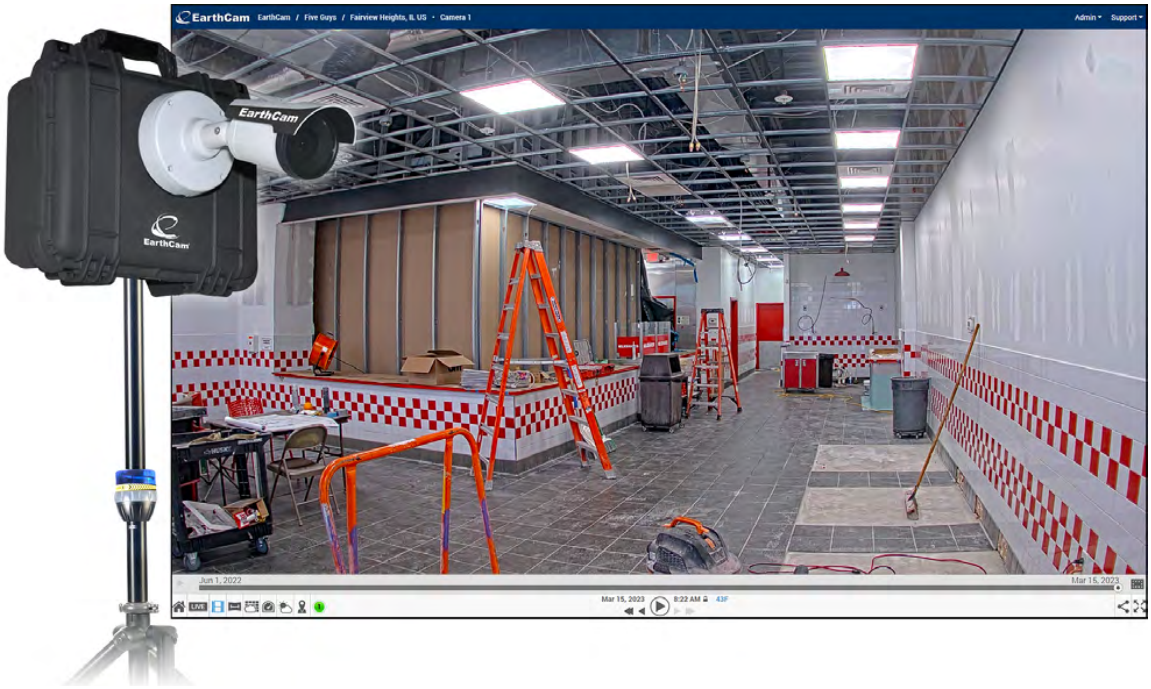
FOR Construction PROS.com

Surprising Ways Contractors Can Use Technology for Theft Prevention

By Charles Rathmann, *June 19, 2023*



Construction contractors have enough to worry about without unplanned losses due to criminal theft. Equipment in the field is just one exposure contractors have to theft, so the traceability, visibility and control offered by modern digital technologies can mitigate risk regardless of the whether losses come in the form of equipment or cash.

Geolocation

Knowing where equipment and tools are and who they are issued to is perhaps the most common way construction technology is preventing theft in the field today. GPS Asset Tracking Hardware topped the list of technologies contractors were using, budgeting or planning for in the 2023 State of the Industry Construction Technology Report.

Some slap-and-track hardware paired with a software application with geofencing can ensure equipment stays where it is supposed to and often if the equipment is started apart from approved operating hours. Most of this software extends well beyond location tracking, to maintenance, parts, work order management, scheduling or even job ticketing and productivity reporting.

“There is so much value in centralized all my data in one place,” Fleetio Vice President of Customer Experience Trey Hoffman said. “Apart from location, you can track who last had this equipment—further combating theft—not only of the piece of equipment itself but the tools linked to a vehicle or piece of equipment.”

In an increasing number of cases, this type of tracking does not even require the contractor to purchase telematics hardware as it is increasingly being installed at the factory. This is driven in part by the demands of large fleet owners.

Officials with Trackunit said OEMs are becoming more aggressive in including and exposing geolocation technology in their products as a standard feature. Major rental companies are one OEM customer demographic pushing for this, and smaller rental companies also find immediate value. The rental companies’ contractor customers are also increasingly making geolocation a factor in their rental decisions.

Construction Video Telematics

Fleet and construction equipment managers may think of video telematics including forward- and rear-looking dash cams as tools to mitigate safety risk or reconstruct events around a safety incident. While video telematics is now considered table stakes in connected asset management software, some of the technology is running ahead in terms of theft prevention capabilities.

Launched in 2021, T3 is billed as an operating system for construction, and expands EquipmentShare's remit beyond equipment management of rental and owned equipment to broader management of assets, people and materials in a construction setting. The application ingests equipment telematics data, data from its own timecard application, mobile expense capture and inventory modules. In January of 2023 the company added their dash cam offering.

"Here with T3, we have a pretty big forestry company that requested from us some cameras we can stick in their equipment," Equipmentshare Senior Director of T3 Sales Kristopher Dunn said. "They need to access them remotely to gather data, and rather than watch five hours of footage, create time lapse so they can see forests being cleared. As logs loaded on the truck, they needed to be able to prove that progression. As a byproduct of the fact they are in logging, they always have vandalism and theft issues."

Dunn said they and their customer found there were limitations to GPS in preventing theft.

