Cyber Threats: Why the Construction Industry Could be the Next Big Target

While the health care sector consistently sees the highest number of cyber threats and data breaches, sectors with heavy construction presences like the technology, energy, professional services and industrial sectors annually make appearances in the top-five targeted sectors.

The Legal Intelligencer, Construction Law Supplement
August 12, 2021
By Karen E. Grethlein and David J. Shannon

A week before Christmas in 2013, a small Pittsburgh-based mechanical contractor gained notoriety as the source of one of the largest data breaches in history. Using a set of pilfered network credentials stolen from that contractor, criminals gained access to the global payment and billing network for retail giant Target. Once inside Target's network, the criminals utilized a sophisticated form of malware (i.e., malicious software) to identify and access approximately 40 million credit and debit card accounts.

Investigations by law enforcement and forensic specialists ensued. Litigation commenced and settled at great expense. By May 2014, Target's CEO had lost his job. By 2016, Target was reporting that the total cost of the breach exceeded $292 million dollars. The Target breach was extensive due in part to the company's size and large customer base, but even for small companies, expenses relating to cybersecurity attacks can accumulate quickly and cause collateral damage.

According to IBM Security and Ponemon Institute's 2021 Cost of a Data Breach Report (IBM report), the average cost of a data breach in the United States is $9.05 million (up from $8.64 in 2020). This staggering figure is comprised of costs falling into four general categories: detection and escalation (e.g., forensic investigation, crisis management); notification (e.g., compliance with regulatory requirements, letters to data subjects); lost business (e.g., business disruption, reputational loss); and post response (e.g., credit monitoring, legal expenditures, fines).

Troubling still, cyberattacks continue to increase exponentially. In 2021, the most prevalent threat continues to be ransomware, malware that restricts a system's files and threatens the victim with extortion and permanent destruction of the system's data unless a ransom is paid. According to cybersecurity vendor SonicWall's 2021 cyber threat report, ransomware attacks increased 180% in North America in 2021.

And while the health care sector consistently sees the highest number of cyber threats and data breaches, sectors with heavy construction presences like the technology, energy, professional services and industrial sectors annually make appearances in the top-five targeted sectors.

Why Are Construction Companies Ideal Targets?

Big Dollar Amounts. To begin with, large sums of money change hands frequently in the construction industry. For context, the price tags on some

recent Philadelphia-based projects exceeded the $1 billion mark: The Comcast Technology Center ($1.5 billion); The Pavilion at the Hospital of the University of Pennsylvania ($1.5 billion); and Schuylkill Yards ($3.5 billion). These costs are comprised of dozens, hundreds, or even thousands of subcontracts relating to the varying phases of construction, e.g., excavation, steel and electrical. Payment models vary, but typically a general contractor can be expected to pay out large chunks of cash to subcontractors over the life of a project via a stream of invoices and receipts for big-ticket items. And while some contractors may still pay via check, the increasing usage of wire transfers and e-payment portals pose an excellent opportunity for criminals to insert themselves in between the payor and payee in any number of transactions, where these large amounts are involved.

Numerous Points of Access. The dense concentration of contractors, design professionals, skilled trades, third-party inspectors, owners' representatives and other vendors on any job, gives criminals myriad opportunities to infiltrate the stream of money flowing through a project. The project's data security is only as strong as that of the entity with the weakest network safety. This stark reality is amplified by the increasing reliance on technology, which often means that each company's employees will be out in the field with their own sets of smartphones, tablets, and computers. Stealing a set of credentials to any one of those points of access, could be the way a cyber criminal gains access to the project as a whole.

Further, the increasing reliance on automation creates more avenues for infiltration and extortion. Contractors are using automation and smart systems for sprinklers, thermostats, elevators, lights, and heavy machinery, to name a few. Hacking into any of these systems could yield disastrous results. For example, think about construction cranes. A common sight in Philadelphia, they play a pivotal role in the construction of skyscrapers and transportation of heavy materials. Infiltrating and controlling a massive construction crane would at the very least inhibit a project's progress and at the very worst threaten the safety and wellbeing of those in the vicinity, depending on the criminal's motivations.

High Concentration of Confidential Data. Blueprints, in and of themselves, can be an attractive target. Accessing a set of blueprints, a cyber criminal can see the configuration of a building's floor plan and they can see where a building's servers, security and communications systems will be located. Worse, a cyber criminal could use this access to alter building plans undetected, the consequences of which could be dangerous and costly. In the national security context, this concept is particularly troubling when considering the motivations a cyber criminal might have to steal plans for, say, a military base.

Beyond blueprints, projects regularly involve trade secrets, copyrightable and trademarked material, and sensitive financial and business strategy information. Disclosure of such information could erode public confidence in a company, harm that company's reputation, and result in litigation and/or the loss of competitive advantages against rival companies.

Contractor Aversion to Down Time Can Result in Desperation to Pay Ransoms Quicker.

Contractors are uniquely vulnerable and arguably more predisposed to pay ransoms to a cyber criminal because of the losses they face during any delay on a project. On a jobsite, schedules dictate so much. Falling behind schedule can have a ripple effect that results in progress delays and expenses.

According to the Coveware Ransomware Marketplace report for Q4 of 2020, the average days of downtime for a company being held hostage by

ransomware is 21 days. And while downtime can mean different things, from mild slowdown to complete standstill, few contractors can afford to fall behind schedule by 21 days on a project. Add the prospect of contractually stipulated liquidated damages to the equation, and a contractor will do everything possible to get their systems up and running to avoid hemorrhaging cash.

How Can Construction Companies Strengthen Their Defenses?

Protect Data. The first and best line of defense against cyber attacks is a well trained and educated work force. Enacting policies to build a strong data security defense can literally save millions of dollars in data breach avoidance. Credentials can be better safeguarded by implementing forced password changes after a certain number of days and enabling multifactor verification (MFA). Minimize the number of employees who have access to confidential or sensitive information. Implement mandatory training for staff on how to identify common threats such as phishing and social engineering. Regularly update device software to make devices less susceptible to attacks. Create and maintain backups.

Have a breach response plan. The longer it takes for a company to identify and contain a breach, the higher the cost will be to address it. By having the plan in place, a contractor can immediately begin to mitigate the costs of a breach when it is discovered. The key personnel for a contractor should be trained and ready to jump in and respond to a data incident as soon as it occurs. Insurance personnel, attorneys and breach response vendors should be known and available for immediate action when the call comes in that a potential data incident has been identified.

Purchase Adequate Cyber Liability Insurance.

Whether a cyber criminal's motivation is making money, making trouble, or political activism, it's worth putting in the time and resources to keep your company properly insured for the risks of a data breach. The costs for attorneys, forensic companies, notification vendors and more can be significant. Cyber insurance can cover all these costs and ensure that experts in the data beach response field are available for your company at a moments notice.

David J. Shannon *chairs both the privacy and data security practice group, and the intellectual property, technology and media litigation practice group at Marshall Dennehey Warner Coleman & Goggin. He concentrates a substantial portion of his practice on privacy law, data breaches, intellectual property, copyright and trademark infringement, as well as trade secret, trade dress technology and media related litigation.* ***Karen E. Grethlein*** *is an associate in the professional liability department at the firm, where she focuses on construction injury and defect litigation, as well as data breach and cyber security. Grethlein is the current president of the Philadelphia Chapter of the National Association of Women in Construction. They may be reached, respectively, at djshannon@mdwcg.com and kegrethlein@mdwcg.com.*