Pinsent Masons

Insights from our Cyber team

Annual Report 2021

A PURPOSE-LED PROFESSIONAL SERVICES BUSINESS WITH LAW AT THE CORE

CONTENTS

HOW WE CAN HELP

Cyber Innovation
As Europe's most innovative law firm (FT Most Innovative Lawyers 2020 Awards), we have developed a number of cyber-specific tools which we can deploy. These include:

Cyber Readiness – Helping organisations become cyber ready, including through tailored cyber simulation exercises and our innovative incident response solution, Cyturion

Cyber Simulation – Our cyber simulation exercises help to identify areas of improvement in your response plans and raise awareness of cyber risks within your organisation

Breach Response – Multi-jurisdictional breach response services following a cyber event, for all our global sectors

Cyber litigation – Dealing with claims connected to a security incident, personal data breach or cyber event

Strategic leadership and tactical advice – Delivering independent advice and guidance on all information security matters

Human Cyber Index® – Improving your Security Culture, Behavioural Change and Security Awareness Transformation

Breach detection services – Working with industry leaders to provide breach telemetry for your business and brand

Introduction

The past year has seen unprecedented times due to the Covid-19 pandemic which has resulted in a dramatic change to our working lives as we have moved to a "new normal" of home-office working. This has created considerable challenges for IT infrastructure and security, providing greater opportunity for attackers to exploit vulnerabilities, particularly in work-from-home technologies.

We have focussed on three key areas for this year's report based on what we have seen "on the ground" in the last twelve months. **These three areas are:**

1. The Threat Landscape

2. Ransomware

3. Data Subject Claims

We have observed a substantial increase in ransomware attacks. The European Union Agency for Cybersecurity, ENISA, in its recently published report into the cyber threat landscape assessed ransomware as the prime threat for 2020-2021 and described the current climate as "the golden era of ransomware".[1]

Ransomware is one of the greatest threats faced by businesses today, irrespective of sector, with attacks now commonly taking the form of a two-pronged approach: (1) the encryption of data or systems along with (2) the exfiltration of data coupled with a threat of publication unless the ransom demands are met.

Data subject litigation following on from a cyber incident is also significantly on the rise. There was significant concern that victims of cyber-attacks would face mass actions from data subjects seeking compensation under data protection legislation. However, the recent UK Supreme Court decision in *Lloyd v Google* and other case-law, may have diluted that risk, in the UK at least. We wait to see how this area of law develops.

As ever, being as prepared as possible for a cyber-attack is of critical importance. From having well-rehearsed incident response and business recovery plans in place, to ensuring that IT security is taken seriously, with senior stakeholder involvement and accountability, are critical. The consequences for an unprepared organisation can be devastating.

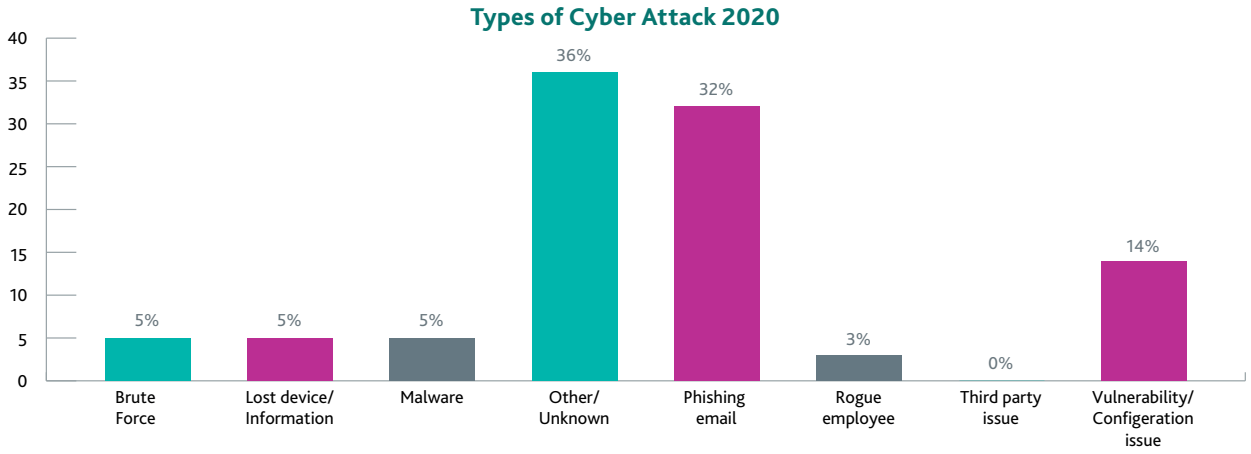
As with previous years, this report has a UK focus but draws upon the experience of our cyber team colleagues from across Europe.

