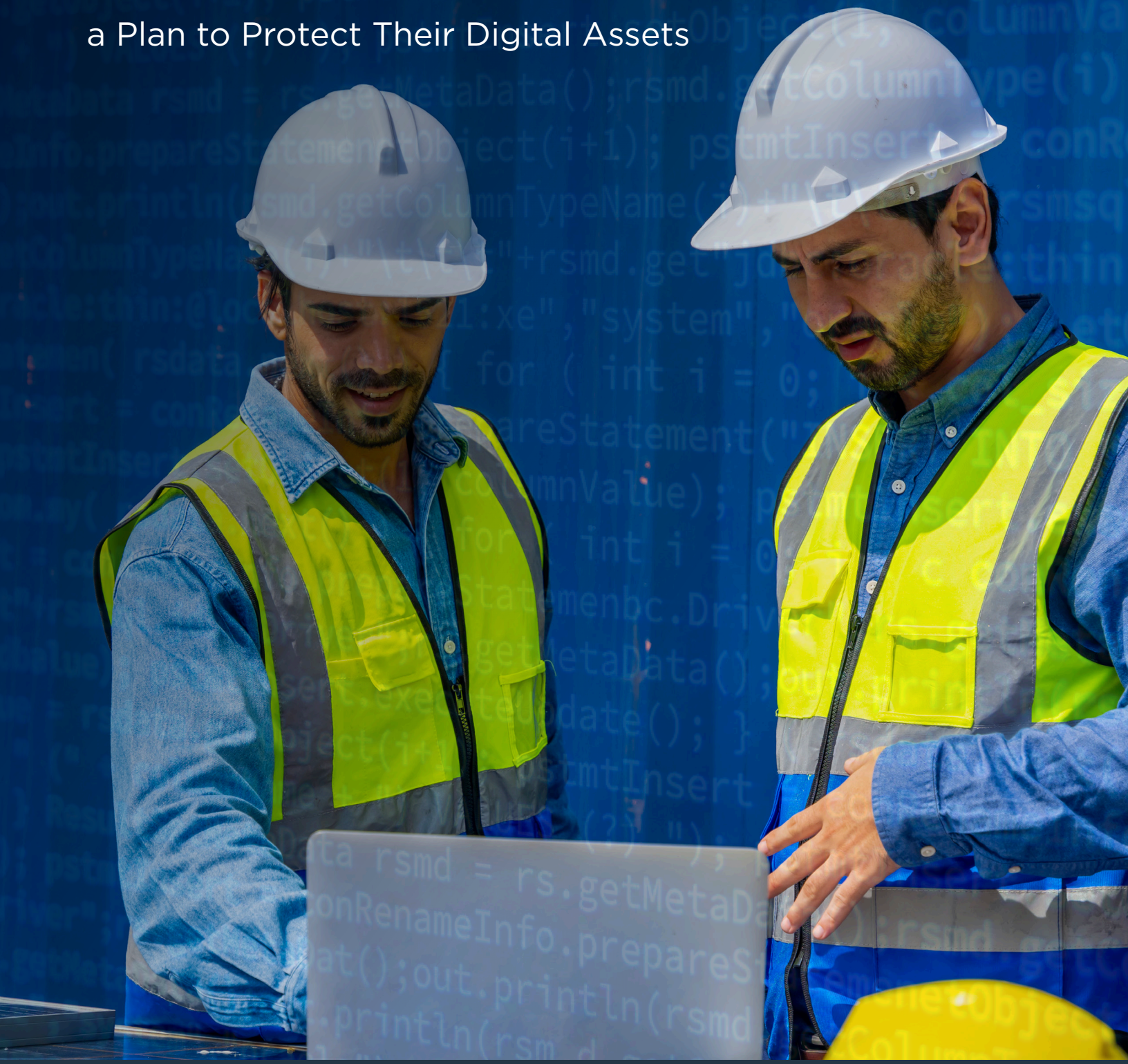
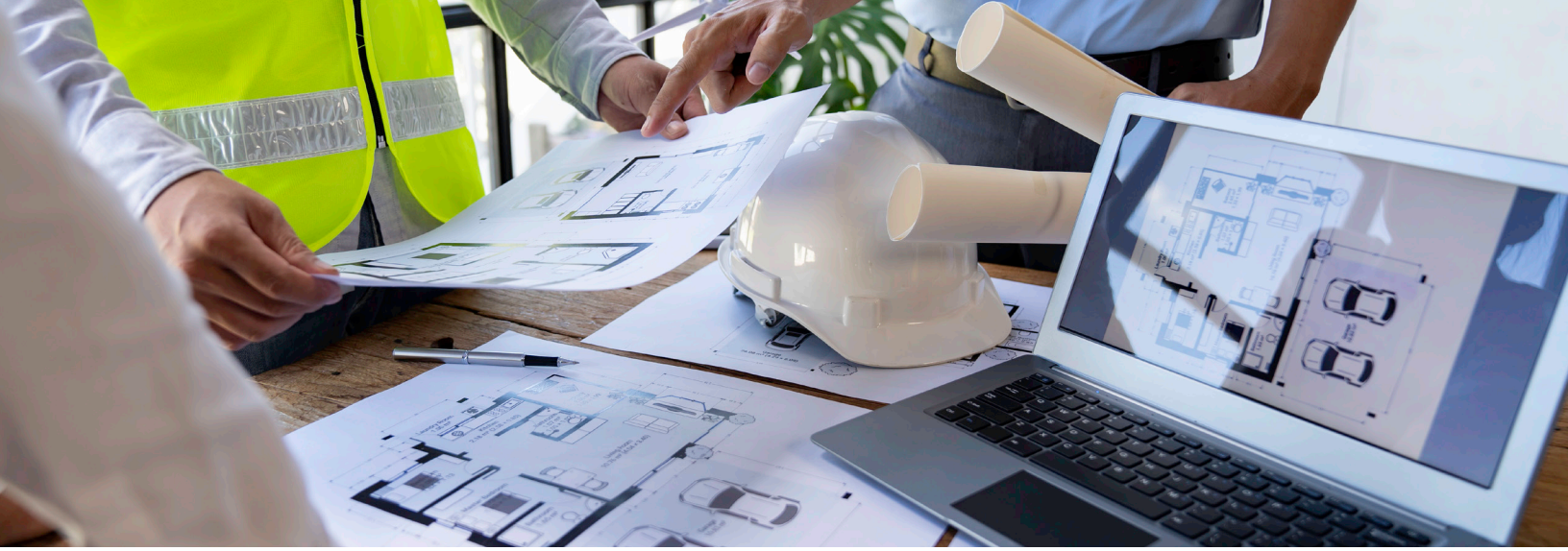
CONSTRUCTION

