

Member Communication Experience

Improving Cyber Defenses in the Construction Industry

Written by: Ryan Bell, Senior Manager of Threat Intelligence Research, Corvus Insurance

It's a list no industry hopes to lead. Construction remained the most-plagued sector for publicly disclosed global ransomware attacks in Q3 2024 with a 7.8% increase over Q2 and a 35% increase for the year so far, according to the Corvus Insurance Q3 Cyber Threat Report.

Cyberattacks have proliferated across the construction supply chain – from attacks on large U.S. construction giants to small trade partners. Construction is an industry where one company in the supply chain being shut down for a few days can mean significant disruptions elsewhere.

What are the drivers behind this uptick in ransomware attacks in the sector? Ironically, the strategies and tools meant to modernize and digitally transform construction companies and their suppliers have opened doors for cybercriminals. It's important for companies to be aware of commonly used attack methods and implement security controls to help mitigate these risks.

REMOTE WORK AND AUTOMATION: UNLOCKING EFFICIENCIES WHILE EXPANDING CYBER RISKS

The adoption of automation and remote work is transforming many industries by delivering efficiencies, cost savings, and productivity gains. As manual, paper-based processes give way to digital systems and automation, companies benefit from streamlined operations and improved supply chain management.

For example, organizations are embracing:



- » **Operational technologies:** Tools like supervisory control and data acquisition (SCADA) systems, building information modeling (BIM) software, machine learning, and robotics are improving processes and decision-making.
- » **Internet of Things (IoT) devices:** Connected sensors, drones, and wearable technology enable real-time data sharing from jobsites to headquarters and suppliers, increasing transparency and responsiveness.
- » **Digitized supply chains:** Information is shared across an extended network of suppliers, contractors, and third-party vendors, facilitating collaboration and efficiency.

However, these same innovations create vulnerabilities. Every connected device, system, or third-party integration in the supply chain represents a potential entry point for

cybercriminals. The rise of remote work has further expanded these risks, as employees access critical systems and data from less secure personal devices. Even tools and software designed to promote secure remote access can have their own vulnerabilities and weaknesses, providing another avenue for attackers. This shift has widened the attack surface, making businesses more susceptible to breaches, ransomware attacks, and data theft.

Ransomware groups tend to target industries with complex and fragmented supply chains, exploiting their many vulnerabilities. Construction firms and contractors are especially at risk, as they often overlook the full extent of their cyber exposure. Without a comprehensive approach to security, including the risks introduced by remote work, these organizations may leave themselves open to costly and disruptive attacks.

To thrive in the digital age, businesses must balance the benefits of automation and remote work with robust cybersecurity measures that address evolving threats.

THE STAKES ARE HIGH

The consequences of a cyberattack can be particularly severe for construction firms due to the nature of the large, complex supply chain and the amount of data and sensitive information being collected and shared electronically, such as financial accounts, business-sensitive data, and intellectual property. A breach or attack can lead to significant financial losses, as well as compliance or even safety risks. Ransom demands and payments continue to climb, with the average payment in excess of \$600,000. Cyberattacks can also lead to reputational damage, with data breaches often impacting customer trust and brand loyalty.

LACK OF READINESS DESPITE HEIGHTENED CYBER CONCERNS

The 2024 Travelers Risk Index reveals an unprecedented level of concern surrounding cyber threats across all sectors. For the fourth time in six years, cyber threats ranked as the top concern for survey participants. A record high percentage of survey participants, 62%, said they worry some or a great deal about cyber risks.

The index further breaks down industry-specific responses.

Business leaders in construction cited the following as their top cyber concerns:

1. Unauthorized access to financial accounts
2. Failure to operate the company due to cyber events
3. Security breach/hackers

However, the concern does not yet equate to cyber readiness. Eighty percent of survey respondents from the construction industry believe having proper cybersecurity controls in place is critical, yet:

- » 70% do not use endpoint detection and response (EDR) tools
- » 70% do not have a post-breach team on retainer
- » 56% do not have a written incident response (IR) plan
- » 50% lack cyber insurance
- » 45% do not use multifactor authentication (MFA) for remote access


HOW TO BUILD BETTER CYBER RESILIENCE

The silver lining of heightened cyber threat awareness is that companies recognize the need for better cyber resilience. The next steps are implementing appropriate security controls:

- » **Implement multi-factor authentication (MFA):** Prevention is the best defense. MFA, which requires the use of two or more authentication factors to verify the legitimacy of account access attempts, can make you 99.2% less likely to be hacked according to the Microsoft Digital Defense Report 2023. MFA should be required for all users to help prevent cybercriminals from accessing a business' system or infiltrating a network.
- » **Keep systems up to date:** Maintaining awareness and control of your IT assets is key to cyber resilience. Keep systems up to date — an unpatched vulnerability is one of the easiest and most common methods used to compromise a computer system or network. Enable automatic updates where possible, replace unsupported systems, and test and deploy available patches quickly.
- » **Have an EDR solution in place:** EDR offers protection against malicious attacks and can provide far greater capabilities than a traditional antivirus solution. EDR can help protect and monitor every asset in an enterprise network by identifying suspicious activity before the rest of

the corporate network is exposed to unnecessary risk. EDR technologies monitor anomalous behavior on each system rather than simply searching for malware.

- » **Back up your data:** Employ regular, thorough backup practices. Make copies of important data and system configurations and protect them. Businesses and organizations typically store many kinds of data, using a variety of computer systems, on networks that may be local, global, or somewhere in between. Data on a system or network can include protected health information (PHI), payment card information (PCI), personally identifiable Information (PII), intellectual property, or other proprietary or confidential information – this data must be backed up and protected.
- » **Have a written incident response (IR) plan:** The goal of an IR plan is to provide a clearly defined, focused, and coordinated approach to responding to cyber incidents. These plans enable organizations to be proactive to a threat, limit the damage, and hasten a return to normal. Getting back to business with limited impact after an attack is one benefit of having an IR plan in place. An IR plan also shows your partners, suppliers, and clients that you take cybersecurity seriously.
- » **Conduct security awareness training:** Employees are the first line of defense against cyberattacks. Regular security awareness training is vital in building better cyber resilience. By incorporating phishing simulations, promoting strong security best practices, and establishing clear incident reporting protocols, companies can significantly reduce the risk of security breaches. Empower employees to act as a line of defense and ensure that any potential issues are identified and mitigated early. Security is a shared responsibility, and with the right training and support, employees can be the strongest assets in protecting an organization from cyber threats.

Cyber threats are top of mind for business leaders throughout the construction supply chain, and ransomware attacks don't show any signs of slowing. But with proper planning and giving priority to putting the right security controls in place, companies can build cyber resilience. 



About the Author

Ryan Bell is the senior manager of threat intelligence research for [Corvus Insurance](#).

About the Article

This article is republished from [For Construction Pros](#). [For Construction Pros.com](#) is one of the largest construction networks in North America, providing the insights, trends, and best practices for those in the construction industry. A contractor's whole-business resource, For Construction Pros analyzes today's news, reviews new construction equipment and methods, and offers business management advice with one goal: to help construction contractors turn better profits.

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.