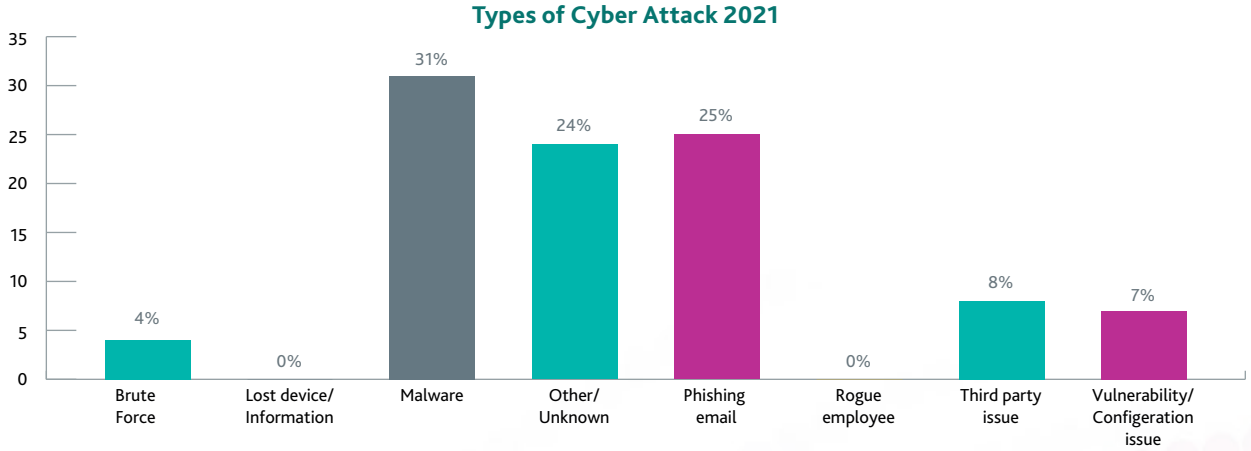
David McIlwaine
Head of Cyber, Partner, London
+44 (0)20 7490 6224
+44 (0)7956 569 887
david.mcilwaine@pinsentmasons.com

1. The Threat Landscape

Cyber criminals continue to develop their methods to gain access to and exploit IT systems. The Covid-19 pandemic which resulted in enforced home working around the globe provided greater opportunity for attackers as an increasing number of functions were moved online at very short notice, resulting in overloaded IT teams, stretched security monitoring protocols / software and slower incident detection. We have seen a number of serious incidents arising because of a lack of security being applied by organisations when employees are working outside of the normal office environment. Vulnerabilities in VPNs or remote desktop protocols appear to have been more readily exploited when employees are working remotely.

Whilst we have continued to see phishing emails as a common attack vector, there has been a shift, most notably in relation to the propagation of malware leading to ransomware attacks and an increase in clients being affected by third-party / supply chain issues. Contrastingly, the number of incidents caused by lost devices has reduced significantly and is a reflection of a year spent in lockdown with strict travel restrictions.





Phishing and Malware

Phishing emails are still a prominent root cause of cyber-attacks, although there has been a slight decrease in our cases from 32% in 2020 to 25% in 2021. We continue to see phishing emails being used where the end goal is to extract data and deliver malware to encrypt systems as a precursor to demanding a ransom payment. However, phishing emails are also the initial point of intrusion for other forms of cyber attack, including the perpetration of further phishing campaigns or payment diversion fraud attempts.

Some phishing emails are very realistic and authentic. We have seen attackers use more sophisticated methods of phishing campaigns, through the sending of phishing emails from genuine accounts of organisations in a client's supply chain. These can be very difficult to identify the threat. However, we continue to see intrusions arising out of phishing emails, which should be much easier to spot, particularly by individuals who have received phishing awareness training.

