Why The Construction Industry Is Being Impacted By Cyberattacks, And What To Do About It

THIS PAPER WAS WRITTEN IN CONJUNCTION WITH A BREAKOUT SESSION AT AGC'S 2021 SURETY BONDING AND CONSTRUCTION RISK MANAGEMENT CONFERENCE.

Paper Title: Why The Construction Industry Is Being Impacted By Cyberattacks, And What To Do About It

Jennifer A. Beckage, Esq., CIPP/US, CIPP/E [Author]
Daniel J. Parziale, Esq., CIPP/US [Author]

Beckage
The Liberty Building
420 Main Street, Suite 1110
Buffalo, NY 14202
716-898-2102
jbeckage@beckage.com
dparzale@beckage.com

Session Title: Cyber Risk: Are You Prepared for Project Disruption Due to a Cyber Attack?

Presented in part by Jennifer A. Beckage, Esq., CIPP/US, CIPP/E, Founder and Data Security Lawyer at Beckage

Author Biographical Information:

Jennifer A. Beckage, Esq., CIPP/US, CIPP/E is Managing Director of Beckage, a 360-degree technology WBE law firm with a recognized focus on data security and privacy. Beckage is a *Platinum Authorized Breach Coach* by *Net Diligence* and Jennifer has been named one of the *Top 40 Data Breach Lawyers in the U.S.* by *Cybersecurity Docket.* She has responded to numerous headline-making data breaches and is cited in national media on topics related to cybersecurity and privacy.

Daniel J. Parziale, Esq., CIPP/US is an Attorney at Beckage who regularly advises clients on matters related to incident response, notification obligations arising from data incidents, and evaluation of impacted information and systems. Daniel's extensive background in insurance provides him with a unique perspective on coverage issues related to cybersecurity and privacy.

Why the Construction Industry Is Being Impacted By Cyberattacks, And What To Do About It

By Jennifer A. Beckage, Esq., CIPP/US, CIPP/E and Daniel Parziale, Esq., CIPP/US

Introduction

For many years, the construction industry has appeared almost immune from cyber events because of the limited personal information it keeps. However, the last 12 months directly negate this view, reminding the industry that this perspective no longer carries weight. The construction industry is one of the leading industries impacted by data security incidents. This begs the question: why? And what can the industry do to address this rise in cyber threats?

Threat actors know that the construction industry is in some areas behind in data security and privacy initiatives. This is in large part because this industry, to date, avoided heavy regulation in data security and privacy laws. The limited regulation and guidance in the construction industry may have contributed to less focus on cyber security than in other industries.

Additionally, many in the construction industry are leveraging artificial intelligence technologies (AI) such as machine learning (ML) and robotics, among others. These new technologies still require data security and privacy risk assessments and proper controls in place, something that may be a second thought for those in the construction industry that may not have historically had cybersecurity top of mind.

Lastly, the threat actors seek to extort money, and the construction industry presents a big, lucrative target. The exposure of cyber-attacks in construction, in part, is amplified by the amount of confidential and proprietary information digitally stored and shared across projects and their long information technology (IT) chains. Infrastructure, financial accounts, as well as the data of employees, projects, and business sensitive information may be at risk. Accordingly, the number of cyber security attacks in the construction industry are growing exponentially.

The legal and threat landscape are constantly changing, requiring those in the construction industry to be familiar or associate themselves with experienced tech and legal providers who can assist in navigating these rushing river waters.

Some of the Largest Cyber Risks Facing the Construction Industry

While the risks of cyber-attacks are not unique to the construction industry, their impact on the industry is distinctive.

For example, on January 30, 2020, French constructing behemoth Bouygues announced that threat actors were holding 200GB of data ransom. *See* Naveen Gourd, *Maze Ransomware hits Bird Construction and Bouygues Construction*, https://www.cybersecurity-insiders.com/maze-ransomware-hits-bird-constriction-and-bouygues-construction/. Ultimately, the ransomware event caused delay to various projects as Bouygues shut down various operational systems to prevent propagation of the attack. *See* Bouygues, Press Release – Information on a Cyber Attack, https://www.bouygues.com/wp-content/uploads/2020/01/prbouyguesconstructioncyberattack01-31-2020-pdf.pdf.

Unfortunately, Bouygues is not alone in their suffering. Bird Construction, a large Canadian construction company, suffered a similar ransomware attack in December 2019, where the threat actors were demanding $9,000,000 CAD in exchange for decrypting the 60GB of data they were holding ransom. *See* Naveen Gourd, *Maze Ransomware hits Bird Construction and Bouygues Construction*, https://www.cybersecurity-insiders.com/maze-ransomware-hits-bird-constriction-and-bouygues-construction/.

These events are, unfortunately, very common in the construction industry.