Building a Strategy for Cybersecurity

How Construction Firms Can Design a Plan to Protect Their Digital Assets





Technology continues to evolve in construction, with new programs, systems, safety devices and Internet of Things (IoT) devices being embraced by construction companies each day. What began as a shift from traditional methods using drafting tables to modern computer-aided design (CAD) and building information modeling (BIM) software has created a transformational reliance on technology, data and other digital assets from project concept to completion. With construction companies housing a den of desirable data, such as intellectual property, government project plans, proprietary designs and financial accounts, construction firms are a lucrative target for cybercriminals.

This risk makes it imperative for construction firms to develop strategies to mitigate their cyber exposure and to create a thorough cyber incident response plan. To ensure business resiliency, construction firms, regardless of size, must first understand ***why*** they are appealing targets, ***what*** are the biggest cybersecurity threats and ***how*** to implement proactive strategies and safeguards to mitigate potential risks.

The Why.

Unprepared & Under Attack

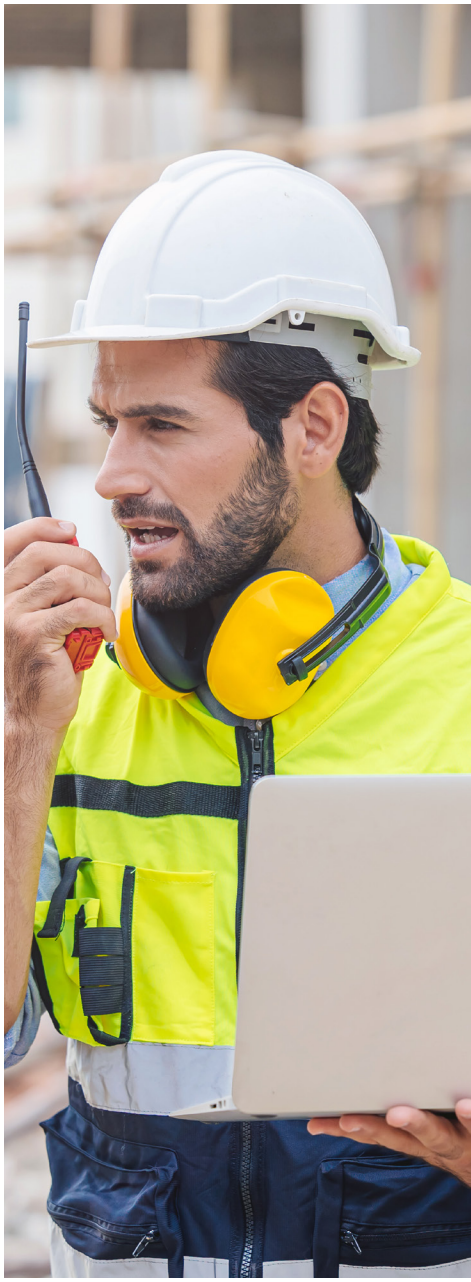
Cybersecurity is crucial for any organization, and the construction industry is no exception, facing such threats as ransomware attacks, malware infections and phishing expeditions. However, many construction companies lack the infrastructure and supports to protect themselves from cyberattacks and are vulnerable to security breaches due to:

