COMMERCIAL BRIEFING

Cyber insurance requirements in commercial contracts: getting it right

Cyber risks are rarely out of the news at the moment. Cyber incidents have the capacity to cause many different types of loss (*see feature article "Cyber security: top ten tips for businesses", www.practicallaw.com/3-621-9152*).

While most people are familiar with ransomware attacks such as WannaCry in May 2017, which caused widespread disruption to many organisations worldwide including the NHS, there are also examples of cyber attacks resulting in physical damage to property, such as when hackers disrupted the control systems of a blast furnace at a steel mill in Germany, causing significant damage (*see News brief "Ransomware cyber attacks: lessons learned at last?", www.practicallaw.com/w-009-3512*).

The increasing use of technology to control plant and operations remotely means that these risks are likely to remain very much live. There is also the risk of direct financial loss, such as the $81 million Bank of Bangladesh cyber heist in 2016, as well as losses resulting from large-scale data breaches, such as the one that affected Equifax from May to July 2017.

Insurance coverage exists for at least some aspects of cyber risks in the UK market. Given the range and diversity of risks that may arise, there are some key issues for businesses to consider when it comes to insuring against cyber risks in commercial contracts.

Purpose of insurance

It is common for commercial contracts to require that one or more parties obtain insurance. Of course, the fact that a contract requires insurance to be taken out does not mean that the insurer will necessarily pay out on the occurrence of a particular event. However, the existence of insurance cover can be a good start to managing a variety of risks, including that one party cannot:

- Meet third-party claims and the claims are therefore redirected at the other party's business.
- Afford to rebuild its damaged property or plant and is therefore unable to perform its side of the contract.
- Meet a damages claim made by the other party's business.

A party to a contract that does not comply with a requirement to procure insurance could face a claim for breach of contract, and possibly contract termination, even if no loss has yet occurred. This should incentivise parties to comply with the contract. In addition, as a matter of practicality, the availability of insurance is likely to assist survival of the contract or project in the event of a major incident.

The more onerous the insurance requirements, however, the greater the cost to one party or both parties. Accordingly, when it comes to cyber risks, it is important to consider with some care what insurance should be required and how specific the requirements should be (*see feature article "Cyber attacks: shoring up the defences", www.practicallaw.com/3-525-0011*).

Defining the cover

Some types of insurance are well understood. For example, if a contract provides that public liability cover is to be obtained, a party can be reasonably confident that the cover would include third-party cover for legal liability for damage to persons, property, or both, but it is likely to exclude or limit liability for strict contractual liability or pure economic loss. It is likely that this type of policy will include loss or damage within the policy period so that there is no imperative to require that the insurance be held for any period after the contract is completed.

Equally, professional indemnity cover will usually cover legal liability to third parties arising from professional services, and will usually cover claims made in the relevant policy period, so it is usual to see a requirement that the policy cover will be kept in place for either six or 12 years following the end of the contract, depending on whether liability arises from a simple contract or a deed.

First-party property cover is again generally well understood to cover physical loss or damage within the policy period.

In each of the above types of cover, it should be fairly straightforward to draft the contractual provisions setting out the key acceptable terms and exclusions for each type of cover, and there is unlikely to be much crossover or overlap between the different insurances.

Cyber risks defy such neat categorisation. A cyber incident could give rise to a whole raft of different losses, both first party and third party, such as:

- First-party losses, including: loss of physical data (if the data are destroyed); loss of funds (if they are diverted into other bank accounts); physical damage to property; pollution or injury to personnel (for example, if access is obtained to centrally controlled plant or equipment, resulting in breakdown or fire); and loss of business either directly resulting from a loss of data, or due to an outage following property damage or from reputational damage flowing from the security breach.
- Third-party losses, including: liability to third parties if their data are made public or if the loss of data causes financial losses to them (either of which could result in a class action); liability to owners of neighbouring property if a collapse or fire at the property causes damage; and liability through breach of contract if the insured is unable to honour its obligations to third parties.
- Legal costs and fines arising from regulatory breaches (*see feature article "Cyber security: litigation risk and liability", www.practicallaw.com/1-568-4185*).
- Costs arising from claims by shareholders if any acts or omissions of directors and officers in managing the risk have resulted in losses to the business.

Determining which risks are the most likely will depend on a range of factors, including: the likely mode of attack; the resilience in the

Example insurance scenario

In the following example, a contract simply requires that "annual cyber cover be obtained by Party A in the sum of £10 million." This clause may leave open a range of questions, such as:

- Whether the insurance is required to cover:
  - the loss of data needed to complete the contract;
  - the loss of third-party data;
  - damage to property needed for the performance of the contract;
  - damage to third-party property; and
  - regulatory fines and costs.
- The period for which cover should be obtained.
- Whether it is sufficient for this cover to be part of cover afforded by various policies, or whether there must be ring-fenced cover for £10 million.
- What terms, conditions and exclusions are acceptable.

The parties may have very different ideas as to what the contract requires. The result may be that:

- Uninsured losses arise that endanger the contract.
- Party B may be unable to prove a breach of the contractual requirement to obtain the insurance. This may affect Party B's termination rights as well as damages claims.
- Party B may be deprived of the chance to identify and manage the risk by an alternative method.
- The price of the contract may be increased because Party A interprets the requirements very widely.

systems; the extent and the sensitivity of the data held; and the plant and machinery used and their location and mode of control. The reality is that reputational fallout from a data breach raises a quite different risk profile to the losses which could flow from an explosion at a plant in a densely populated area.

Cover for cyber risks might accordingly be found in a number of different insurance policies. Depending on the applicable exclusions, it might form part of both first-party property and third-party liability policies. There may also be a free-standing cyber policy which seeks to provide cover for some of the cyber risks to which an entity may be exposed (*see box "Example insurance scenario"*). Depending on the nature of the cyber incident, any cover or exclusions for terrorism, war or similar risks may also be relevant to whether the insurance will pay out on a particular claim.

Setting out what is required

To manage these risks, businesses should consider setting out in a reasonable amount of detail what types of risks the parties are expecting the cyber insurance to cover.

It is important to keep in mind that the market is continuing to develop in this area. Accordingly, what is available on economic terms may be different now than in a couple of years' time. For a short-term contract, this may not be problematic but, for longer term contracts, it may be prudent to build in some review points. While it is not unusual for contracts to provide that insurance need only be obtained "so far as reasonably available on commercial terms", that may not be a complete solution in circumstances where what is available in the market may increase, rather than diminish, over time.

The alternative to setting out precisely what is required at the contract stage is to provide that the terms of the insurance must be acceptable to Party A, and that it is for Party A to accept or reject Party B's proposed insurance cover.

The difficulties with this approach are that:

- There may be sensitivity over the disclosure of Party B's full policies to Party A, or the policies may be subject to confidentiality provisions that prohibit their disclosure.
- Unless careful drafting is used, this approach may mean that Party A has, in effect, decided whether or not the insurance is adequate and, in doing so, has relieved Party B of its obligations to obtain compliant cover.

Insurance is only one aspect of the management of cyber risks but whether a business is required to take out insurance or is requiring another to do so, careful thought is needed to ensure that both parties are clear on what is required.

Sarah McNally and Andrew Moir are partners at Herbert Smith Freehills LLP.