There are three main cyber-attacks that could impact a construction company: i) ransomware; ii) fraudulent wire transfer; iii) downtime or business interruption; iv) breach of intellectual property; and v) breach of bid data. Each present their own impact and harm.

- *Ransomware*: Ransomware, or when a threat actor holds a computer system hostage for payment, can limit a construction company's access to critical systems and potential delay work at Project. Moreover, a construction company may be left with little choice but to incur the financial responsibility of paying the ransom. However, damage from a ransomware event is not simply limited to the payment of the ransom but may also include reputational damage.

- *Fraudulent Wire Transfers*: Fraudulent wire transfers, often the result of social engineering, present a substantial risk the construction industry, who are often moving large sums of capital around. Falling victim to fraudulent wire transfer not only presents dire fiscal issues for a construction company but can also lead to server reputation harm.

- *Downtime or Business Interruption*: The construction industry is heavily reliant on the ability to deliver projects on a deadline. A cyber-attack on a construction company's software or equipment could potentially cause a delay in the project while the cyber-attack is properly addressed.

- *Breach of Intellectual Property*: If a construction company is holding highly sensitive blueprints or schematics in its computer system, breach of these computer systems could result in major reputational damage and potential lawsuits.

- *Breach of Bid Data*: If a construction company holds information regarding its bidding strategies on a computer system, access and acquisition of these files could lead to a loss of a competitive edge.

What Happens In A Data Breach

The fast-moving cyber threat landscape above is juxtaposed with emerging data security and privacy laws. In the United States, there is no over-arching data security and privacy law(s). Instead, we have a patchwork of federal and state laws that may apply to an organization.

For example, let's pretend that Company XZY suffers a data breach that not only seizes access to systems, but one such system is a human resources program that contains all of the employee's personal information (whether hosted internally or with a third-party provider). Perhaps another system is a client management program that has sensitive design or tenant plans or city or government projects with confidentiality treatment requirements. Assuming in this scenario that the threat actor accessed and then exfiltrated the human resource system and client management program data, then Company XZY would have to provide notice to all potentially impacted persons (the employees in our scenario) under a myriad of state and perhaps federal laws, but also under contract to the third parties' whose confidential business information was impacted.

As it relates to the employees, it is important for legal counsel for Company XZY to review where each employee resides to determine applicable laws that will direct notification requirements for employees. As one can imagine, in a data breach with hundreds or thousands or more employees who are impacted, this could become complicated, but there are seasoned professionals who can help the organization prepare and respond. Unfortunately, most organizations are not prepared.

Besides operational setback from a data security incident and notifications to potentially impacted persons, there could also be perhaps revenue loss, reputational harm, legal fees, technical costs, call center expenses, credit monitoring costs, regulatory reporting, third-party claims, and more.

There are, however, ways that this risk can be shifted.

Actionable Steps the Construction Industry Can Take to Mitigate Cyber Risk

There are a number of methods your organization can leverage to limit its exposure to cyber risks. These include but are not limited to: 1) building a team of trusted advisors; 2) picking the Plan that is right for you; 3) evaluating risk so it is properly allocated through contract; 4) evaluating whether your organization has a strong cyber liability insurance policy; and 5) implementing good cyber hygiene and best practices.

1. *Build A Team of Trusted Advisors*

Cybersecurity preparedness will require knowledge and awareness across a number of roles within the organization. The leaders of the organization, information technology, legal, and most likely also marketing, sales, customer service, accounting, finance, human resources, and other groups to the extent they exist at the organization.

Third parties will likely need to be engaged as the legal and technical areas are emerging at rapid speeds. Further, the market is oversaturated with vendors, providers, partners of all types and sizes. Organizations should take time to validate credentials, years of experience, contractual terms, insurance carried, and more before you engage third-party partners to assist with your cybersecurity program development.

2. *You Pick the Plan*

The organization's team should, through a risk assessment, determine its cybersecurity program goals. Too often organizations are "sold" by a vendor as to a Plan, but if a breach occurred such plan would do very little to prevent legal and technical risk.

Some in the construction industry have robust experience with information technologies and others rely heavily on third parties. If the later, find a trusted partner to help you manage your third-party provider if your organization does not fully understand technically what they are doing. Just like an employee, those third parties should be reviewed on a regular basis (more on that soon).

3. *Contract with Strong Data Security & Privacy Provisions*

Another method of mitigating cyber risk is through contract. When reviewing your company's agreements with third-party vendors and subcontractors, it should pay close attention to indemnification and insurance procurement provisions for how they might allocate cyber risk between the parties. A data security incident at one of your company's vendors may have serious consequences when it

exposes your businesses information. To that end, your company may want to consider including language in its third-party contracts which require vendors and subcontractors to indemnify your company in the event the third-party vendor or subcontractor suffers a data breach. Similarly, your company might want to consider requiring a third-party vendor or subcontractor to name your company as an additional insured on its cyber liability insurance policy. Both of these steps help in the event your third-party vendor suffers a data security incident, as the financial impact on your business would be minimal.

