BASSFORD REMELE

DIGITAL RISK AND THE CONSTRUCTION CONTRACT: A GAP THE INDUSTRY HAS NOT FULLY ADDRESSED

Kyle S. Willems
Bassford Remele, P.A.

Introduction

Construction projects today run on digital infrastructure. Schedules, drawings, pay applications, change orders, and payments all move through cloud-based platforms and electronic systems. That shift has been underway for years and is now effectively complete on most medium and large projects.

The contracts governing those projects have not kept pace. Almost all construction contracts were built around a pre-digital model of project management and project risk. They address delays, defects, disputes, and cost overruns. They say very little about the risks that come with running a project through connected digital systems.

There is significant room for improvement. A fully modernized construction contract might address artificial intelligence use and data ownership, cybersecurity standards, cyber liability insurance, digital document authentication, and data retention and destruction obligations, among other things. That is a longer conversation. This article focuses on three issues that come up often in practice and that carry the most immediate financial and legal exposure.

The first is the theft of intellectual property and proprietary project data through improperly secured shared platforms. The second is payment fraud, most commonly through business email compromise, which has cost the industry billions. The third is the security vulnerability created when a party with access to shared project systems lacks the practices or awareness to protect that access. Each is addressable through targeted contract language. None are routinely addressed in construction agreements today.

Intellectual Property and the Vulnerability of Shared Project Data

Large construction projects generate substantial amounts of proprietary information. Building Information Models, engineering specifications, design files, proprietary construction methods, and client data collectively represent significant intellectual and commercial value. Access to that information is routinely extended to dozens of parties (i.e., subcontractors, vendors, and consultants) as a practical necessity of project coordination.

Standard confidentiality provisions do not adequately protect that information. They establish an obligation to maintain confidentiality but impose no requirements on how. They do not specify security standards, restrict internal access within a subcontractor's organization, or address the

termination of platform credentials when a party's scope of work is complete. A subcontractor that finishes its work in month four of a twenty-month project may retain active platform access through project completion unless someone manually revokes it. Few contracts require that anyone do so.

The threat is not limited to external actors. Competitors have obtained proprietary design files through improperly secured platforms. State-sponsored groups target infrastructure project data specifically for its engineering content. Internal threats, such as a departing employee, a disgruntled subcontractor, represent meaningful exposure as well. In each case, the contract as typically drafted offers little basis for accountability after the fact.

Effective contract language should define the scope of confidential information, require two-step authentication that can be activated and deactivated by the owner and/or general contractor, limit platform access to personnel with a genuine need, require credential deactivation upon completion of each party's scope, and establish clear consequences for breach. These are not novel legal concepts. They are standard in technology and finance sectors. They are largely absent from construction contracts.

Payment Fraud and the Business Email Compromise Problem

Business email compromise is among the most financially damaging forms of cybercrime targeting the construction industry. The mechanism is straightforward. An attacker either gains access to a legitimate email account or creates one designed to appear identical to a known address. Using that access, the attacker intercepts or initiates a payment-related communication—typically a request to update banking or wire transfer information. Then, the bad actor redirects funds to an account under their control.

Construction contracts rarely address this. There is no standard requirement that parties use multi-factor authentication to access payment systems. There is no protocol for independently verifying changes to banking information before a transfer is made. There is no provision allocating liability when a payment is misdirected due to one party's failure to maintain reasonable security practices. The contractual fix is not complex. Requiring multi-factor authentication for any platform used to approve or transmit payments is a reasonable baseline. A verification protocol, such as a provision requiring that any change to payment instructions be confirmed through a separate, independent channel before it is acted upon, would prevent most of these frauds from succeeding. These are just two examples that, if implemented, could reduce the billions in cyber crime impacting the construction industry annually.

Third-Party Access and the Security of the Broader Project Network

A shared digital project environment is only as secure as the least secure party with access to it. That is not a theoretical concern. It is the defining feature of how construction projects operate digitally, and it is the risk that standard contracts are least equipped to address.

A general contractor may maintain strong internal security practices: enforced password policies, encrypted systems, logged access, and active monitoring. Those measures offer limited protection

when a subcontractor with equivalent platform access maintains none of them. Attackers have learned this. Documented incidents show attackers deliberately targeting smaller subcontractors not for their own data, but as access points into the systems of larger contractors and project owners. The path of least resistance runs through the party least likely to have thought about cybersecurity.

The practical consequences are significant. Consider a mechanical subcontractor on a hospital project with full access to the project's cloud platform. The company performs quality work. But no one on the team has considered data security, and nothing in their subcontract required them to. Employees share login credentials for convenience. Passwords are simple and unchanged. Multi-factor authentication has not been enabled. When an attacker compromises one of those accounts, the exposure is not limited to the subcontractor's own data. The attacker now has access to the hospital's floor plans, security and utility infrastructure layouts, and the project's complete payment schedule -- information with value far beyond that subcontractor's scope of work, and with implications that extend to the building's future occupants.

That outcome is difficult to prevent under current contracting practices because smaller subcontractors are typically selected for their trade expertise, not their security posture. Cybersecurity has not historically been part of that evaluation, and the subcontract has not historically made it one.

Contracts can change that. Requiring all parties with platform access to meet a defined security baseline is a proportionate response to a documented risk. At a minimum, that baseline should include multi-factor authentication, maintained security software, and a designated point of contact for access management. For projects involving sensitive client data, significant intellectual property, or high-volume electronic payments, requiring cyber hygiene training and written confirmation of cyber policies compliance, and evidence of cyber liability insurance, is a reasonable and enforceable condition. The specific requirements will vary by project. The principle should not.

Conclusion

The construction industry has adapted its operations to a digital environment without adapting its contracts to match. The result is a meaningful and largely unaddressed category of legal and financial exposure that sits across every project involving shared platforms, electronic payments, or digitally stored project data.

Addressing it does not require rebuilding standard agreements from the ground up. It requires adding provisions that reflect current project realities: how data is shared, how payments move, and what security obligations each party should be expected to meet. The appropriate scope of those provisions will depend on the nature and scale of the project. A straightforward commercial build with a small subcontractor list calls for different protections than a hospital, data center, or large public infrastructure project.

What every project calls for is a contract that acknowledges the digital environment in which it operates. Most do not. That is worth changing.

About the Author

Kyle Willems is a shareholder and member of the board of directors at the law firm Bassford Remele, P.A. Kyle is also the co-chair of the firm's construction and real estate practice group, and has significant experience litigating construction and real estate matters. Kyle is licensed in Minnesota and Wisconsin. kwillems@bassford.com, 612.376.1604.

DISCLAIMER: THIS ARTICLE IS NOT INTENDED TO BE RELIED UPON AS LEGAL ADVICE. THERE IS NO ATTORNEY-CLIENT RELATIONSHIP BETWEEN BASSFORD REMELE, P.A. AND ANY READER OF THIS ARTICLE.

6/12/2026