in project timelines. Third-party outages, such as those from subcontractors, could also lead to significant delays.

Contingent Bodily Injury or Property Damage: Security breaches or system failures could result in physical harm or property damage. For instance, a hacked "smart" crane might cause damage to a building or pose risks to workers or civilians.

Contractual Penalties: Contracts may impose penalties for failure to deliver products on time due to cyber events.

Ransomware, Phishing, or Social Engineering: Threats such as ransomware attacks, phishing scams, or social engineering tactics aimed at stealing money or confidential information remain prevalent. These threats can originate from cybercriminals or malicious competitors.

As the owner of a large construction project, you should be acutely aware of the myriad cyber exposures that can impact your operations. In today's digital age, construction projects are increasingly reliant on sophisticated technologies and interconnected systems, which, while improving efficiency, also introduce significant vulnerabilities. One major concern is the potential for unauthorized access to project management systems and databases. Cyber attackers can exploit weaknesses in your network security to gain access to sensitive information such as project plans, financial records, and personal data of employees and contractors. Such breaches can lead to data theft, financial losses, and even sabotage of the construction process.

As a project owner managing multiple construction projects across various global locations, the risk of cyber exposures is exponentially magnified. Each project involves a complex web of stakeholders, including contractors, subcontractors, suppliers, and regulatory bodies, all of whom need access to shared digital platforms and sensitive data.

This interconnectedness increases the potential entry points for cyber attackers. The diversity of locations also means dealing with varying levels of cybersecurity maturity and regulatory requirements, making it challenging to maintain a consistent security posture across all projects. Furthermore, the reliance on different technology vendors and platforms for each project introduces additional risks, as vulnerabilities in one system could compromise others. The stakes are higher, as a cyber incident in one project can have cascading effects, potentially disrupting multiple projects simultaneously and causing significant financial and reputational damage.

To mitigate these risks, you must implement a multi-layered approach to cybersecurity. Firstly, ensure that all your digital systems are protected by robust firewalls and encryption technologies. This makes it significantly more challenging for unauthorized users to penetrate your network. Regular security audits and vulnerability assessments should be conducted to identify and address potential weak points in cyber infrastructure.

You need a robust incident response plan to ensure that we can quickly and effectively respond to any cyber incidents that do occur. This plan outlines clear procedures for isolating affected systems, communicating with stakeholders, and initiating recovery processes to minimize downtime and financial impact. Make sure you have comprehensive cyber insurance coverage to provide an additional layer of financial protection against the potential costs associated with cyberattacks. By taking these proactive measures, you can safeguard each construction project from the growing threat of cyber exposures and ensure its successful completion.

If you have any questions on cyber risk or security, or want to review your company's cyber threats, please contact Jon Edwards, Managing Director, at 732-395-4281 or jedwards@thealsgroup.com.