A very unwelcome intrusion

17 June 2016

Peter Armstrong discusses a pervasive threat that demands understanding and attention

---

It is sad but true: the property and construction sector needs to confront serious issues to mitigate the risk it faces from cyber attack. In a broad sector that includes rented portfolios, mixed-use developments, large capital projects with dynamic physical construction and associated architectural and survey services, care must be taken to recognise the nature and source of the cyber threat. This means that taking a simple one-dimensional view of data breach is dangerous for our environment.

Important innovations

There are significant innovations in the project context such as building information management systems and building information modelling (BIM), as well as the advent of new building techniques including additive 3D and 4D printing, autonomous construction equipment and drone surveying. Each of these represents significant new potential for vulnerabilities.

Significant data management and security issues prevail for BIM, as everyone in the project lifecycle shares and uses the same core data. Each party in the supply chain is responsible for data in the BIM either as an owner or custodian. However, not everyone will apply the same rigour or invest to the same extent in protecting that data.

Significant data management and security issues prevail for BIM, as everyone in the project lifecycle shares and uses the same core data

As an example, imagine I am a Chinese construction contractor about to bid on an international, large-scale capital project and want to access sensitive commercial or bid-sensitive data. The likelihood is that I am targeting rival bidders' junior partners or specialist service providers in the supply chain for attack. This is a real scenario: according to page 8 of the Mandiant APT1 report Occupying the information high ground: Chinese capabilities for computer network operation and cyber espionage , prepared for the US?China Economic and Security Review Commission by Bryan Krekal, Patton Adams and George Bakos, there are 130,000 cyber warriors in the People's Liberation Army and they are busy supporting Chinese commercial entities around the clock.

Unintentional victims

The simple but flawed assumption that cyber attackers would not be interested in you because you are only the supplier of concrete is dangerous, because you can still be a victim without being the target. Consider the construction stage: autonomous equipment is

now being deployed on site. The control networks for these machines rely on the building information management systems and other data, providing a great opportunity to interfere with day-to-day site operations. At best this means schedule interruption; at worst it could result in the main foundation slab not being poured to the right consistency or configuration.

The construction of a sensitive installation such as High Speed 2 infrastructure, a nuclear power plant or the cable runs for the data centre of a mixed-use estate would all be of very great interest to nation states and organised criminality. The common link, of course, is the building information management systems data that, if accessed, could allow insight into sensitive locations and protection systems. It could also enable changing the configuration for modular manufacturing, so that manufacture does not match the associated schedule impact, or allows attacks on the controlling database for additive 3D or 4D printing on site.

Looking beyond the project environment towards the owner-operated model of property portfolios presents a more hybridised environment of data and industrial control systems. For example, the risk profile of a mixed-use complex with many tenants will be determined by the business of those tenants, whether they are retail outlets, banks or financial institutions. Use of a drone with cyber-attack tools hovering next to the ventilation grille in a tower block, meanwhile, gives access to its heating, ventilation and air conditioning system; the German blast furnace that was seriously damaged in 2014 attests to the danger of a vulnerable system.

Again, the facilities management contractor engaged by the owner to support properties in the portfolio represents a significant area of susceptibility.

CCTV cameras

The contract may well be price-sensitive when CCTV cameras are installed ? which is disturbing because, although they do not have screens or keyboards, they are still addressable computers once they have been connected.

In February, there was another example of a camera manufacturer having its products hacked. This underlines the fact that these cameras must be configured according to IT security requirements. If not, criminals can access the organisation's networks right at the points of entry, where it is acknowledged there are assets or information of great importance to the business and its operations. It is important to ensure that third-party facilities management or engineering contractors apply the same level of vigour as your organisation does to cyber defence.

...the facilities management contractor engaged by the owner to support properties in the portfolio represents a significant area of susceptibility

This is a procurement governance issue that needs to be addressed urgently. If a completed property is attacked through the back-up diesel generator that is owned and operated by a third party, this could have a major impact on that contractor's networks, as happened in the high-profile attack on the American retailer Target in 2013 .

The owner needs to think about the infrastructure provided for the tenants, such as the wifi, cabling, data centre ventilation and automated building management systems. To what degree do these installations represent upstream vulnerabilities and how do we

mitigate the associated exposure?

These observations illustrate that cyber exposure is a major issue. We need to understand what it means for individual organisations and the sector in the context of joint responsibility. The whole is as strong as the weakest link, and there are a lot of links in the value chain.

Risks and mitigation

Organisations need to reflect on their treatment of cyber exposure. For every other danger, an organisation first quantifies the likelihood then makes informed choices about the deployment of its capital by balancing mitigation, retained (and funded) risk and risk transfer. Very little, if anything, is spent on combating cyber attack, although a lot may be spent on consultants to help firms understand vulnerabilities, and then even more on strategies to reduce the possibility.

So what should you be doing? Put simply: treat cyber attack the same as all other risks.

First, quantify and understand the location of the exposure peril. If an organisation has already identified project vulnerability of $100m and risk of cyber attack doubles the probability of occurrence, the exposure is in fact $200m.

Cyber risk enables, accelerates and amplifies existing exposures, and organisations need to understand where their incremental peril resides to decide how best to address this

Second, knowing the location of the incremental risk enables the organisation to reconsider its decisions about the speed of mitigation spend, scale of retained risk (perhaps reviewing funding treatment, maybe using a captive), and whether or not it has bought big enough limits for property or casualty in this case.

Cyber risk enables, accelerates and amplifies existing exposures, and organisations need to understand where their incremental peril resides to decide how best to address this, which is why there is an increase in cyber liability insurance. The products are principally designed to provide first-party cost offset for recovery from a successful breach. They can provide for technical expertise to contain and remediate the breach, for PR and legal support for engagement with customers, regulators and credit-monitoring services for third parties who may be affected by data theft. The scale of capacity and the role of the product relevant to the challenge are a sensible addition to the portfolio, which now reflects more meaningfully the overall scale of incremental exposure consequent on cyber vulnerabilities.

The EU recognises the significance of the probability of successful cyber breaches in its approach to the new General Data Protection Regulations (GDPR) , scheduled for ratification this year. Current legislation assumes that, in the event of a successful breach, the organisation must have done something wrong. Under the new legislation, the assumption is that breaches are inevitable; therefore, the question is to what degree were they aggravated by the organisation's actions or inactions. In the most aggravated cases, penalties will be draconian: a ?77m fine or 2?5% of global turnover, whichever is greater.

Peter Armstrong is Executive Director of Cyber for Willis Towers Watson Global

Further information

Related competencies include: Data management

This feature was taken from the RICS *Property journal* (May/June 2016)