- **Insufficient preparation.** The majority of construction firms — nearly three-quarters[1] — haven't prioritized cybersecurity and are not prepared for a cyberattack or system breach. In 2023, construction/real estate was cited as the No. 1 sector breached in the U.S., with more than 1.5 billion records compromised by bad actors.[2]

- **Increased use of technology.** Technological devices such as robotics, on-site systems, machine controls, artificial intelligence and drones have increased workplace efficiency at project sites, but devices are exceptionally vulnerable to breaches and require a cybersecurity assessment.

- **Third-party exposures.** The industry has become a complex network that collaborates with multiple firms, material suppliers, vendors, contractors, etc. Every new third-party connection tying into these different technologies creates integration challenges and more cyber exposures. In fact, construction-related companies rank third among North American industries in ransomware attacks, so it's important to know and evaluate the security dispositions of your third parties.

- **Information storage.** Construction firms store massive amounts of personal and sensitive business data, including proprietary information, intellectual property, government plans, project designs, company/client financials and corporate bank accounts, which makes them a lucrative target for cybercriminals.



[1]Construction Today, "Safeguarding the Construction Industry in the Digital Age," October 3, 2023.

[2]IT Governance, "Data Breaches and Cyber Attacks in the USA in December 2023," January 10, 2024.

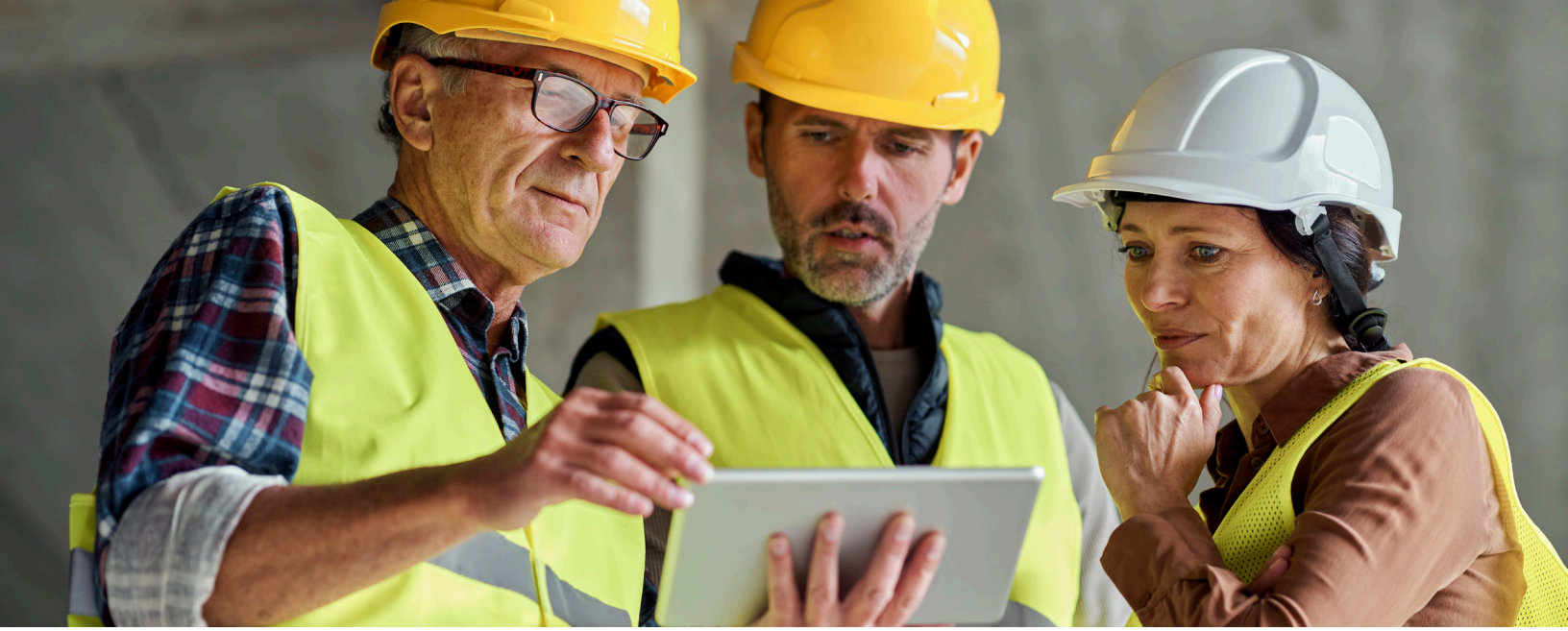
The What.