The key to guarding against these types of attack remains largely down to educating employees through methods such as conducting simulated phishing campaigns to raise awareness. In addition, we recommend the use of multi-factor authentication across systems, maintaining robust back-ups, and adopting principles of least-privilege and network segregation to protect against an attacker moving laterally through the IT estate.

Third-party / supply chain issues

Additionally, we have seen a marked increase this year in third-party / supply chain issues causing the problems, e.g., where the intrusion originates with a supply chain entity (as was the case with British Airways), with 8% of our cases, compared to 0 in 2020.

There has been a number of high-profile cyber-attacks involving third-party software supply chain issues in the past year, most notably the Solar Winds and Kaseya cyber-attacks. In the Solar Winds incident, attackers inserted malware into software updates. When customers downloaded these updates, they inadvertently downloaded malware onto their systems, which created a backdoor for the attackers to access the customers' systems and deploy further malware.

Similarly, the Kaseya attack involved the leveraging of a vulnerability in Kaseya's Virtual System Administrator software which was used by a number of managed service providers ("MSP") to administer their customers' network. Through this vulnerability, attackers were able to access and encrypt the MSP's end customer systems.

We have also seen a number of ransomware incidents affecting clients' data processors. We advised several clients whose data was impacted in the ransomware attack on Blackbaud, a technology provider that operates and supports the online donation technology platforms and databases for a large number of organisations worldwide. As part of the attack a backup file containing data relating to Blackbaud's clients was exfiltrated by the attacker. We advised several clients on the impact on their obligations as data controllers and consequent reporting obligations under the GDPR as well as other regulatory regimes.

In supply chain based cyber incidents, data controllers are heavily reliant upon the data processor / managed service provider to provide information and support during the course of a cyber event. However, many controllers will also – at an early stage – will want to consider the potential legal recourse against such the third party, particularly in circumstances where there is clear evidence of a vulnerability the third party should have protected against.

Vulnerability / configuration issue

We have also experienced a decrease in cyber-attacks which have a vulnerability / configuration issue as the source of incident. In 2020, this was the source of incident in 14% of cyber-attacks, falling to 7% in 2021. Examples of vulnerabilities include weaknesses in firewalls and running outdated software. Employing a regular patch management and security update policy can help to significantly reduce the risk of exploitation.

We have seen organisations be much more aware of the importance of good logging processes; as such logging can be of critical importance to understanding exactly what happened, and what data may be impacted. That said, the more sophisticated threat actors are particularly good at anti forensic work to eradicate logs. Such activity can make it very difficult to ultimately identify the original point of intrusion.

2. Ransomware

Ransomware attacks are never far from the headlines. There have been a number of very high profile incidents this year, ranging from high-end jewellers, to oil and gas pipelines, to a country's whole health system. It is clear that no organisation – no matter how big – is immune from this threat, and it is one that affects all sectors. We have seen our clients be affected by a range of threat actor groups. Ironically, the well known prolific cyber groups can be something of a known issue; conversely, the proliferation of "ransomware-as-a-service" has led to a large number of new groups coming to light, which can be much more unpredictable.

With financial gain continuing to be the key motivation behind cyber-attacks in the private sector, and the disruption to businesses caused by the Covid-19 pandemic providing an ideal attacking ground, we have seen ransomware attacks increase at a significant rate over the past year. Ransomware is now one of the top form of attacks experienced by our clients, with 31% of our cyber cases this year involving ransomware.

