Closed-door policy

1 August 2017

The increasing use of data in building information modelling and other applications requires robust cyber defence measures, warn Emma Vigus and Philip Tansley

---

The Ipsos MORI Cyber Security Breaches Survey 2016 reveals that only 29% of surveyed companies have cyber-security policies and just 10% have formal incident management plans. Given the lack of preparedness, 65% of respondents said they had detected a cyber-security breach or attack in the preceding year.

The 2016 Crime Survey for England and Wales exposed online fraud as the most common crime in the UK. It is more prevalent and complex than domestic burglary, with criminals using methods from malware to spyware to exploit data for financial gain. In addition to the criminal threat, human or hardware error continues to be a key cause of data loss.

Leaving doors unlocked

Unless an organisation is specifically targeted, which is rare, cyber criminals indiscriminately ?knock? on lots of system ?doors?. When they find one open ? an easily accessible system ? they enter. Very few of us leave our house unlocked, and yet many leave the virtual door to their business ajar.

The impact of a traditional property break-in is immediately obvious, but that of a cyber breach is much harder to spot. The initial electronic break-in may go undetected; its effect may be difficult to ascertain, but an immediate and informed response can make a significant difference to the severity of the outcome, and this is why cyber-liability insurance policies are so valuable.

Covering your buck

Perhaps because of the use of the term insurance and the big numbers cited in press coverage of cyber attacks, the value of cyber-liability cover is generally assessed on its ability to remedy a financial loss. As a result, the buying decision is heavily influenced by whether or not that loss would be covered by another form of insurance, such as professional indemnity insurance (PII). Because it often can be covered in this way, firms are understandably reluctant to buy a stand-alone cyber policy.

A firm that purchases, for example, an RICS-compliant PII policy should continue to look to that policy for indemnification from third-party civil liability claims arising from the conduct of professional business. This would include a claim from a client who has lost money as a direct result of a cyber attack against your business. PII policies are, however, largely untested in terms of their response to cyber attacks and cover may not always be available.

Furthermore, unless your PII policy contains a first-party fidelity extension, it is unlikely to offer any protection for loss of your business?s own funds. This leaves a potential exposure to electronic funds transfer fraud, ransomware and cyber extortion, which are expected to be the most prevalent cyber threats of 2017.

Cyber-liability insurance provides 24/7 access to an incident response team that will help manage everything from communication with your clients and employees through to the provision of identity theft mitigation services and assistance with managing your reputation. The team will collectively ensure your business is fully operational as soon as possible, which is critical in the case of a ransomware attack.

Very few firms have access to this expertise in house, and equally few will know which third-party providers to approach. A cyber-liability policy will not only ensure you know where to turn, it will also cover the cost.

Cyber-liability cover is relatively inexpensive in the UK at present. Until recently, there have not been many claims, and our regulation and litigation is several years behind the USA?s. As claims increase, however ? which they inevitably will ? insurers are likely to give greater scrutiny to a firm?s approach to risk management.

In many cases, a little thought will help you identify which aspects of your business are the most vulnerable and how you can manage that risk. Where you do not have the necessary expertise in house, a growing number of consultants and government schemes are available to help assess and manage risk, such as Cyber Essentials .

Complex exposures

However, it may be less obvious how to protect yourself where the potential exposures are in a complex system such as building information modelling (BIM). Whichever BIM platform is used and irrespective of where it is hosted, all project participants need to be aware of potential cyber-security issues.

The most obvious of these is the loss or corruption of data held on the platform, whether accidentally or maliciously caused. Plainly, this brings a risk of significant delay and additional cost, even where data can be replicated or restored. Ransomware attacks ? which can encrypt a BIM database if left unchecked ? are the most common form of cyber attack, a trend that is forecast to continue.

Such risks also raise the potential for contractual penalties, or litigation for project delays or breach of the responsible party?s obligations to keep data secure.

Intellectual property

BIM data is likely to be commercially confidential or proprietary. Accordingly, its loss or disclosure creates a significant first-party risk, and the potential for the owner of those intellectual property rights to face third-party exposure.

BIM data is likely to be commercially confidential so its loss or disclosure creates a significant first-party risk

Increasingly, regulated personal data is held in a BIM platform. Unauthorised access to it has various regulatory implications, most notably the need to evaluate whether it must be disclosed to the Information Commissioner?s Office (ICO), and may occasion regulatory enforcement or enforcement and privacy actions by consumers. Bear in mind, too, that the increasing power of analytics software means BIM data that maps the behaviour of the occupants of a building may, in certain circumstances, become regulated as well.

A significant data breach may have other regulatory implications: for example, the Architects Code requires that adequate security precautions are in place to safeguard clients? data. The regulatory burden will only increase with the advent of the new General Data Protection Regulation (GDPR) which brings with it compulsorily notification obligations and increased fines of up to ?20m or 4% global turnover in the most severe cases.

Specific risks

These risks manifest themselves in different ways to different project participants. Industry standards such as the Construction Industry Council (CIC)?s BIM Protocol and PAS 1192-5 require the appointment of a BIM information manager. For all but the largest projects, this role is likely to be taken by the design lead or project lead, although it is beginning to be outsourced to specialists, and that trend is likely to continue.

The information manager has overall responsibility for establishing and maintaining the BIM platform, which also covers cyber security. This includes ensuring that, when established, the platform hardware, software and system architecture are sufficiently robust to withstand cyber attack, as well as mandating the protocols and procedures to be followed by BIM users, such as implementation of plans for information management and breach response.

Once the platform is up and running, the information manager has a continuing responsibility to ensure that it operates properly, monitoring adherence to procedures and implementing necessary updates and security enhancements. If there is a breach, the information manager will be the most likely subject of any ensuing liability claim.

Ultimately, however, project security measures will be mandated by the employer according to the sensitivity of the project. The employer?s main exposure arises from its responsibility for appointing a qualified information manager; failure to exercise this responsibility properly could make the employer liable.

Every project member with access to the BIM system shares responsibility for protecting platform security, though. Principally, this will mean they each adopt high standards of cyber security to ensure that issues such as unauthorised access do not arise from their failure to follow agreed processes or adhere to basic security standards.

Risk v reward

The use of any new technology presents cyber risks, and though BIM is no exception, the benefits of it should outweigh the risks. These should be managed in a proportionate way. The CIC and PAS guidance, particularly the triage process set out in PAS 1192-5, are very clear that the level of cyber-security precautions depends on the level of risk in particular cases.

One of the main lessons emerging from cyber-security issues in the automotive and engineering industries is the importance of designing systems with cyber security in mind from the outset, and privacy by design will become a regulatory requirement under the GDPR. It is also critical that cyber risk is recognised and managed at board level.

The most basic protection available is to be more security-conscious. It is important to train staff and introduce breach response plans and information security policies that are reviewed on a regular basis. You must also ensure that you understand any regulatory requirements, such as whether registration with the ICO is necessary under the Data Protection Act 1998 .

As a last line of defence, good-quality cyber insurance policies start at just a few hundred pounds ? less than a typical home insurance policy. In contrast, the cost of managing a breach can easily run into hundreds of thousands.

Emma Vigus is Director of Professional Indemnity at Howden Insurance Brokers and Philip Tansley is Legal Director at RPC and co-founder of its ReSecure cyber incident response service

Further information

- Related competencies include Building information modelling (BIM) management
- This feature is taken from the RICS *Building control journal* (June/July 2017)