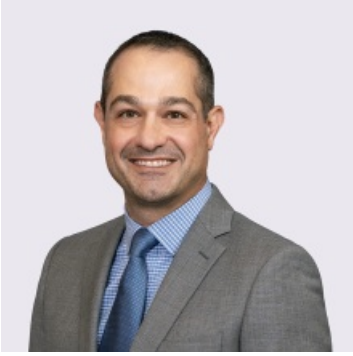
Legal Update Article

Construction Industry: Data Security Considerations

By Jason C. Gavejian & Joseph J. Lazzarotti

March 31, 2022

Meet the Authors



Jason C. Gavejian
Office Managing Principal
908-795-5139
Jason.Gavejian@jacksonlewis.com

Joseph J. Lazzarotti
Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Related Services

Construction
Privacy, Data and Cybersecurity

No industry is immune to privacy and cybersecurity risks, and the construction industry is no exception. Those in the construction industry can protect against a potential cyberattack by understanding the risks and vulnerabilities and developing a plan.

Ransomware costed businesses more than $20 billion in damages in 2021, according to Cybersecurity Ventures, and a study by Safety Detectives found that construction was the third most common industry to experience ransomware attacks in 2021 (13.2 percent of total ransomware attacks in North America).

The industry appeals to cyber attackers in many ways. First, the industry is largely unregulated when it comes to cybersecurity and privacy. This may explain why construction organizations have not prioritized implementing privacy and security measures. A study conducted by IBM Ponemon found that 74 percent of construction-related organizations are not prepared for cyberattacks and do not have an incident response plan in place.

Second, construction transactions contain *significant* amounts of personal information and sensitive business data, particularly regarding financial data, which entices threat actors.

Third, construction companies work with a variety of vendors, and each transaction may involve several parties, providing ample opportunity for an internal or external bad actor to wreak havoc.

Finally, in recent years, the construction industry has increasingly implemented artificial intelligence and robotics, which, given their interconnectivity, require additional data security and privacy considerations.

Understand Risks and Vulnerabilities

Not all construction organizations are faced with an equal amount of inherent business risk of a cyber breach. That would depend on factors such as the nature of the projects they work on (public infrastructure versus residential home builders), their customers (*e.g.,* governments, corporate, and individuals), the technologies involved in the project (*e.g.,* internet of things, drones, GPS, and biometrics), the jurisdictions in which business is conducted, and the amount and nature of the personal information and sensitive business data in the organization.

In addition, the level of risk can depend on how well an organization is prepared for the challenge. For example, members of the organization's IT staff may be adept at systems management, but are they up to speed on the latest cybersecurity tools and attack methodologies to provide competent leadership and execution?

Develop and Practice an "Incident Response Plan"

As an initial step, organizations can develop and practice an incident response plan before a breach occurs. A good start includes the following:

- Identify the internal response team (*e.g.,* leadership, IT, in-house counsel, and HR). These are the persons in the business who will direct the response to any data incident. They will make quick, informed, and prudent decisions that likely will be critical to the success of the response process and, possibly, the future of the business.
- Identify the external response team (*e.g.,* outside legal counsel, forensic investigators, notification vendors, and public relations). Having external members of the team identified ahead of time and negotiating and agreeing to any applicable contracts can be vital to the success of any preparedness plan. When a breach happens, valuable time can be lost trying to identify, evaluate, negotiate with, and engage third-party service providers necessary for the response.
- Anticipate critical business continuity and worksite safety issues that could be jeopardized by a compromise to information and control systems. To the extent possible, contingency plans should be laid out to enable operations to continue while investigating the incident and mitigating harm.
- Consult with insurance brokers or cyber-insurance carriers to confirm applicable coverage or to discuss coverage options for cyberattacks. If coverage exists, notifying the insurance carrier should be one of the organization's first steps in response to an incident.
- Take into account all legal and contractual obligations that may affect the response process.
- Clarify the roles and responsibilities of the team members at key points in the response process: discovering the incident, investigation, coordination with law enforcement, remediation, notification, third-party inquiries, compliance, and reevaluation. This should include a well-defined decision-making process to facilitate good choices and avoid delays.
- Practice, practice, practice. Members added to the response team likely do not have first-hand experience with helping to coordinate a data incident investigation or response. Unfortunately, even a well-drafted plan does not give persons charged with implementing the plan proficiency in executing it. Once the organization creates its plan, it should gather its internal and external breach response team members to simulate an incident to help members gain valuable experience navigating the investigation, mitigation, and overall response process, as well as working with each other. Just like a fire drill, practicing this process will help ensure any data incident is addressed in an efficient and orderly fashion.

Create Awareness Throughout the Organization

It is important that organizations create awareness of the risk of cyberattacks and of cybersecurity risks. This can include the following:

- Educate employees on how to recognize and avoid potential ransomware attacks and other forms of data breach.

- Instruct employees on what to do immediately if they believe an attack has occurred (*e.g.,* who to notify [generally, IT] and how to disconnect from the network). This may include coordinating with the organization's worksite safety team to ensure, for example, compromised systems and equipment do not cause physical harm to individuals or property damage.
- Instruct employees on what *not* to do (*e.g.,* delete system files and attempt to restore the system to an earlier date).

Preparedness can make all the difference in the success of a construction organization's ability to handle a cyberattack. An incident prevention and response plan is only as strong as employee awareness. Employees must understand the risks involved in maintaining complex data-driven systems and equipment and the basic steps they can take to prevent or mitigate a cyberattack and, if needed, respond to one.

Please contact a Jackson Lewis attorney with any questions.