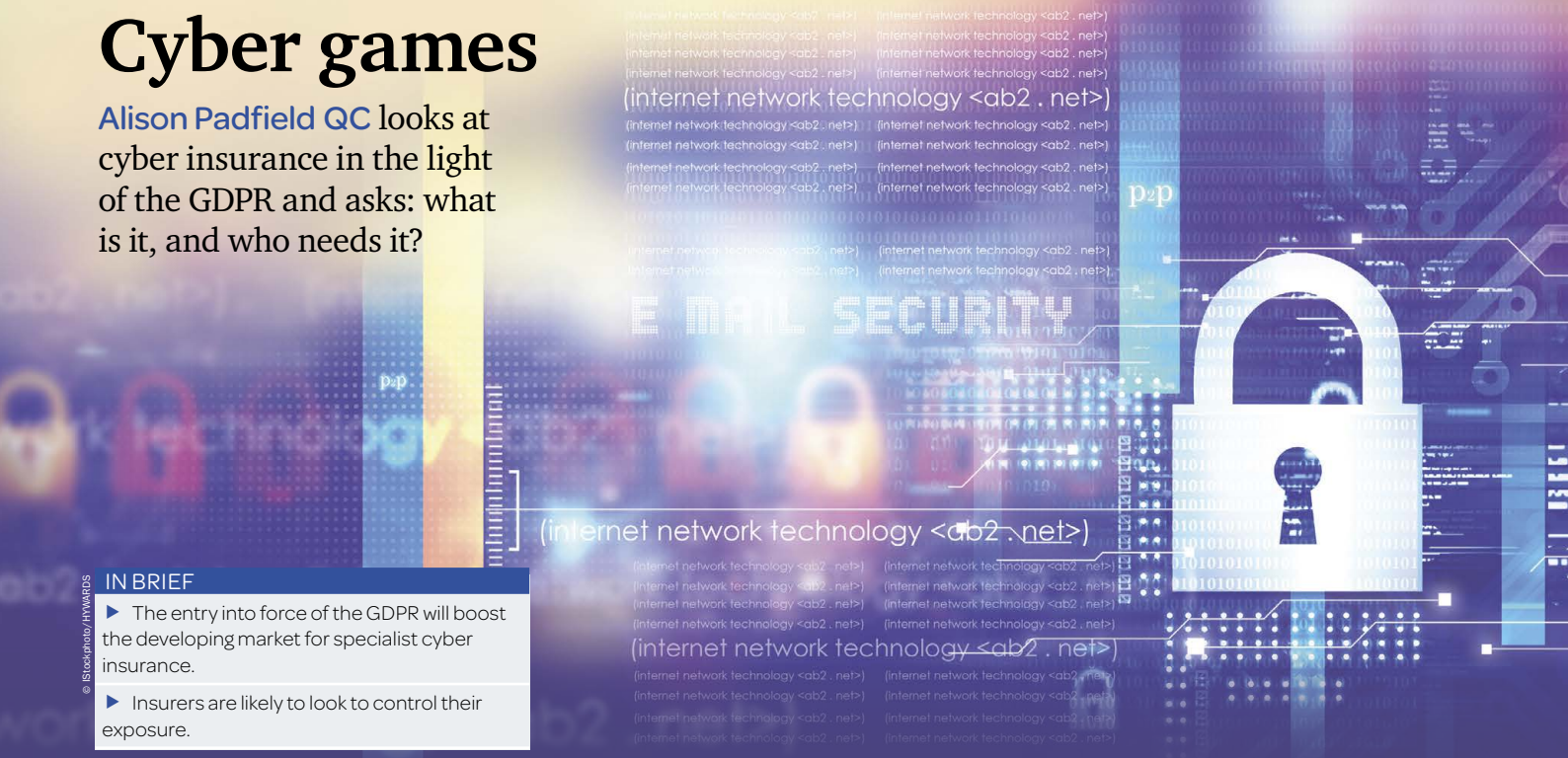
Cyber games

Alison Padfield QC looks at cyber insurance in the light of the GDPR and asks: what is it, and who needs it?