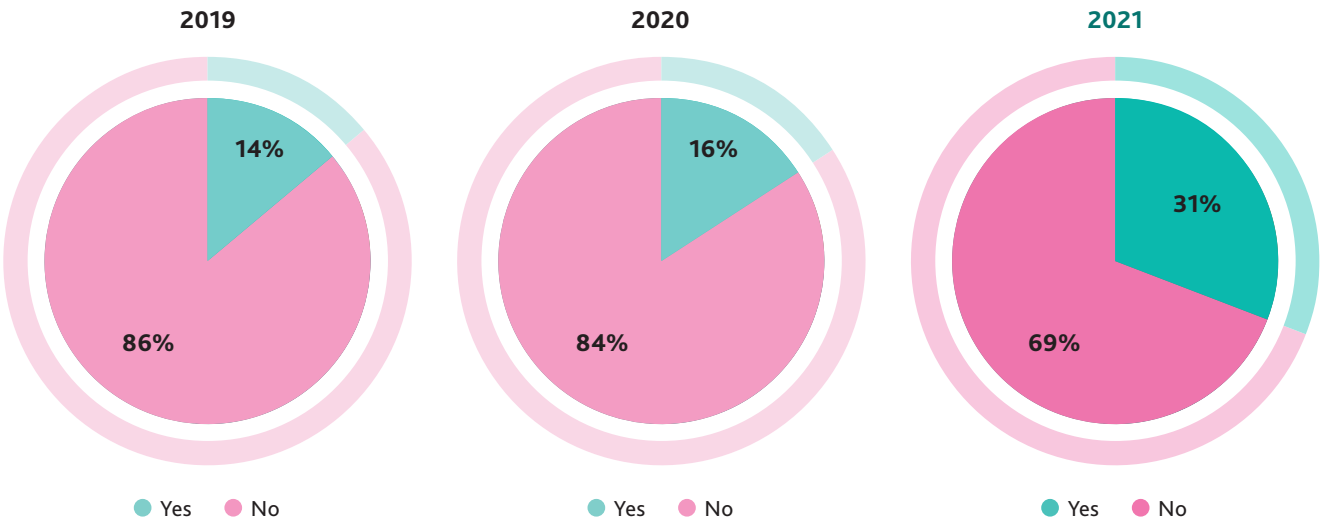
We started to observe an increase in ransomware attacks in our previous 2019-2020 White Paper. However, there has been a very significant increase this year compared to the previous two. Attacks now typically have a two-pronged approach, with attackers first gaining access to our clients' systems and exfiltrating a significant amount of data, only then to encrypt the data and demand payment for the decryption key. Often attackers also threaten to publish the stolen data online or on the Dark Web, as a way of adding more pressure on our clients to make a payment.

At its 2021 conference held in May of this year, the ICO confirmed that it had seen an increase from 13 reported ransomware cases per month to 42 per month that year. At the conference, the ICO emphasised the importance of having policies and procedures in place to help organisations in the event of a successful attack. It went on to say that when it is notified of a ransomware incident, it will start its investigation by looking at the organisation's general GDPR posture, with an initial focus on Article 5 (seven key principles of data protection regime) and Article 32 (the requirement to implement technical and organisational measures that ensure a level of data security appropriate for the level of risk presented by processing personal data).

Whilst in all of our reported ransomware cases in 2021, the ICO closed its investigation without any enforcement action being taken, this is not to say that the ICO does not take ransomware cases seriously. In all cases serious consideration needs to be given not only to the commercial and criminal risk factors in whether or not to pay a ransom and/or engage with the attacker but also, on whether or not there is a duty to report to organisations such as the ICO, other supervisory and regulatory authorities and/or the police, notify the stock market, as well as the data subjects themselves.

A decision to notify the ICO and data subjects (or not to) must be well documented and a risk assessment clearly set out – these steps are direct statutory requirements.

Was a ransom demanded?



The amount of ransom demanded varies but is typically somewhere between $30,000 and $250,000, although we have had some clients who have experienced demands as high as $9.5 million in the past year. Those clients who do choose to pay the ransom, however, often have success in negotiating a lower figure, by an average of 39% through the use of an expert ransomware negotiator.

Amount typically demanded

The amount of ransom demanded varies but is typically somewhere between $30,000 and $250,000, although we have had some clients who have experienced demands as high as $9.5 million in the past year. Those clients who do choose to pay the ransom, however, often have success in negotiating a lower figure, by an average of 39% through the use of an expert ransomware negotiator. However, organisations that do choose to engage with a threat actor group should be under no illusions that this is a quick process; whilst it is difficult to predict, the process can take several weeks to get to a point where a valid decryption key is handed over.

No demand made?

It is important to note that whilst 81% of our ransomware cases over the past year have involved a ransom demand, in the remaining 19% of cases, no ransom payment was demanded at all.