Types of Attacks & Threats

Although construction companies are vulnerable to many different types of cyber threats, ransomware, data theft and fraudulent funds transfers rank as the top three concerns.

Ransomware attacks involve cybercriminals infecting a company's system with malicious software that encrypts files until payment is made for their release. Damages from ransomware events are not confined to just payments: The fallout can include unauthorized access to business information, potential liability to vendors and clients and reputational harm. Cyberattacks can disrupt supply schedules and project deadlines that may result in delays, cost overruns and quality issues. Companies may also incur financial penalties or lawsuits for missed deadlines.

Data theft — whether acquired through ransomware, social engineering schemes or cyberattacks — remains a significant issue. Construction firms handle confidential intellectual property (design documents, patents, bid strategies, etc.), making them a prime target for cybercriminals who recognize the value of such data.



Fraudulent funds transfer, also known as **electronic payment compromise**, is another cyber risk scheme that construction firms face due to the substantial amount of funds that are transferred to various business, customer or vendor accounts via online banking. Fraudulent wire transfers are often the result of social engineering, which involves psychological manipulation by attackers who use emails and phone calls specifically designed to trigger emotional responses, such as creating a sense of urgency or fear to gain trust from an unsuspecting victim. Cybercriminals lure or trick them into providing access to restricted systems, exposing private data or downloading malware infections.

Design and construction firms also face social engineering attacks, phishing and spear phishing, as well as internal and external breaches from bad actors attempting to infiltrate their computer systems to access private information and disrupt business operations.

By understanding the anatomy of various cyber threats, companies will be able to identify vulnerabilities, implement appropriate security measures and develop an action plan in the event of a breach.

DID YOU KNOW?

Phishing breaches cost businesses an average of $4.72 million in 2023.

The How.