© iStockphoto/HYWARDS

IN BRIEF

- The entry into force of the GDPR will boost the developing market for specialist cyber insurance.
- Insurers are likely to look to control their exposure.

The General Data Protection Regulation (GDPR) entered into force in English law on 25 May 2018 amid huge publicity. The reporting obligations under the GDPR include reports of serious data breaches to the supervising authority within 72 hours (Article 33) and to affected data subjects (Article 34). The GDPR also facilitates group actions (Article 80) and increases the ceiling for fines to €10m or €20m, or 2% or 4% of total worldwide annual turnover, depending on the type of breach (Article 83). Against this background of more extensive reporting obligations and the encouragement of group actions, the volume of civil claims and the number of fines imposed by the Information Commissioner's Office (ICO) are likely to increase. Civil claims may include not only damages for financial loss, but also for non-financial loss ('non-material damage') such as distress and inconvenience (Article 82). Businesses and those who run them will be reaching for their insurance policies. When they do, what might they find?

Cover for malicious or deliberate acts

The Prudential Regulation Authority's (PRA's) July 2017 Supervisory Statement on Cyber insurance underwriting risk (SS4/17) divides cyber related losses into two classes. First, those which emanate from malicious acts such as cyber attack or infection of an IT system with malicious code. Second, those which emanate from non-malicious acts such as loss of data, accidental acts or omissions. This highlights an important point, which is that data breaches may be deliberate or accidental. But whether any individual breach is deliberate or accidental may depend on perspective: a deliberate data breach by an employee may be accidental from the point of view of a business.

This issue has arisen previously in the context of insurance against liability for civil claims for damages for bodily injury. In *Hawley v Luminar Leisure Ltd* [2006] EWCA Civ 18, a nightclub was held to be entitled to an indemnity against its vicarious liability for bodily injury inflicted by a door supervisor. The Court of Appeal said that whether the liability was covered was a question of construction of the policy wording, including its commercial purpose and whether the state of mind of the employee should be attributed to the insured. Taking all those factors into account, they decided that the infliction of the injuries by the employed door supervisor was 'accidental' within the meaning of the policy.

Even where a policy does not provide that liability is in respect of 'accidental' data breaches, an insured may find that it is not covered for a deliberate breach. This is because insurance by its very nature provides cover for chance events (sometimes described as 'fortuities'), not deliberate acts. Whatever the terms of a policy of insurance, it will not be construed to provide cover against deliberate acts by the insured.

'Silent' cyber insurance

Cyber losses may be covered expressly in a policy of insurance. The PRA refers to this type of insurance, from a regulatory perspective, as 'affirmative' cyber cover. But cyber losses may also be covered under a policy of liability insurance if it provides broad cover for liability for financial loss, subject to a series of stated exclusions. This is known as 'silent' cyber cover (although the PRA prefers the term 'non-affirmative'). This is because the policy does not explicitly include or exclude cover for cyber risks, but the insuring clause is broad enough to respond to a cyber incident and there is no applicable exclusion.

In liability insurance, this is unlikely to apply to a public liability policy. This is because a public liability policy provides insurance against liability for property damage or personal injury. Unless there is an express extension of cover, a public liability policy does not provide insurance against pure financial loss suffered by third parties.

But professional indemnity policies do cover this type of loss, and may provide silent cyber cover if there is a broadly worded insuring clause and no applicable exclusion. Relevant exclusions might be, for example, for liability arising out of viruses, hacking or denial of service attacks. Even in the absence of a specific exclusion, liability arising from a deliberate data breach, or a denial of service attack, might be excluded by a widely drawn terrorism exclusion. This would depend on whether the insurer could prove the purpose of the breach or attack, as a terrorism exclusion might exclude acts

'designed to influence the government of any nation' or 'in pursuit of political, religious, ideological or similar purposes to intimidate the public'.