4. Cyber Liability Insurance

If the third parties the organization is using do not want to (or they should not) carry certain risk, one potential method of mitigating risk associated with cyber-attacks are a cyber liability insurance policy. These policies generally provide coverage for the following types of attacks:

- *Data Breach Expenses:* When a threat actor accesses or acquires Personal Identifiable Information as defined by applicable law, your company has suffered a data security incident. Cyber liability insurance policies typically cover the costs of hiring of lawyers, forensic IT security vendors, public relations, or crisis communication costs to assist you in handling your response. Moreover, cyber liability insurance policies cover the cost associated with notifying to individuals and state regulators, providing identity and/or credit monitoring services to affected individuals, and running a call center.

- *Cyber Extortion or Ransomware:* When a threat actor acquires access to your company's systems and encrypts or otherwise locks you out of the network, demanding the payment of a ransom to unlock the system. Cyber liability insurance policies typically cover the cost of negotiating with the threat actor as well as potentially paying part of the ransom.

- *Fraudulent Wire Transfer:* When a threat actor misdirects a wire transfer from your company to a vendor, your company is victim of a fraudulent wire transfer. Cyber liability insurance policies will normally cover such fraudulent wire transfers if your company took certain steps to prevent them. Coverage for fraudulent wire transfers is generally limited to the amount of the wire transfer itself.

- *Business Interruption:* When a threat actor conducts a cyber-attack occurs, some cyber liability insurance policies provide coverage for the loss of business income as a result of being locked out or shut down as part of the cyber-attack.

As provided above, cyber liability insurance policies generally cover the major forms of a cyber-attack a construction company may face; however, cyber liability insurance is not the only means of mitigating the risk of a cyber-attack.

Cybersecurity insurance can provide first-party and third-party damages. Other insurance such as Tech Errors & Omissions may be options for some organizations to consider as well.

5. *"What's Good for the Goose is Good For The Gander" Policies and Practices*

a) *Policies & SOPs*

Applicable here is the old proverb "what's good for the goose is good for the gander" (what is good for the female should be good for the male).

If an organization is going to require that their vendors and third-party partners have certain controls and practices, then that organizations should perhaps think about their own practices. In fact, its insurance carrier may require it. Also, the organization may have requirements under laws and regulations, under contract, or other duties owed.

This is where most organizations are paralyzed – it sounds overwhelming. Or they find some stock policies, modify slightly, and place the policies on a virtual shelf.

In creating policies, the team charged with building a construction cybersecurity program will identify first the laws that apply to the organization, IT standards it wishes to follow, along with other guiding principles – organization mission, vision, codes of conduct or company ethics policies, and more.

Policies and standard operating procedures can come in a myriad of shapes and sizes, which makes creating them sometimes difficult for organizations – too many choices – so they pick and chose from numerous templates and the result is frankly a mess often times.

Organizations should plan to take time to put together written policies and procedures that reflect the *organization's* goals, vision, standards, controls, and more – not some other organization's that is in a template found online.

What are some good cyber security controls and practices? The National Institute of Standards and Technology's ("NIST") Cybersecurity Framework Version 1.1 offers for some a good place to start looking at what a cybersecurity program may look like on the technical side for your organization. *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf).

b) *Controls*

The organization will need of course a variety of physical, administrative, and technical controls.

Physical controls include safeguarding server rooms to video monitoring of secure areas (*careful if you are collecting biometric information, this is also a fast-moving area).

Administrative controls include the policies and SOPs discussed earlier, but also that there are folks responsible for these duties, there is training, review, auditing, discipline, and more.

Technical controls can take many forms but can include changing passwords regularly, implementing two-factor authentication where possible, and a regularly informing employees of the dangers of social engineering. Good cyber hygiene can prevent a cyber-attack from occurring in the first place, and in that regard is one of the most effective means of mitigating cyber risk.

6. Construction Cyber Culture

On final method of mitigating cyber risk is through fostering good cyber culture across the organization.

An organization is on its way to great construction cyber culture through the actional items above: 1) team of trusted advisors, 2) selecting a plan, 3) third-party contracting and auditing, 4) cybersecurity insurance, and 5) policies and procedures.

A great construction cyber culture begins with a buy in at the top and a demonstrating by example (so no exceptions!).

Conclusion

Unfortunately, organizations in most every industry are navigating cyberthreats and the construction industry is no exception. There are, however, a number of risk mitigation strategies that can be reviewed for applicability to an organization. As discussed, the first step is to find those experienced trusted advisors to help navigate this complex and sophisticated legal and technical terrain.