Whilst it may seem strange for an attacker to go to the effort of infiltrating a target's system, exfiltrating and encrypting large amounts of data, only to walk away without making a ransom demand; one explanation may be that on reviewing the data the attacker has realised that it is not particularly sensitive, or is unlikely to cause a high degree of disruption to the target company if unrecoverable, and so there is either a limited incentive for the company to pay the ransom to restore it, or to prevent publication.

Cyber criminals are unlikely to simply pursue only one victim at a time, as they recognise that it is more expeditious to target multiple victims at the same time to see who they can successfully infiltrate and what data they can access. If an attacker fails to leave a ransom demand, it is therefore likely that they have simply moved on to focus their efforts on a more lucrative target. Unsurprisingly, we have mostly observed this with our SME clients, whose services are solely business-to-business and the amount of personal data processed on their systems is limited.

Considerations on whether to engage with an attacker

If a demand is made, the decision as to whether to engage with an attacker and/or make a ransom payment is often a complicated one, involving important commercial, ethical and reputational considerations, as well as complex legal and compliance issues. Typically, we caution against engagement with the attacker if a client has no intention at all to make payment, on the basis that they run the risk of further antagonising the situation, which could speed or worsen the publication process or result in the attacker publishing any communications.

Whilst we guide victim organisations through the various considerations, this decision lies firmly with the business, and of all the cases we handled in this past year, 38% of our clients paid either the amount demanded, or a lower negotiated figure, while 62% chose not to engage at all.

The following factors play a role in the decision making process when considering whether or not to make a ransom payment:-

The extent to which the client's encrypted data can be restored from backups or is available by alternative means. If this is limited, engagement may be needed to obtain the decryption from the attacker to restore the data. This is often the key driver behind decisions to engage.

If there is a credible threat to publish exfiltrated data which is sensitive or high risk, (for example, forensic investigations indicate that sensitive data has been exfiltrated as part of the attack). However, getting a criminal's word that stolen data will not be misused, is unlikely to avoid an organisation having to make relevant regulatory notifications.

Having the financial means to pay the demand, plus the additional third-party professional fees involved. This usually includes the costs of engaging a ransomware negotiator to communicate with the attacker and facilitate the payment, which is typically paid via bitcoin, and forensic experts analysing the decryption key to check it works and is clean of any threats.

If forensic investigations cannot confirm (i) how the attacker 'got in', or (ii) what data has been exfiltrated, the attacker may provide further information if a ransom is paid.

The level of confidence that the attacker will keep their word and not publish and/or will delete the data exfiltrated (even if demand is paid).

Company values, ethos and morality of negotiating with criminals.

Reputational and PR risks, as customers / employees / media may look unfavourably on a payment being made, if this information were made public.

The legality of making a ransom payment. Whilst making a payment is not per se illegal, there are offences relating to money-laundering and/or the arrangements with entities associated with terrorism or sanctioned entities. Specific legal advice must always be taken in the event consideration is being given to paying a ransom demand, and certain notifications may be necessary to UK and other enforcement agencies.

Injunctions

For those organisations that are unfortunate to fall victim of an attack, we often consider with our clients the merits of seeking an injunction. An injunction is a legal order for a person to do something or not to do so. The type of injunction sought can vary depending on its purpose, with the most common, in our experience being to prevent publication of the confidential data by the attacker or anyone else. For example, in a recent case in which we acted, an injunction was obtained prohibiting the use, publication, communication or disclosure of information listed in a confidential schedule.

The problem with cyber-attacks is, of course, that the attackers often remain unknown, and so the identity of the individual(s) against whom the injunction will be sought is not clear. In this regard, the law allows, in certain circumstances, for injunctions to be obtained against "persons unknown", i.e. the unidentified attacker in the context of a cyber-attack.

A cyber-criminal is highly unlikely to engage with the Court proceedings. This is particularly so where quite often the cyber criminals are outside of the jurisdiction of the injunction and in countries such as Russia, North Korea, Iran.

However, the existence of an injunction is of more use against websites (such as blogs, social media sites, and hosting providers) on the surface web, who will be bound by the terms of the injunction once put on notice of it. This can therefore be used as a way in which to limit the scope of publication. Moreover, we have found that obtaining an injunction can also provide a helpful narrative from a PR perspective. However, given that the website must be given notice of the injunction, with the threat of penal action if it does not comply with the terms of the injunction, means it is difficult to use such an injunction against websites on the dark web, which commonly obfuscate their ownership and location.

