MINESH PANDYA
PRINCIPAL, CYBERSECURITY & RISK HKA

Increasing cyber attacks in the construction industry are causing disruptions and delays

Introduction

Historically, construction has not been high on the list of targeted industries by attackers, who have typically chosen industries such as financial, government and healthcare, where financial rewards–from sensitive and personal data rich firms–are more lucrative. In recent years, we have seen a step change with several high-profile successful cyber-attacks within the construction industry causing delays, business disruption, financial impact and reputational damage.

Investment by construction companies in cyber defences has typically lagged behind other industries. This is largely due to fewer mandatory regulations and guidance, and partly due to lack of compelling board level business cases to invest in cyber defences, when the chances of getting attacked were relatively low and therefore did not justify the return on investment.

Attackers now view construction as an easier target when compared to other industries as their cyber defences are not as mature, therefore the effort and cost on the attackers' behalf to launch a successful cyber-attack is far reduced. Additionally, financial rewards for the attacker are becoming more lucrative as many construction firms embark on digitisation programmes and introduce new technology, for example Internet of Things (IoT), to monitor the real-time health and performance of their resources. These initiatives are rapidly increasing the firm's digital footprint and therefore attack surface, giving the attacker more opportunity to launch cyber-attacks.

Here we will explore the top five common cyber-attacks faced by the construction industry, provide examples of real incidents that have occurred and discuss what we can do to reduce the risk of a successful cyber-attack.

"Attackers now view construction as an easier target when compared to other industry as their cyber defences are not as mature, therefore the effort and cost on the attackers' behalf to launch a successful cyber-attack is far reduced"

Top Cyber Attacks and Impacts Facing the Construction Industry

1. Ransomware

   a. For Financial Gain

Ransomware is a type of malicious software used by attackers that typically infects computer systems and encrypts files, making users unable to use or access encrypted files until a ransom is paid. The software can be installed in several methods, such as an employee opening legitimate looking emails with malicious attachments,

unpatched or vulnerable software, or by visiting a legitimate website whose security has been compromised, hiding malicious scripts.

The ransomware threatens to publish sensitive data unless a ransom is paid, leaving the firm unable to recover the files without a decryption key. The attacker is typically difficult to trace and prosecute as they use digital currencies such as Bitcoin and other cryptocurrencies for the ransom demand.

The impact of ransomware is not simply limited to the payment of the ransom and associated clean-up costs, but may also include reputational damage.

b. To cause Disruption and Delay

Ransomware can also be used by an attacker, with the primary goal to disrupt business operations by denying users access to systems or equipment, rather than demanding a payment. The attacker infects computer systems using the same methods described in 1.a. above.

The impact of such an attack could hinder the construction firm's ability to meet a project deadline which may incur contractual financial penalties and lawsuits.

2. Business Email Compromise (BEC) for Financial Gain

BEC can also be known as whaling, spear-phishing, or CEO/CFO fraud. The attackers perform research on the victim firm and then target employees with access to company finances. The method of attack is where the attacker fraudulently accesses company funds by sending an email purporting to be from a legitimate sender such as a customer or trusted company executive. The emails typically pressure employees to act quickly, and request funds be transferred to the attackers' bank account to pay an invoice for example.

3. Data Breach of Intellectual Property or Personal Data

Construction companies often hold and work with highly sensitive information such as blueprints, or schematics in their Building Information Modelling (BIM) system, breach of these systems, other technology devices, and their vendor supply chain could result in major reputational damage and potential regulatory fines and lawsuits where personal data is involved.

4. Supply Chain Attacks

Complex projects in the construction industry poses a particularly high risk to cyber-attack, as they often involve multiples entities such as suppliers, contractors and partners. These entities, if compromised by an attacker, can then be used as a platform or conduit to launch attacks against the target firms' systems and employees. The attacks are usually less likely to be detected due to the trusted relationship between the parties.

Potential impacts are wide ranging, from disruption, delay, financial loss and reputational damage.

5. Insider Attacks

Insider threats include, malicious insiders, disgruntled employees, reckless third parties, insider agents, careless employees or compromised employees. Potential impacts are wide ranging as described in 4. above.

Recent Cyber Attacks in the Construction Industry

1. Bird Construction – *Ransomware for Financial Gain*

Bird Construction, a Canadian construction company suffered a ransomware attack. The attackers were demanding payment in cryptocurrency (the amount equivalent to approximately 9 million CAD) as payment to prevent the attackers releasing stolen personal information.

2. Royal Bam Group - *Ransomware to Cause Disruption and Delay*

Attackers found a vulnerability in the firm's website that enabled them to access the firm's corporate network. From there, the attackers used tools to encrypt the firm's files – stopping the company from accessing them. The hackers then started sending messages, demanding payment for the firm to gain access to its own files.

3. Solid Bridge Construction – *BEC for Financial Gain*

BEC attacks tend to be less widely reported by firms that have fallen victim, largely due to reduced regulation to mandate reporting of such incidents. One reported incident however occurred when Solid Bridge Construction, a company which helps develop large scale commercial projects, based in the city of Huntsville, Texas, was subject to such an attack.

One of the companies that Solid Bridge worked with is Chance Contracting LLC, based in Pinehurst, Texas, who are involved in the construction of road surfaces for large commercial construction projects.

Solid Bridge received an email claiming to come from Brett Chance, the owner of Chance Contracting. The email claimed that Chance Contracting was having "issues" receiving check payments and asked that a payment could be sent to a different address – one located in Washington.

Solid Bridge duly sent a check for $210,312.00, believing it was making a payment in response to a legitimate invoice from Chance Contracting. The payment was in fact sent to an attacker email address that looked very like, but not quite the same as, the one used by the genuine Brett Chance of Chance Contracting.

"Insider threats include, malicious insiders, disgruntled employees, reckless third party, insider agents, careless employees or compromised employees."

How to Reduce the Risk of a Cyber Attack in the Construction Industry

There is no one silver bullet for business leaders of construction firms, however important factors in reducing cyber risk include, top level

management support and fostering a cybersecurity culture across the firm.

A risk assessment should be performed to identify the cyber security risks applicable to a particular firm due to its unique operational environment and activities. Risks should be quantified and explained in simple language to top level management to ensure business cases can be understood, reviewed and approved.

A comprehensive cyber security strategy and implementation plan helps ensure that the firm has the most appropriate people, processes and technology in place to help mitigate cyber risks.

Firms should also have an incident response plan that is regularly tested to ensure the impact of a successful cyber-attack is minimised.

If you require any further information, please contact Minesh Pandya at mineshpandya@hka.com

HKA