A KCA Construction Industry Article of Interest:

Cybersecurity in the Construction Industry – It Is Not a Matter of If, But When…

By Michael J. Brodzinski, Senior Vice President for Lockton Companies in Pittsburgh, PA

NOTE: *This article first appeared in Pietragallo's Construction Legal Edge Fall 2019 Issue.*

Businesses operating in the construction and design industries are quickly becoming aware of the challenges they face against an unfamiliar adversary – cyber criminals. However, many companies have been slow to properly identify and address their cyber risk vulnerabilities. It is estimated that damages associated with cybercrime will costs businesses in all industries approximately $6 trillion per year on average through 2021 and a recent survey revealed that more than 75 percent of respondents in the construction, engineering and infrastructure industries had experienced a cyber-incident within the last 12 months.[1] It seems now more than ever that it is not a matter of if a firm will experience a cyber event, but rather a real probability of when it will occur and how it will occur.

Cybercriminals are always evolving, changing their methods to by-pass protections and using unique methods of social-engineering to exploit basic human behaviors for their own financial gain. The construction industry needs to be equally aggressive in its response, viewing cyber risk from an enterprise-wide perspective in the boardroom, at the project site, and throughout the culture of the entire organization. While there is not a "one-size-fits-all" approach to cyber breach prevention, this article will discuss scenarios and basic risk management protocols.

The construction industry is particularly vulnerable to breaches because of its reliance on mobile communication and file and data sharing among many parties. Firms of all sizes are at risk and 50% of all attacks in the country are targeted to businesses with less than 1,000 employees.[2] With the average cost of a data breach at $3.8 million, construction firms have more to lose than

simply stolen data. Many attacks are aimed at interrupting business operations and creating project delays in exchange for ransoms, which often start at $500,000.2 Below are recent real-life scenarios presented at the 2019 Lockton Construction & Design Conference:

1. In early 2018 a firm discovered that more than 500 Microsoft Office 365 accounts were compromised by hackers, including 43 administrative accounts. The compromise was traced to IP addresses in Russia and the Netherlands. While the breach was discovered in early January, the firm believes the hackers were in the system for several weeks before being discovered.

    - Once inside the firm's system, the hackers accessed email mailboxes and client project sites containing sensitive data.

    - It was ultimately determined that no notification to individuals was required, but the firm incurred significant costs to investigate and respond including $22,114 in legal advice and $376,346 in forensics costs. They did not have cyber insurance.

2. A firm's system was breached, and data was stolen by hackers who demanded a ransom of 135 Bitcoin (worth about $500,000 at the time of the loss) to return the data. The firm engaged a forensic investigator who was able to restore all the data from a backup system and therefore the firm decided not to pay the ransom demand.

    - The firm incurred $430,000+ in forensic and restoration costs, as well as $8,500 in legal costs. All costs in excess of the firm's $10,000 retention were covered by the cyber insurance carrier.

3. A firm hired an entry-level associate to assist various executives with special projects (none were HR or personnel related). After the associate had worked at the firm for several months, the firm was contacted by another associate indicating that someone with the entry-level associate's name attempted to open a credit card using the other associate's identity.

    - The firm did an investigation and found that the entry-level associate accessed personnel files on nearly 400 employees. This was outside of the scope of the associate's work for the firm and there 3 was no legitimate purpose for the accessing of these files.

    - Before the firm could act against the entry-level associate, the firm was contacted by local law enforcement alleging that the associate was involved in a large identity theft ring. Law enforcement coordinated with the firm to execute an arrest warrant for the associate.

    - The firm had to notify all 400 employees of the compromise of their personnel files and offered two years of credit monitoring (a cost of ~$35/employee per month) and make notice on their website and other media outlets causing unknown reputational damage.

4. A firm was notified of an incoming EFT payment of $1.9M – it was owed this amount by a client. When the firm didn't receive the payment within a few days it called the client to inquire about the payment. While the client was checking on the status of the $1.9M payment, the client wired a separate $497,055 amount it owed to the firm from a separate invoice. After the firm did not receive either payment, a deeper investigation ensued.