Ultimately however, obtaining an injunction is not always available, and – when it is – getting one is an expensive undertaking. They are certainly not suitable in every case of ransomware that we have worked on.

US Developments

Whilst the focus of this paper is mainly on the risks presented with paying a ransom under UK law, in our experience it is useful, and indeed often necessary, to also consider the legal obligations that might arise in other jurisdictions. In this regard, it is interesting to note that the United States has observed a similar surge in ransomware cases. In its annual statistics report for 2020[2], the Federal Bureau of Investigation ("FBI") reported a recorded 2,747 complaints related to ransomware, with associated losses of over $29.1million, and in President Biden's words, cyber security now represents "*the core national security challenge*" the US is facing.

It is therefore not surprising that the US Department of the Treasury's Office of Foreign Assets Control (OFAC) has recently issued advisories to highlight the sanction risks to companies who make payments to cyber attackers and encourage full and frank transparency with the authorities. The most recent advisory was issued on 1 October 2021[3] and confirms that businesses that facilitate ransomware payments, including financial institutions, cyber insurance providers, and companies involved in digital forensics and incident response, "*not only encourage future ransomware payment demands but also may risk violating OFAC regulations.*"

OFAC therefore encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations. In particular, the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve a payment to a sanctioned person or sanctioned jurisdiction. In this regard, OFAC has effectively suggested that it may be willing to penalise dealings with sanctioned parties/jurisdictions even where, as with ransomware, it is often very difficult (or impossible) to know who is responsible for an attack or where the money is being sent.

OFAC goes on to say that under its enforcement guidelines it will also consider a company's full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome. It therefore strongly encourages all victims and those involved with addressing ransomware attacks to report the incident to CISA, their local FBI field office, the FBI Internet Crime Complaint Centre, or their local U.S. Secret Service office as soon as possible.

Whilst the focus of this paper is mainly on the risks presented with paying a ransom under UK law, in our experience it is useful, and indeed often necessary, to also consider the legal obligations that might arise in other jurisdictions. In this regard, it is interesting to note that the United States has observed a similar surge in ransomware cases.

3. Data Subject Claims Landscape

Article 82 GDPR codified an EU-wide entitlement to compensation for data subjects that suffer material or non-material damage as a result of infringement of data protection legislation. Further, many member states (as well as the UK) have confirmed that "damage" includes distress, which has further widened the scope of data claims. Under the GDPR (and in the UK), national data protection authorities cannot order compensation – instead, claimants must turn to the courts for that. This has provided the basis for what is a growing tide of data subject claims following on from cyber breaches.

The perfect storm has arisen with an increased awareness by data subjects of their data rights, an obligation to notify data subjects where there has been a personal data breach resulting in a high risk of harm to the individual (under Article 34 of the GDPR), a number of high-profile data incidents, and a focus by claimant law firms to industrialise the process for data subjects to bring actions. Coupled with this is the exponential growth of ransomware which commonly involves exfiltration, and the consequent loss of control of data by the data subjects.

Current landscape

The UK has seen a very significant increase in the amount of litigation by data subjects for compensation under data protection legislation, both where the infringement was allegedly deliberate, such as misuse of personal data by the controller, and where it was not, as in the case of a cyber-attack. To put this in context, every single entity that has received a monetary penalty notice issued by the ICO following a cyber incident that occurred since GDPR has been in force, is now also the subject of data subject claims, including British Airways, Marriott and Ticketmaster. With the exponential rise of cyber-attacks during the pandemic, litigation in this area is expected to increase dramatically. However, the very recent decision of the UK Supreme Court in *Lloyd v Google*[4] (in which Pinsent Masons acted for Google and which we discuss further below) will have a very significant impact on this area of litigation.

In the UK, many of the growing number of data protection-related claims being filed against businesses or that have fallen victim to cyber-attacks are being brought not just under data protection legislation (primarily as a breach of Article 5(1)(f), i.e., failure to take appropriate technical or organisational measures to secure the personal data) but also as claims for breach of confidence, misuse of private information and negligence.

