

## Digital Threats Lurk Around Every Corner. Do You Know How to Stay Safe?

Written by: Brian J. Schnese, who works in Regulatory Compliance and Risk Management

For the construction industry – long plagued by lagging productivity – the growing availability and accelerating adoption of technology have been hugely beneficial.

In fact, improved productivity has been only one of the advantages. Construction’s tech-driven transformation has been marked by improved safety, better collaboration and communication, cost reductions, smarter and more efficient operations and services, and more cost-effective and sustainable construction practices.

But there has been a distinct downside, too. The digital evolution has left construction firms more vulnerable than ever to cybercrime.

The risk of financial losses is just the tip of the iceberg. This means direct losses stemming from theft, fraud, or ransom payments, as well as costs required to deal with and recover from an attack, such as legal fees or remediation. But cyberattacks can also delay and disrupt projects and supply chains, creating financial and reputational havoc. And that reputational damage can have long-term impact on a business’s fortunes.

Mitigating the risk requires an organization-wide focus on the worsening problem, backed by a detailed strategy to guard against the risk and respond fast should a breach occur. Here’s what construction firm owners and their teams need to know.



### PREPAREDNESS — OR LACK THEREOF — IS A BIG ISSUE

Many construction firms aren’t well equipped to protect themselves adequately from cyberattacks. They’ve become vulnerable for several reasons.

One issue is lack of preparedness. Nearly three-fourths of firms haven’t prioritized cybersecurity, according to IBM. The result? Construction/real estate was the No. 1 sector breached by bad actors in 2023, with 1.5 billion records compromised, IT Governance USA reported.

Greater use of technology by the industry also has made for a bigger target. The benefits of robotics, Internet of Things (IoT) systems, machine intelligence, and drones are inescapable, but

all are vulnerable to breaches. Cybersecurity assessments and protective measures become critical.

Further, construction has become an increasingly complex network of interconnected firms and trade partners, material suppliers and vendors, and other parties. This creates third-party connections tying into different technologies, making for integration challenges and cyber exposures. Safety Detectives reported that construction-related firms have the third-most ransomware attacks in North America, so it has become critical for firms to stay on top of the cybersecurity practices of their third-party partners.

Another vulnerability of construction firms is in their practice of storing massive amounts of personal and sensitive business data. This can span proprietary information to intellectual property and company/client financials to corporate bank accounts. All are valuable targets prized by cybercriminals.

### THREATS CONSTRUCTION FIRMS SHOULD WORRY ABOUT

Any type of cyberattack can harm a construction firm, but the three most common and concerning are listed below:

- » **Ransomware attacks:** Ransomware is part of a one-two attack by cybercriminals. The first step is a phishing attack – using fake emails and messages to trick employees into an action like downloading malicious software. Once in the system, that malware encrypts files; they're held for ransom until payment is made to release them. Given construction's heavy reliance on project deadlines and data accessibility, this can be costly, beyond the financial payments. The disruption can delay work and cause cost overruns and quality problems. Plus, potential exposure of business information can also put vendors and clients at risk. There may be an added cost of financial penalties or lawsuits over missed deadlines.
- » **Data theft:** By whatever means it is stolen – say ransomware or social engineering schemes – data theft is a significant issue for the construction industry. Firms often manage confidential intellectual property like design documents, patents, and bid strategies that cybercriminals target. Also at risk, though, is social security and credit card information, along with personal information of employees, vendors, and customers.


- » **Fraudulent funds transfer:** Substantial funds are transferred via online banking between construction firms and business, customer, and vendor accounts. These make for another attractive target for cybercriminals who use emails (like social engineering) or phone calls, preying on human psychology to trick a response from victims. It takes training and awareness for people to avoid becoming victims of these scams.

### HOW TO GUARD AGAINST THE RISKS

Managers and employees alike become knowledgeable of the types and nature of cybercrimes most common to construction firms. Education, planning, and prevention – with ownership and management of these responsibilities assigned to a specific team member – will minimize digital risks and establish a culture of security. Efforts should include the following:

- » **Conduct a comprehensive risk assessment.** This is important for identifying and prioritizing the firm's particular vulnerabilities and ensuring sufficient safeguards are in place.
- » **Establish a cybersecurity training program.** The number of scams that can come through unaware employees makes training essential, including refreshers and updates as new types of criminal intrusions emerge. Training should cover how confidential information should be handled and cyberthreats identified. A multistep process should be instituted, and training provided, for confirming changes to vendor and/or client bank routing. A process for reporting questionable cyberactivity, like suspicious links, is also key.
- » **Good cyber hygiene counts.** Fundamental cyber-hygiene practices should be emphasized. One starting point is multifactor authentication, providing an extra security layer for accessing sensitive information – think bank accounts, invoices, and legal documents. This is essential for email, the corporate network, privileged system administration accounts, and accessing system backups. Strong passwords, regular software updates (including antivirus programs), and properly configured firewalls are also important.
- » **Guard against external exposures.** Many breaches are a function of lax practices by outside partners – software services, trade partners, or vendors and suppliers. These risks should be evaluated and contractual relationships

reviewed to ensure their cybersecurity practices are up to snuff.

- » **Form a response plan.** An incident response plan will enable a swift mobilization if a cyberattack occurs. Have experts lined up and ready to help – IT, incident response teams, insurance brokers, and breach response counsel. Knowing what not to do will also help mitigate the damage.
- » **The right insurance matters.** Cyberinsurance has never been more important. What's key, though, is to use the services of insurance professionals who specialize in the construction industry and understand the cyber-coverage particulars that apply to it. 



---

### About the Author

---

Brian J. Schnese has over 15 years of professional experience in regulatory compliance and managing risk in state and federal government agencies, as well as private industry operations including retail, supply chain, transportation, health care, and the financial industry.

---

### 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.