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

Further, construction has become an increasingly complex network of interconnected frms 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 frms have the third-most ransomware attacks in North America, so it has become critical for frms to stay on top of the cybersecurity practices of their third-party partners.

Another vulnerability of construction frms 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 fnancials 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 frm, but the three most common and concerning are listed below:

» Ransomware is part of a one-two attack by cybercriminals. The frst 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 fles; 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 fnancial 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 fnancial penalties or lawsuits over missed deadlines.

» By whatever means it is stolen — say ransomware or social engineering schemes — data theft is a signifcant issue for the construction industry. Firms often manage confdential 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.

» Substantial funds are transferred via online banking between construction frms 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 frms. Education, planning, and prevention — with ownership and management of these responsibilities assigned to a specifc team member — will minimize digital risks and establish a culture of security. Efforts should include the following:

»

reviewed to ensure their cybersecurity practices are up to snuff.

» An incident response plan will enable a swift mobilization if a cyberattack occurs. Have

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,