    - Upon further investigation, the firm determined that a bad actor hacked the firm's systems, amended instruction on pending invoices, and sent those invoices to customers while purporting to be a firm employee.

    - The client refused to pay the invoices a second time and did not have insurance coverage for this scenario (i.e. social engineering coverage). The firm itself had a cyber policy but did not have "invoice manipulation coverage" and therefore it still has a $2M+ open account receivable.

    - Invoice manipulation coverage is a very new coverage available in the cyber insurance market.

All contractors and project owners are aware of construction risk and while basic general liability, builders' risk, professional liability and other insurance solutions protect against various forms of losses and project delays, many of these policies exclude cyber related losses. Only about 15% of construction companies purchase cyber insurance today.2 Cyber insurance can reduce the likelihood of a company exhausting all of its resources to investigate and recover from an attack. In the event of an attack, cyber insurance would cover the potential demand and extra expenses, including forensics and investigation, up to the specified cyber policy limit in excess of a deductible or retention.[3] Many of the leading insurance carriers have created cyber policies and there are nearly 100 different versions available in the marketplace. Because there is no standard ISO policy form, it is critical that construction companies work with an expert risk management professional to amend the standard policy language with exclusive amendatory endorsements to ensure that they are receiving optimal coverage options.

The value that cyber insurance provides is demonstrated through the extensive core insuring agreements and enhancements available in the marketplace, such as: Network security liability, Privacy regulatory proceeding, Breach response costs, Cyberextortion reimbursement, Hardware replacement (bricking), Data recovery, Business interruption and extra expense, Dependent business interruption, Reputational harm and the previously mentioned Invoice Manipulation.

Cyber insurance is only one way to protect businesses and projects from these types of attacks. There are several risk management protocols to institutionalize within a firm which starts with establishing a strong team of stakeholders from inside and outside the organization. Some risk management protocols to consider are:

- Create a security education, training and awareness (SETA) program.

- Implement password security and require two-factor authentication at a minimum.

- Use the "principle of least privilege," where users are granted access only to the information they need to do their job.
- Think beyond computers and software to other tech-enabled products, such as HVAC, fire suppression, BIM, and waterflow systems.
- Keep up with advances, including the latest patches for software.
- Consider a penetration test, where "ethical hackers" attempt to find their way into your system. With 4 the findings from the test, firms know where to make adjustments.
- Because it's impossible to know exactly where or how the next cybercriminal will strike, prioritize your most critical data first.[2]

In an increasingly digitized and connected world, cyber security needs to be considered at all stages of a firm's operation. While it may seem daunting, cyber security can be approached in the same way as any other risk. Crucially, cyber risk should not be seen as an issue solely for a contractor's IT department or provider. While IT infrastructure is an important factor in managing cyber risk, it is just one piece of a much larger puzzle. It is important for construction firms to appreciate the likelihood that they will fall victim to some form of cyberthreat and cyberattack. Once cyber is accepted as a key strategic risk, organizations can progress to not only protect themselves, but plan how they will respond and recover when an incident occurs.[4]

Sources:

(1) The Case for Cyber Coverage in the Construction Industry https://riskandinsurance.com/case-cyber-coverage-construction-industry/

(2) Experts in AEC firms: stop ignoring cybercrime vulnerabilities https://www.constructiondive.com/news/experts-to-aec-firms-stop-ignoring-cybercrime-vulnerabilities/556162/

(3) Ransom where? Holding data hostage with ransomware http://www.locktononline.com/iknowledge/Lockton%20Toolbox%20Documents/White%20Papers/Barnes-Ransomware-May%202019.pdf

(4) Cyber security and the construction industry https://www.zurichna.com/en/knowledge/articles/2019/08/cybersecurity-and-the-construction-industry

Michael J. Brodzinski, Senior Vice President for Lockton Companies in Pittsburgh, PA. Mr. Brodzinski can be reached by phone at 412.577.2981 and email at Michael.brodzinski@lockton.com.