Cyber risks in the construction industry

Gallagher

Insurance | Risk Management | Consulting

With ransomware attacks such as WannaCry and NotPetya and data theft from major companies such as Equifax repeatedly hitting the headlines last year, it is unsurprising that an increasing number of companies are questioning their resilience to cyber risks. While historically the construction industry has been less of a target due to the fact that the majority of construction firms' revenue generating activities are conducted offline, changes within the industry and the increasing importance of technology means that the industry is not entirely free from cyber risk.

Construction contributes 7% of the UK's GDP, which makes it a more valuable target than you might initially expect. With an increased reliance on remote systems such as Building Information Modelling (BIM) and also project management systems, the construction industry's exposure to cyber risks is changing.

What types of threats exist?

There are a variety of different threats that the construction industry could be impacted by, but the most common include:

- **Phishing** – malicious emails designed to look like genuine emails which encourage employees to click – infecting their computers in the process.
- **Viruses** – code which infects computer system, corrupting or deleting data.
- **Hacking** – an individual or group attempting to gain access to company systems with the intent to steal or destroy data.
- **Ransomware** – a malicious programme which locks access to company files and data until a ransom payment is made, after which time access may be restored.

The business implications

All data, whether that is customer databases, employee files, financial information, or even project specific contracts, plans, or correspondence, holds value for cyber criminals so businesses need to take steps to protect their data. Every company holds customer data to a greater or lesser extent, and every company has to issue invoices and use payment systems for both payroll and processing, so theoretically, any company can be made a target for cyber criminals. Data can be stolen (potentially causing financial loss through fraudulent transactions) or sold online, impacting the company that has suffered the breach, and potentially, depending on the nature of the data stolen, also impacting a third party, such as a client. There have also been an increasing number of ransomware cases; not only is there a cost associated with paying a ransom to re-access your systems and files, there is no guarantee that access will be granted even after a ransom has been paid, leaving companies to the whim of cyber criminals that demand additional sums.

Construction industry risks also include the stealing of designs and blueprints, which could lead to an extensive project delay. A serious attack could see a company lose access to their systems, causing a significant impact on day to day operations, project progress and relationships with clients. Indeed, the reputational risks could outweigh the financial; customers are unlikely to work with a company that cannot demonstrate resilience to cyber risks.

The legal implications

A recent Gov.uk survey discovered that senior managers in construction do not prioritise cyber-security, with 41% admitting that senior managers were not focused on cyber security and only 35% agreeing that cyber security was a key part of their daily work. Yet with the EU's new data protection standard, General Data Protection Regulation (GDPR), due to be introduced on 25 May 2018, failing to adequately secure client data specifically, could see the company facing a hefty fine. Companies may also find themselves on the receiving end of litigation by third parties that have been impacted by a cyber event if they believe that their data had not been suitably safeguarded.

How can you protect your business?

With any good risk management policy the key is training and awareness. Educate your staff on how to identify phishing emails and encourage them to report anything suspicious to senior staff. Reinforce the importance of setting good passwords and back up data regularly so that if systems are compromised, operations need not grind to a halt. Treat cyber risks like any other risk to the balance sheet or reputation, rather than leaving the management of cyber risks exclusively in the hands of the IT department.

Cyber insurance

While prevention is better than cure, a robust cyber insurance policy can help to mitigate some of the financial and reputational damage of an attack and will help companies get back up and running with minimal interruption.

All of Gallagher's cyber protection programmes are carefully designed to provide comprehensive cover for a range of risks including:

- Cyber extortion and cyber terrorism
- Data asset loss
- Business interruption and loss of income
- Breach response costs
- Regulatory investigations and defence costs
- Civil fines and penalties (a major concern with GDPR)
- Litigation damages and costs from individuals/class actions
- Multimedia liability.

Extensions are also available for reputational damage and cybercrime.

SOURCES
1. rg-group.co.uk/whitepaper-cyber-crime-and-the-construction-industry/
2. www.gov.uk/government/statistics/cyber-security-breaches-survey-2017
3. www.gov.uk/government/statistics/cyber-security-breaches-survey-2017

Case study

Type

Data breach and ID theft using a fake email

Scenario

An employee in a large construction firm responded to an apparently genuine email request from a trusted source for confidential employee tax records and other information.

Sting

'Spear phishing' involves sending a fraudulent email that looks genuine. Hackers spoof the 'From:' line of the email so the sender feels real – say from the CEO or a trusted third party. The victim recipient then responds, clicking a malicious link in apparent good faith but that response - including any attachments – is re-routed to the hacker's email account.

Investigation

That single email reply harvested the full names, addresses, employment status and tax records for every employee working for the company during that year.

Conclusion

Never put blind faith in what arrives in the inbox. The sender may be fake and click-through links may be malicious. Human processes are key: always double-check all sensitive requests for information directly with the requester to establish bona fides.

TO FIND OUT MORE ›

TOM DRAPER
Technology & Cyber Practice Leader
+44 (0)20 7204 6223 | Tom_Draper@ajg.com

@GallagherUK_ | /arthur-j-gallagher-international | ajginternational.com

Arthur J. Gallagher (UK) Limited which is authorised and regulated by the Financial Conduct Authority. Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AW. Registered in England and Wales. Company Number: 1193013. www.ajginternational.com. FP294-2018 Exp. 26/03/19.

Gallagher
Insurance | Risk Management | Consulting