Published on *The National Law Review* https://natlawreview.com

# Cybersecurity in the U.S. Construction Industry: Navigating Challenges and Strategies for a Secure Future – Part 2

Article By:

Sinan Pismisoglu

**Introduction**

In today's digital era, the construction industry faces a growing threat from cyber risks that can have significant impacts on projects and operations. As technology continues to revolutionize the industry, it is crucial for construction companies to prioritize the mitigation of these risks and safeguard their valuable assets, data, and infrastructure. Part 1 of this series outlined key cyber risks currently confronting the U.S. construction industry; Part 2 focuses on addressing those risks and their associated impact.

## Mitigating Cyber Risk

- **Cyber-Physical Systems (CPS) Security**

Cyber-Physical Systems (CPS) are revolutionizing the construction industry by promoting vertical integration, improving efficiency, and enhancing collaboration throughout the value chain. These systems integrate computational and physical processes, allowing them to sense, analyze, and control the physical environment. As a result, they have become increasingly prevalent in the construction sector, bringing substantial benefits to decision-making and overall project execution. Examples of such systems include smart grid and industrial control systems.

With the growing adoption of CPS, securing these systems is a critical challenge for the industry. To develop a comprehensive CPS security strategy, companies need to adopt a holistic approach that manages operational technology (OT), the Internet of Things (IoT), the industrial Internet of Things (IIoT), and IT security as part of a single coordinated effort. This integrated approach helps mitigate the growing risk of cyberattacks targeting CPS in OT environments, which may be exacerbated by faster 5G connectivity.

CPS are employed in various applications in the construction sector, such as automated construction equipment, remote monitoring and control of machinery, and building management systems. Ensuring the security of these systems is essential to protect valuable assets, maintain business continuity, and prevent potential disruptions to critical infrastructure projects.

- **Digital Identity and Privilege Access Management**

When various stakeholders collaborate on complex projects, a robust digital identity and privilege access management strategy is crucial. With the growing reliance on digital technologies and the increase in cyberattacks targeting critical infrastructure sectors, construction companies need to prioritize secure and efficient access management to protect sensitive data and resources.

Enhancing digital identity and access management involves implementing strong authentication and authorization protocols. This includes measures such as multi-factor authentication, single sign-on, and password management solutions. These protocols ensure that only authorized individuals can access sensitive project information and systems, reducing the risk of unauthorized access and data breaches.

Continuously monitoring and reviewing access rights is another vital aspect of a secure access management strategy in the construction industry. With various stakeholders involved in a construction project, including architects, engineers, contractors, and suppliers, tracking who has access to specific data and systems is crucial. Regular access rights reviews help identify potential vulnerabilities and ensure that access permissions align with each individual's job responsibilities.

Adopting role-based access control effectively manages access to sensitive information and resources in the construction sector. By granting privileges based on an individual's job responsibilities, the organization can ensure that only those who require access to specific data can obtain it. This approach reduces the risk of unauthorized access and enhances overall data security in construction projects.

- **Data Governance and Security**

Data classification is the main pillar of data governance. Prioritizing data classification and security is essential for the construction sector as it enables companies to protect their valuable project information, maintain a competitive edge, and reduce the risk of potential cyber threats.

The data classification process involves categorizing data based on sensitivity, helping organizations identify and prioritize protecting their most valuable and sensitive information. Data classification enables organizations to allocate resources effectively, ensuring that the highest levels of security are applied to the most critical data, such as project designs, cost estimates, and bid data.

Moreover, implementing robust security measures to protect sensitive information is essential in preventing data breaches, cyber espionage, and other forms of cyberattacks. Data security measures can include strong access controls, encryption, secure data storage, and regular security audits.

Proper data classification and security can provide a competitive advantage for construction companies. Organizations that demonstrate a strong commitment to data protection will be more attractive to clients and business partners who value the security of their project information. By protecting sensitive data, companies can minimize the risk of losing their competitive edge due to intellectual property theft or compromised bid data.

- **Enhanced Secure Backups and Network Segmentation**

The construction industry rapidly embraces digital technologies such as Building Information Modeling (BIM) and digital twins to streamline project management, design, and collaboration. With this shift, ensuring data integrity and availability is vital to successfully completing construction projects and ongoing operations.

Network segmentation is particularly relevant to the construction sector, as it often involves working with numerous stakeholders, including contractors, suppliers, and architects, each requiring different levels of access to sensitive information. By dividing its network into smaller, isolated segments, the organization can restrict unauthorized access and limit the potential spread of cyber threats among project teams and partners.

Moreover, it is crucial to establish secure backup environments for the organization's project data, whether on-site or through a cloud-based solution. Regularly testing the backup strategy ensures successful data restoration in a cyberattack, minimizing downtime and data loss, which can otherwise lead to costly delays and disruptions.

- **Third-Party Risks**

Reliance on external partners, such as subcontractors, suppliers, and service providers, is common in the construction industry. This reliance, however, creates potential vulnerabilities that can expose construction companies to various cyber risks.

To mitigate third-party risks, it is crucial to establish cybersecurity requirements within contracts and perform comprehensive vendor risk assessments. Collaboration with external partners to enhance their cybersecurity posture is vital, as their security practices directly impact the overall security of construction projects.

Additionally, organizations may consider establishing clear policies and protocols for granting and monitoring access to external partners. This includes setting up role-based access controls to ensure that vendor and subcontractor access is limited to the minimum necessary for performing their tasks. Closely monitoring the activities of external partners can help detect potential security issues and prevent unauthorized access to sensitive data and systems.



National Law Review, Volume XIII, Number 176