There is still relatively little case law on the appropriate amount of damages payable in a data protection claim. Attempts have been made by claimants in various European jurisdictions to argue that a breach of data privacy rights amounts to a loss of control or a loss of personal autonomy and therefore an interference with fundamental rights, such that compensation should be paid for the infringement of the right itself. However, very recently (on 10 November 2021) the UK Supreme Court unanimously decided in *Lloyd v Google* to reject the notion that every data subject affected by a non-trivial data breach is entitled to an award of compensation for the mere "loss of control" of their personal data[5]. However, that case does not affect the situation where an individual data subject can prove an infringement of data protection legislation and show that they have individually suffered non-trivial loss as a consequence e.g., distress. In this event the data subjects remain entitled to compensation. Nevertheless, there is a paucity of cases on how the damages recoverable should be calculated.

In the UK, the case of *Halliday v Creation Consumer Finance*[6] is often cited by claimants as a benchmark for damages. In that case the claimant recovered £750 for non-material damage, but the court's judgment is very specific to the facts and therefore not as instructive as claimants tend to suggest. However, there are other privacy related cases where the claimant has recovered significantly more damages, for example in *Gulati v MGN Ltd*[7], which related to the newspaper hacking scandal, damages were awarded in excess of £260,000. However, that was an exceptional case involving deliberate intrusion into the private lives of celebrities for commercial gain. There is also *TLT v Home Office*[8] where damages of more than £12,000 were awarded to certain asylum seekers who had suffered loss as a result of the Home Office erroneously publishing asylum seeker data.

Obviously, the concern for data controllers following a cyber incident is that even relatively small damages awards for individual claimants could amount to a substantial amount if high numbers of claimants are successful in bringing claims.

It is not at all straightforward to arrive at a calculation of potential damages. The law in this area is in its very early stages of development. If a data subject has suffered financial loss then that may be recoverable, subject to principles of causation and remoteness. If the data subject has suffered distress, then that may similarly mean they are entitled to compensation. The data subjects may also be able to show some other circumstances specific to their situation which means that they should be additionally compensated.

In addition to damages, litigation rules in England and Wales potentially allow claimants to recover their legal costs reasonably incurred in progressing an action. However, since the Jackson reforms of civil court costs, the ability for successful claimants to recover any success fees (that they pay to their lawyers) and premiums incurred in obtaining "after the event" (ATE) insurance has been significantly curtailed by measures aimed at curbing what was perceived to be a growing litigation culture. One exception to this broad reform was made for the purposes of "publication and privacy proceedings", i.e. claims in defamation, malicious falsehood, misuse of private information, breach of confidence and harassment. Though the scope of this exception was reduced in April 2019 to exclude success fees from being recoverable in publication and privacy proceedings under conditional fee arrangements entered into from that point onwards, the exception otherwise remains in place in relation to the recoverability of ATE premiums in publication and privacy proceedings.

It has therefore become common practice for claimants to bring claims in misuse of private information and breach of confidence alongside claims for breach of data protection legislation, with a view to recovering an ATE premium if the claim is successful. This has ramifications for the commercial dynamics of such cases where the amount claimed is often small in comparison to the cost of the ATE premium. In addition, claims involving breach of confidence must be commenced in the High Court, which has led to the Media and Communications List at the court becoming heavily populated with these low value claims. One claims management company issued close to 150 such claims in the first half of 2021 alone.

The recent case of *Warren v DSG Retail Ltd*[9] has changed the landscape in relation to (i) the grounds of claim maintainable in cyber-related litigation; and (ii) the recoverability of ATE premiums for these claims. In his claim, Darren Warren was seeking to recover damages for distress caused following a cyber incident. He advanced his claim under various guises, arguing that there had been breach of confidence, misuse of private information, negligence and breach of various provisions of the Data Protection Act 1998 – including the seventh data protection principle under the Act which concerns data security (DPP7) – the equivalent of Article 5(1)(f) under GDPR. DSG Retail Ltd (represented by Pinsent Masons) applied to the court to strike-out of all the claims made other than that under DPP7. The judge struck out Warren's claims in both breach of confidence and misuse of private information, finding that both causes of action require some form of "positive conduct" by a defendant and that this was lacking in a cyber-attack scenario, i.e., the defendant had not disclosed or misused the data at issue, but was itself the subject of a criminal act.