"They need to leave this equipment on logging road, whether it is kids or some other group, GPS is great at recovering the asset but you never catch the person—so GPS is not really a deterrent," Dunn said. "Now we have very clear infrared video."

Fixed security cameras for use in interior builds as well as on job sites is also advancing. Earthcam in April launched its IoT StreamCam 4k for indoor job sites, which offers 365 days of encrypted digital recording. The company also released an AI safety trailer for mobile security. Based on camera and sensor data, the trailer creates alerts by flagging security, vandalism and theft events. AI Object Detection recognizes specific vehicle types, or unauthorized interactions with equipment or vehicles.

Office-Based Theft Risk

Reducing equipment and tools lost in the field is only one way technology can help contractors reduce shrinkage caused by theft. Risk of theft using digital means was one of the issues raised on an Association of Equipment Manufacturers at the IGNITE 2022 Construction Summit.

"Spending on security has increased 188% between 2018-2019, and has likely only increased more since the pandemic," Asphalt Contractor Editor Brandon Noel wrote.

"The reputation of firms in this industry is largely built upon on-time service delivery, which is at risk during any delays caused by ransomware attacks," Nordlocker cybersecurity expert Oliver Noble said. "This factor, together with the industry's razor-thin profit margins, provides the ransomware groups with conditions that make a payout more likely. Additionally, the industry could be a tempting target to ransomware gangs because of its relatively traditional business model, which is to a large degree yet to implement advanced cybersecurity solutions."

While construction, in some studies like this one from Nordlocker, may be the number one target for ransomware attacks, these attacks are only the tip of the iceberg, and represent a small fraction of the risk contractors are exposed to from theft.

The "Three Risks Lurking in Your Construction Accounting Software" IRONPROS research paper explains how, in the early days of business software moving to the cloud, the supposition was that moving mission-critical data and processed outside the four walls of the business would create security risk. Yet on-premise solutions are highly vulnerable and one reason construction is the number one target for ransomware attacks. Applications enable remote administration of on-premise systems like ConnectWise and Kaseya have been used to install ransomware on on-premise software systems. These software products are also often updated infrequently, and if a contractor stops paying for updates, choosing to run indefinitely on an old version, malicious actors have plenty of time to figure out and exploit vulnerabilities across a large installed user base with identical vulnerabilities.

According to John Meibers, vice president and general manager at Deltek and ComputerEase, contractors running software on-premise can get help protecting their instance of software as well as ensuring they can recover quickly if they are hit by ransomware or other types of malicious acts.

"The best defense is a reliable, easy-to-restore backup," Meibers said. "If the hackers get in, if I don't need the data, I don't have to pay."

Contractors may also be vulnerable thanks to security holes in open source technologies they use in their business. Software licensed under the Open Source Initiative (OSI) enables a software developer to use it while disclosing what these licensed components are to their own buyers. The community of users collaborate to identify potential exploits and share patches, but this information can also be used illicitly to attack systems left unpatched.

Which technologies are we talking about? Argo, a tool used to manage containers in a cloud environment, e-commerce tool Magento, now Adobe Commerce, the ElasticSearch Database, MySQL, Linux operating system, MongoDB, the Redis in-memory data structure store and others have all been hit—plus many others. It will make sense for contractors to ask potential software vendors about the technologies inside the product and how often they are patched.

Contractors Defrauded From Within

Keeping external hands off of private data and monies is hard enough. But the dynamic nature of project-related expenditures and subcontracts can obscure a number of common embezzlement schemes run by employees.

From simple schemes like employees illicitly writing checks to themselves to pay rate fraud or buddy punching, dishonest behavior can thrive without the preventive controls to stop it from happening and the detective controls to prove later who did what and when. More contractors are effectively implementing business software designed for construction. Enterprise software enforces consistent processes and provides those preventive and detective controls.

According to the Construction Labor Market Analyzer 20% and 40% of the cost of a total project budget percent of the cost of construction consists of staffing, so implementing cloud timeclock or human capital management software can close some of these internal value leaks.

“The trick is to get what you are paying for using tight payroll controls to know how workers are spending their time,” FCP Columnist Garry Bartecki wrote. “Use fingerprint or face ID time clocks, accessible via mobile devices, for time tracking to eliminate buddy punching and other potential forms of timesheet fraud.”

Human resources software can also help contractors stop pay rate fraud, where someone with access to payroll grants another employee an unauthorized raise, and fraud perpetrated by supervisors skimming from their employees’ payroll.

Protections in software like enterprise resource planning (ERP), accounting and procurement can also segregate duties so the same person cannot, for instance, create a new vendor in the system, issue a purchase order to that vendor, approve the purchase order and take delivery on the order.

In both ERP and best-of-breed procurement tools though, it is still largely up to the contractor or user organization to configure these controls to deliver on the roles and segregation of duties they decide on.

“You could certainly build those business rules in the platform” PaperTrl President & CEO Steve Weber said. Launched in 2018, Papertrl delivers integrated cloud-based accounts payable automation. “We have decoupled the rules engine from the objects. So where you want to create an automation, when a bill is created for instance, here are the steps you can go through for the required approval to happen. The software can also notify a given person when, for instance, a vendor has been created.”

But Weber pointed out how modern, centralized and traceable procurement workflows are just more resistant to scams, both internal and external.

“We do help with phishing attacks,” Weber said. “We see them in our customer base—it may be something as something as a fraudulent request to change direct deposit information for a vendor. But we have a portal where vendors can do things like that. If you do everything with our vendors inside our portal, that eliminates a lot of problems.”