Insurability of 'administrative fines'

So much for liability for civil claims. What about 'administrative fines' imposed under Article 83 of the GDPR? What are these fines, and are they insurable as a matter of English public policy? This depends on the application of the *ex turpi causa* principle. This is a slippery concept, and the survival of this Latin legal phrase probably reflects the difficulty the courts have found in defining and applying the principle. But the particular aspect of the *ex turpi causa* principle which is relevant here was considered and explained recently by Lord Sumption in *Les Laboratoires Servier v Apotex Inc* [2014] UKSC 55.

Lord Sumption, with whom the majority of the Supreme Court agreed, said (at para [25]) that: 'The *ex turpi causa* principle is concerned with claims founded on acts which are contrary to the public law of the state and engage the public interest. The paradigm case is… a criminal act. In addition, it is concerned with a limited category of acts which, while not necessarily criminal, can conveniently be described as "quasi-criminal" because they engage the public interest in the same way. … [T]his additional category of non-criminal acts giving rise to the defence includes… the infringement of statutory rules enacted for the protection of the public interest and attracting civil sanctions of a penal character, such as the competition law considered by Flaux J in *Safeway Stores Ltd v Twigger* [2010] Bus LR 974.'

Safeway Stores Ltd v Twigger concerned a claim by an employer against its employees for an indemnity for fines imposed for breach of the Competition Act 1998. Flaux J decided that the principle of *ex turpi causa* was engaged. There was no appeal against this aspect of the decision, and it was implicitly approved by Lord Sumption in the Supreme Court. The Court of Appeal reversed Flaux J's refusal to strike out the claims on the grounds that the companies were personally liable to pay the penalties and it would be inconsistent with that liability for them to be able to recover an indemnity from their employees.

Article 83 of the GDPR provides that each national supervisory authority shall ensure that the imposition of administrative fines shall in each individual case be 'effective, proportionate and dissuasive'. It also provides that when the national supervisory authority is deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, due regard shall be given to a series of factors. These include the intentional or negligent character of the infringement; the degree of responsibility of the controller or processor; any relevant previous infringements; and any other aggravating or mitigating factor applicable to the circumstances of the case. It seems likely that administrative fines for data breaches under the GDPR will be characterised by the courts as 'quasi-criminal' and 'the infringement of statutory rules enacted for the protection of the public interest and attracting civil sanctions of a penal character' as described by Lord Sumption in *Les Laboratoires Servier v Apotex Inc*.

Investigation & defence costs

Nonetheless, there may be valuable cover under D&O (directors' and officers') or similar insurance policies. These policies typically provide cover for the costs of an investigation and for criminal defence costs, and provide that this cannot be withdrawn until the insured person has entered a formal admission or has been found to have committed the relevant infraction. The fact that the result of an investigation may—eventually—be the imposition of an administrative (or indeed criminal) fine or penalty does not preclude the payment by insurer of the costs of the investigation in the interim. These costs may be significant, particularly if expert IT evidence is required. Early intervention may also mean that a fine or penalty is avoided, or at least minimised.

Although professional indemnity policies may provide cover for the costs of investigations, this will typically be subject to the insurer's prior written consent. The insurer is likely to withhold consent unless the investigation is likely to impact on or give rise to a potential civil claim against the insured which would be covered under the policy.

The future

The entry into force of the GDPR will boost the developing market for specialist cyber insurance. The nature of data breaches means that incidents can have an effect similar to a natural catastrophe: a single incident could potentially give rise to a huge number of claims under very many separate policies. Insurers are likely to look to control their exposure not only by reinsurance but also by narrowing the potential for policies to provide 'silent' cyber cover. They can do this most readily by applying specific, widely drawn, exclusions. Brokers, always in the firing line when something goes wrong, will need to be alert to changes in wordings which affect cyber risk, and draw them to the attention of insureds on placement or renewal. **NLJ**

Alison Padfield QC is a barrister at 4 New Square specialising in commercial law including insurance, & the author of *Insurance Claims* (4th edition, 2016, Bloomsbury Professional), (*www.4newsquare.com, a.padfield@4newsquare.com, @chaffanbrass*).