Willis Towers Watson

Managing cyber risk in the Construction sector

March 2019

If you think it can't happen to you...think again.

Cyber security represents a rapidly evolving challenge for the construction sector and should now be a top priority for industry leaders. The idea of a rogue actor hacking into operational machinery, seizing control of it and wreaking havoc may sound like a Hollywood script. The threat however, is real. Some of the greatest potential financial and reputational risks lie with the loss of access to critical systems and the data, both of which are increasingly governing the success of construction projects.

Technology has transformed working practices in the construction industry, driving operational efficiency and innovation. The increased adoption rates and increasing reliance on digitised technology means increased interconnectivity and a widening attack surface of systems for network- born security threats. If the construction industry does not focus on a holistic approach to cyber risk, through the lenses of people, capital and technology, all of these operational efficiencies may be lost.

Increasing reliance on technology and access to data.

To illustrate the sheer pace of technological advancement in the sector, one has to look at the rapid adoption rate of Business Information Modelling (BIM) in the construction sector. According to a recent report by the National Building Specification (NBS)[1], adoption rates have increased from 13% in 2011, to 74% in 2018, nearly a six fold increase over seven years. Within the next three to five years, this is expected to increase to over 90%.

One of BIM's main advantages is its ability to act as a computer-based control system, used for designing buildings. This enables full integration and collaboration between contractors via a shared project model through a single repository of information – where all parties can access and change the model. Having large amounts of information centrally, places reliance on the critical systems being readily available, with accurate data; thus heightening the potential financial and reputational outcomes of lost access to the data or unavailability of the systems.

The methodology behind the operation of these systems, as well as the potential numbers of individuals that have access to it when working on construction projects, make them vulnerable to **malicious** and **non-malicious** threats from both external and internal actors. For instance:

- External malicious actors may want to abuse confidential data, corrupt BIM or simply disrupt operations.
- WTW insurance claims data shows that specifically 58% of cyber incidents are the direct result of employee negligence,[2] illustrating that the internal threat can't be ignored. This could be as a result of a malicious act through a disgruntled employee, or a simple (non-malicious) mistake by an employee. By way of example, non-malicious mistakes could include opening a phishing email with a malicious attachment, plugging in an infected USB stick into a system or simply leaving a laptop on a train (those listed above are by no means exhaustive).
- Alternatively, your systems may just fail, whether this is through a bug in the operating software or a failed upgrade.

---

1. http://www.bimacademy.global/wp-content/uploads/2018/05/NBS0850-BIM-Report-2018-LR-.pdf
2. https://www.willistowerswatson.com/en/campaigns/cyber/services/cyber-risk-culture-survey

Tightening regulatory environment and data risk.

Construction firms collect and store a variety of different forms of data, which may include client data, sensitive commercial material, sub-contractor data, employee data and financials. As highlighted above, this is more likely than ever to be stored electronically in a single location.

Consequently, this makes for a larger potential prize for malicious actors who may seek this data to plan terrorist incidents, sell it on the dark web for financial gain by encrypting it, making it unusable and demanding money from you to decrypt and regain access to that it (this is known as a ransomware attack). Building specifications and architectural drawings can also provide a roadmap for criminals to gain access to personal data e.g. financial accounts and employee data.

Alongside this, regulation relating to cyber and information security is continuing to tighten globally. As with any legislation, this will continue to drive the behaviour of organisations to achieve compliance, as the potential financial and reputational consequences of not doing so can be significant (as highlighted by the General Data Protection Regulators (GDPR), where fines for non-compliance can be up to EUR 20 million or 4% of the company's global turnover, whichever is the greater). [3]

What can be done?

To manage cyber risk effectively across the enterprise and ensure resiliency, construction firms need a fully integrated, comprehensive plan for managing people, capital and technology risk that extends to your supply chain and the subcontractors.

People risks are the next frontier in cyber risk management. Understanding that technology solutions are only as effective as the people operating and managing those solutions is critical. As highlighted above, people are invariably the weakest link. Here are some steps that can be taken to mitigate people risk:

- Ensure that you have a user education and awareness programme; conduct mandatory cyber risk training for employees and sub-contractors and ensure that security policies are read and adopted;
- Set minimum IT security standards for your suppliers and sub-contractors that may interact with your IT network;
- Enforce the use of PINS and strong passcodes for devices and laptops; and
- As laptops are being constantly taken off site, it is also vital that employees understand the consequences of connecting to public or other untrusted WiFi networks. Appropriate protections need to be in place for these shifts in the working environment.

Ensure that you have a robust technology programme: it is vital that technology solutions are constantly reviewed, monitored and address your business management exposures. Some practical steps are as follows:

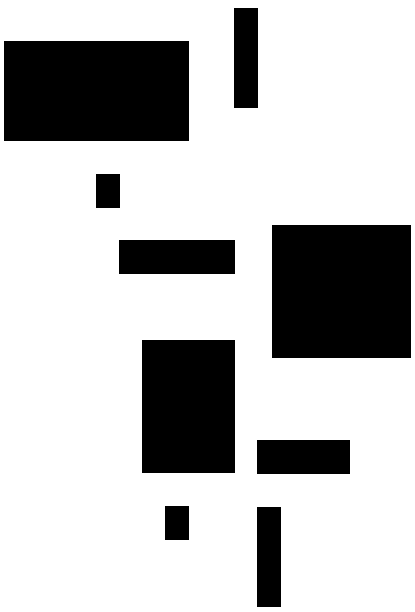
- Invest in the malware protection and detection software;
- Maintain user privileges; keep authorised users to critical systems to a minimum and maintain privileged access accounts;
- Secure configuration; apply security patches are adopted and implanted regularly;
- Consider multi-factor authentication for your most critical systems, these heighten the verification protections for your most critical system;
- Ensure that cyber risk is built into your business continuity and incident response plan and regularly test these plans.

Transfer the risks you can't remove. A robust cyber risk management programme will reduce the probability of an event occurring, as cyber risk can never be fully eliminated. Cyber insurance risk transfer solutions exist to mitigate the financial impact when things go wrong. As a starting point, check your existing insurance coverage; understand what cover you've got and what options are available.

For further information please contact:

Elliot Bryan, BA (Hons), ACII
Account Executive, FINEX Cyber and TMT
+44 (0)203 193 9513
+44 (0)7507 876733
Elliot.Bryan@WillisTowersWatson.com

Jon Thacker
Executive Director, UK Construction Practice
+44 (0) 203 124 8271
+44 (0) 7904 432901
Jonathan.Thacker@WillisTowersWatson.com



3. https://www.gdpr.associates/data-breach-penalties/

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

Willis Limited, Registered number: 181116 England and Wales.
Registered address: 51 Lime Street, London, EC3M 7DQ.
A Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority for its general insurance mediation activities only.

FPS443 WTW-FINEX-306701/03/19

willistowerswatson.com

Willis Towers Watson