

Safeguarding Data for Fleets in Construction

Written by: Robert Nawy, CEO, IPKeys Cyber Partners

HOW TO BUILD A CYBERSECURITY PROGRAM TO KEEP YOUR EQUIPMENT COVERED

Data security is of paramount importance to fleets – even the smallest data breach could lead to a company's loss in revenue and customers, as well as a potential hit on its reputation. As the fleet industry continues to focus on digital transformation initiatives, management has become more concerned with data security because many companies still have outdated information technology (IT) infrastructure that lacks modern tech safeguards. In regard to construction fleets, employees accessing company information through various networks – along with vendors and subcontractors accessing certain systems and data – create many susceptible points of infiltration for cybercriminals.

The increased adoption of telematics devices has also transformed fleets into mobile data factories. While it is vital that fleet operations have the ability for information to flow freely, there must also be stability when balancing openness and the protection of sensitive data. Newer vehicles utilize some of the most complex and connected technology – making them vulnerable to hackers. Some hackers can control nearly every function of a vehicle, including engine performance, braking systems, airbag deployment, power steering, windshield wiper functionality, and security features.

New forms of tech provide numerous benefits to fleets and are becoming more of the standard, as the tech can



reduce accidents while allowing fleet managers to prioritize operations and fulfillment. While many features improve safety, efficiency, and convenience, the evolution of digitized technology in fleet vehicles essentially makes them a moving target for cyberattacks if not properly secured. Fleet companies can minimize threats by implementing a robust cybersecurity infrastructure that will protect all their confidential data and avoid exposing even the most minor vulnerability.

Construction Fleet Cybersecurity

Compared with other sectors that are late to the adoption of tech solutions, construction is under a greater threat, with

lower historic investment in security infrastructure and a workforce that needs upskilling in using tools effectively and safely.

Construction is also vulnerable because of the way the industry has historically worked. Many contractors still rely on paper documents and drawings for their everyday tasks when managing different projects. By adopting tech solutions such as data analytics, companies can reduce their direct labor costs and avoid unexpected claims and other costs.

Through the adoption of technology, the sector has become richer with data along with organizations seeking to educate themselves on what can be done to protect themselves.

The team charged with building a construction cybersecurity program will identify first the laws that apply to the organization and IT standards it wishes to follow, along with other guiding principles.


With robust cyber protection, managed cybersecurity solutions reduce costs while enhancing the ability to maintain security policies. From the initial stages of implementing a cybersecurity service, the tech can accept software source code in a secure lab for analysis during a company's software development cycle. It resolves security issues through the design of safety systems and information, rather than executing fixes after product releases.

Additionally, while keeping a company informed of its system's defensive stance, it is also deployed on-site to ensure the protection of a company's systems and information.

Managers can safeguard their fleets by arming them with the necessary protections to eliminate vulnerabilities for the foreseeable future. Through the implementation of a third-party managed cybersecurity service, managers can ensure all the cyber doors are locked and gain second-by-second monitoring capabilities. The tech supports IT personnel, essentially giving them eyes on any potential vulnerabilities so they can address them long before they are discovered or penetrated by cyberattackers. The tech also provides any necessary training and education that can help team members avoid the risk of displaying valuable data, as well as ensure they are adapting to companywide best practices.

Navigating Future Risks

Unfortunately, organizations in almost every industry are navigating cyber threats, and the construction industry is no exception.

There are, however, a number of risk mitigation strategies – the first step is to find experienced advisers to help navigate this complex legal and technical terrain. 



About the Author

Robert Nawy is CEO of [IPKeys Cyber Partners](#), a provider of an industry-leading, secure operational technology (OT) and information technology (IT) intelligence platform that addresses the complex cybersecurity, data and critical infrastructure protection challenges faced by operators of mission-critical networks for customers in the energy, government and public safety communications, and industrial markets.

About the Article

Republished from [Construction Business Owner](#). Construction Business Owner (CBO) is the leading business magazine for contractors and is designed to help owners of construction firms run successful businesses. Founded in 2004, CBO provides real-world business management education and knowledge that is of real value to the owners of construction companies.

Any views and opinions expressed in this article may or may not reflect the views and opinions of the Construction Management Association of America (CMAA). By publishing this piece, CMAA is not expressing endorsement of the individual, the article, or their association, organization, or company.