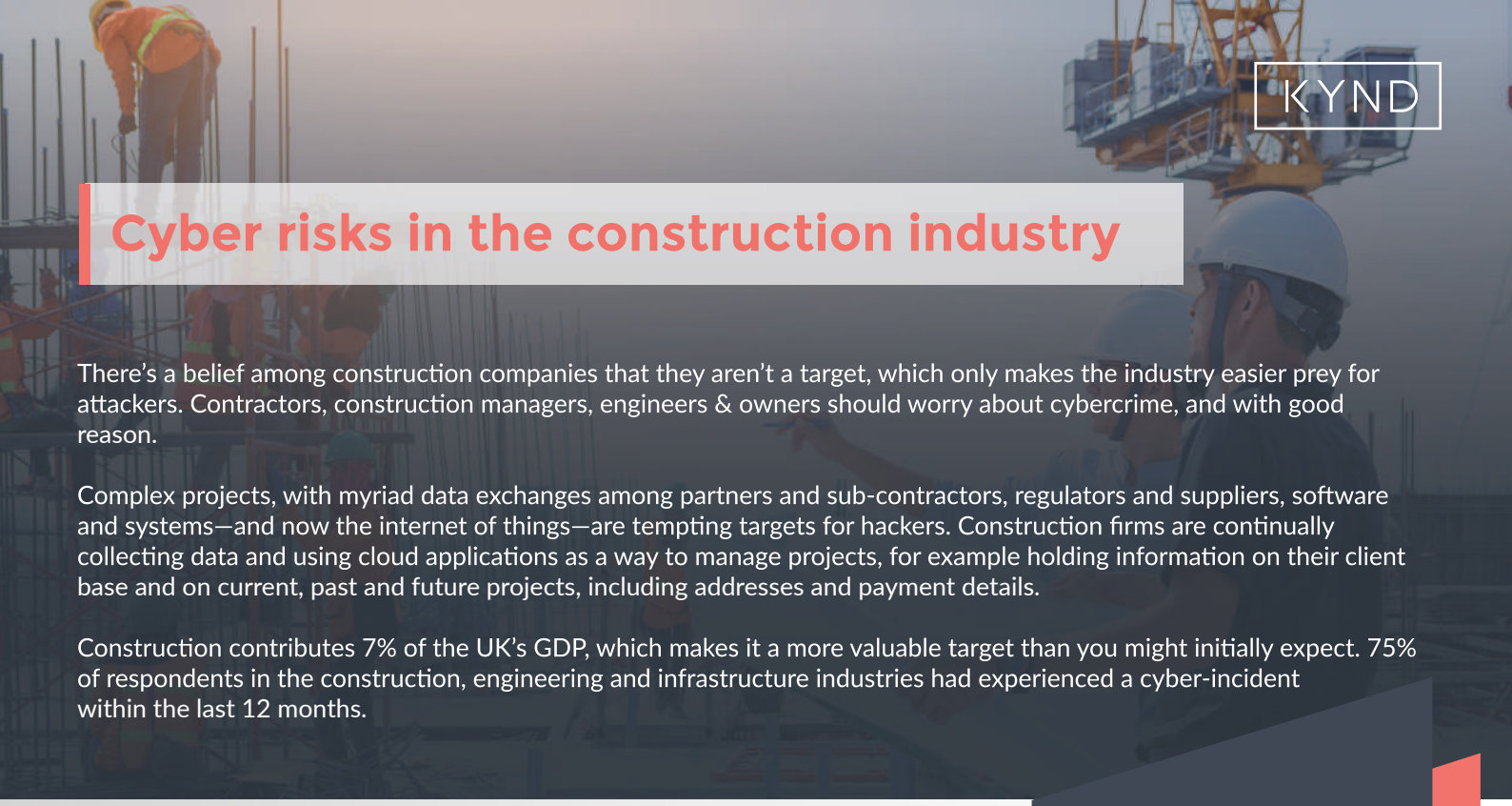

KYND

Cyber risks in the construction industry

There's a belief among construction companies that they aren't a target, which only makes the industry easier prey for attackers. Contractors, construction managers, engineers & owners should worry about cybercrime, and with good reason.

Complex projects, with myriad data exchanges among partners and sub-contractors, regulators and suppliers, software and systems—and now the internet of things—are tempting targets for hackers. Construction firms are continually collecting data and using cloud applications as a way to manage projects, for example holding information on their client base and on current, past and future projects, including addresses and payment details.

Construction contributes 7% of the UK's GDP, which makes it a more valuable target than you might initially expect. 75% of respondents in the construction, engineering and infrastructure industries had experienced a cyber-incident within the last 12 months.

Business exposure and implications

Access to clients' confidential information

Compromised intellectual property such as building specifications and architectural drawings can provide a roadmap for criminals to gain access to valuable personally identifiable information (PII), including financial accounts and employee data.

Business interruption exposure

As in any industry, cyber attacks can result in costly business interruptions for construction companies. A delay in a construction project can mean the difference between a small profit and a devastating loss.

The legal implications

Failing to adequately secure client data could see the company facing a hefty fine under GDPR. 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.

Mobile dependency

Many stakeholders involved in construction projects are highly dependent on mobile devices and laptops, offering multiple access points to networks and creating vulnerability if they are not all adequately trained on cyber security. Adding another layer of exposure, valuable technology (such as laptops) is often stored on job sites in unsecured trailers, making this information an easy target for thieves.

Increased reliance on technology

Wearables and drones provide real-time monitoring and data collection, while virtual reality can create simulations of building designs. These technologies open a world of safety, training and efficiency opportunities, but also give malicious actors potential access to valuable information.

Key industry statistics

75%

of respondents in the construction, engineering and infrastructure industries experienced a cyber-incident within the last 12 months[1]

61

is the average number of email fraud attacks a company in the construction industry will face every three months[2]

77,000

incidents of online crime against construction companies last year[3]

2,000

construction firms have had their online accounts raided by thieves in 2015[4]

What types of risks exist?

There is 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 or stealing passwords in the process.

Viruses
Code which infects computer systems, 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.

KYND

KYND's analysis of key cyber risks of the top* 100 UK construction companies
*by turnover

Ransomware Risk

47.5% of companies had at least one external internet service exposed which would place them at a higher risk of a ransomware attack.

Email Spoofing

91.5% of companies were vulnerable to having their email addresses spoofed.

Vulnerable Services

85.0% of companies were running at least one service, such as an email server or web server, with a well-known vulnerability to cyber attack.

Out of Date Software

41.5% of companies had at least one service that was using software which was out of date, no longer supported and vulnerable to cyber attack.

Certificate Issues

31.5% of companies had at least one security certificate which had expired, been removed or distrusted.

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.

How KYND can help

- With just a website name, KYND reveals your organisation's cyber risks
- Instantly KYND lets you know if your emails are spoofable or if you're vulnerable to a ransomware attack
- KYND provides clear and easy recommendations without using technical jargon
- KYND continuously monitors and alerts you instantly if any new cyber risks are found

Get in touch
broker@kynd.io
www.kynd.io