Plan & Prevent

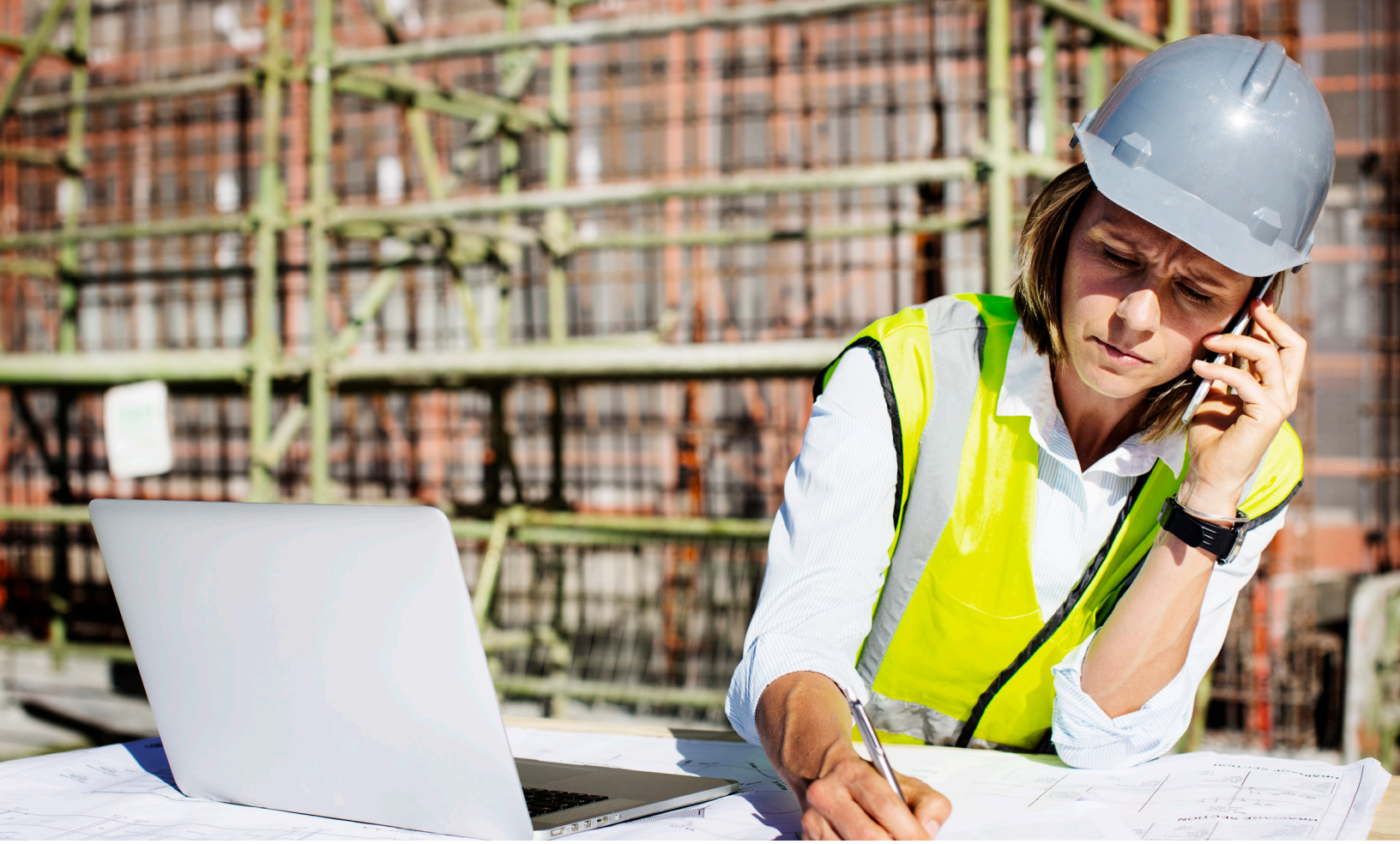
While cyber threats are increasingly prevalent, construction firms can take preventative measures to minimize their risks. An effective program starts with establishing a culture of security by selecting and supporting an individual within the organization to own and manage cybersecurity risk. To protect themselves, construction firms should:

- **Encrypt data, update system software and firewalls.** One of the easiest ways cybercriminals can gain access to company data is through outdated software and obsolete applications. Whether it's software from established third-party vendors or custom apps created by the company IT team, always patch vulnerabilities and perform regular updates. Enabling or configuring data encryption also protects sensitive information in transit or at rest.

- **Train employees in cybersecurity.** Cybercriminals can access company data and transfer funds through employees by using social engineering and business email compromise (BEC) scams. Educate employees on how to handle confidential information, implement multistep processes for confirming changes to vendor or client bank routing, train workers on how to identify cyber threats and report suspicious links and other questionable activity.

- **Use multi-factor authentication (MFA).** MFA provides an extra security layer when attempting to access sensitive information, such as bank accounts, construction invoices and legal documents. In addition to ensuring MFA is implemented on access to email and the corporate network, it should also be used to protect privileged or system administrator accounts and be required for access to system backups.

- **Develop and exercise an incident response plan.** Know what to do, who to call and how to mobilize in the event of a cyberattack. Consult with experts in the field including IT, incident response teams, insurance brokers and breach response counsel. Also, know what not to do in the event of a breach to avoid further compromising security and the company's reputation. Bring those plans to life by facilitating tabletop readiness exercises that include scenario role-playing.



- **Prioritize outside exposures.** Identify and mitigate cyber risks when working with external organizations. Review and reinforce contractual relationships to ensure adequate cybersecurity safeguards are in place for all project participants, including subcontractors, vendors and suppliers.

- **Secure proper insurance.** Enlist the help of trusted insurance professionals and risk services specialists to secure sufficient cybersecurity coverage and implement mitigation strategies.

Construction companies must build a strong foundation in cybersecurity to protect their digital assets and safeguard the confidential information of their clients and business associates.

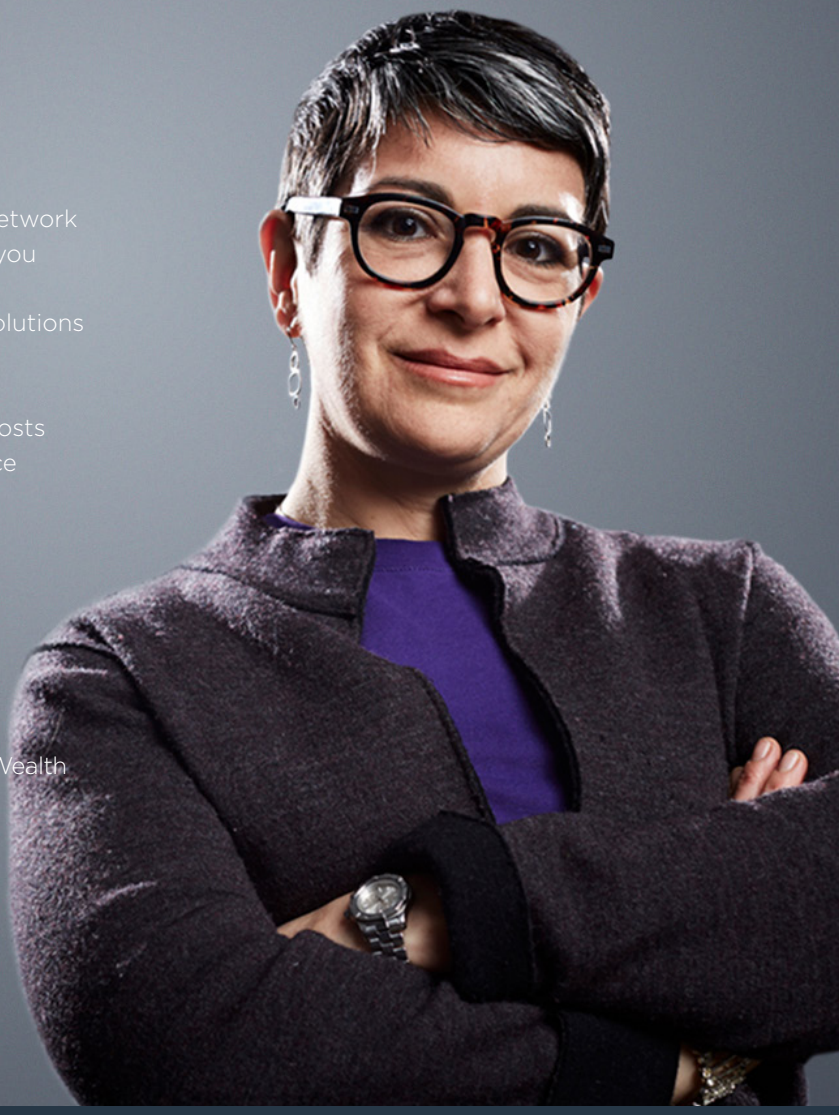
Contact **HUB International's construction insurance specialists** to learn more about protecting your business from a cyberattack.

Strategic support that puts you in control.

When you partner with us, you're at the center of a vast network of experts who will help you reach your goals. With HUB, you have peace of mind that what matters most to you will be protected — through unrelenting advocacy and tailored solutions that put you in control.

For more information on how to manage your insurance costs and reduce your risk, contact a HUB construction insurance specialist.

hubinternational.com/construction



Ready for tomorrow.

Risk & Insurance | Employee Benefits | Retirement & Private Wealth

HUB