The judge in this case also confirmed that a duty of care relating to data security does not arise on data controllers under the common law, and there is no need for the law to be extended in that way given that such a duty already exists under data protection legislation. As such, any claims should be rooted in GDPR rather than in the law of negligence. Although the case was decided by reference to the 1998 Act, the same points will apply to claims under the current UK GDPR regime.

This decision is a positive development for those defending data breach claims as it means that it will no longer be possible to contend that ATE premiums are recoverable from unsuccessful defendants in such cases and largely should remove misuse of private information, breach of confidence and negligence as grounds of claim. As such, the need for claimants to incur an irrecoverable ATE premium up front – which can be 50% or more of the claimant's estimated losses in such cases – may mean a substantial reduction in such cases in future. For the moment, however, it remains too early to tell.

In addition to damages, litigation rules in England and Wales potentially allow claimants to recover their legal costs reasonably incurred in progressing an action.

Mass Actions in the EU

In **England and Wales**, there are a number of routes available by which mass or collective actions may be brought. First, multiple claimants may group together to bring similar actions on the one claim form, and we see this occurring reasonably frequently. Secondly, the court may order a Group Litigation Order (GLO) allowing the individual claims made by multiple individuals to be managed together. Finally, a representative action may be available pursuant to Civil Procedure Rules (CPR) 19.6 — the "opt-out" class action, i.e., all individuals that meet the class criteria are included (even without their knowledge or approval) unless they opt-out. However, the Supreme Court decision in *Lloyd v Google* means that a representative action is unlikely to be an appropriate vehicle for data protection claims for damages, as each individual must prove the infringement and the resulting non-trivial damage they have suffered.

The most significant GLO in the data privacy space is that affecting British Airways. There are in excess of 20,000 claims proceeding under that GLO — far more than is typical for GLOs generally[10] . That said, a GLO is an "opt-in" procedure (i.e., the claimant must take a positive step to opt-in to the litigation), so quite different from the "opt-out" class actions which are commonplace in the US (where the claimant need take no step, but benefit from any damages awarded to the class of claimant). As a result of *Lloyd v Google*, it may be that the GLO is the preferred route to bring claims for volumes of individuals.

The Supreme Court's decision in *Lloyd v Google* brings the position on representative actions firmly into line with the outcome of the UK government consultation conducted last winter on the possibility of introducing a bespoke procedure for opt-out class actions in the data protection space. The Department of Culture, Media and Sport said that the case for introducing an opt-out procedure into law was not strong enough: "*There is insufficient evidence of systemic failings in the current regime to warrant new opt-out proceedings in the courts for infringements of data protection legislation, or to conclude that any consequent benefits for data subjects would outweigh the potential impacts on businesses and other organisations, the ICO and the judicial system.*"

In **France**, class actions are still largely uncommon. French class actions, or "group actions", became available to the data privacy field only in 2016. However, the procedure is difficult in a number of respects, which impact the benefits for plaintiffs. Group actions proceedings are very lengthy — it often takes years to obtain a first ruling — and such actions are only available to limited categories of plaintiffs, commonly representative unions and certain categories of associations. Further, damages will not be assessed until any appeals of liability or procedure have been exhausted, which again delays the action significantly.

Because of these issues, group action proceedings have failed to attract victims in the field of data privacy. Although some were brought to court during the last few years, France has yet to see distinct results from such group actions.

The **Netherlands'** regime for class actions was reformed in early 2020, allowing for "opt-out" style class action claims for any type of damages. Some 27 class actions claims have been filed to date, including the multibillion class action damages claim against Oracle and Salesforce for alleged use of cookie-data in breach of the GDPR. Whilst damages are limited in the Netherlands, it still appears to be a favourable jurisdiction for class actions due to its legal system, and this has also been picked up by litigation funding companies. The outcome of the Oracle and Salesforce matter will likely determine whether class actions in the data space will become the next big thing or not.

In **Ireland**, section 117 of the DPA introduced a mechanism for "opt-in" class actions but there is currently no legislative framework to allow collective redress or mass actions in Ireland. Instead, such collective redress actions typically proceed before the courts as 'test cases'. The damages covered in a test case need to be identical or very similar to other cases seeking to recover damages pursuant to the test case.

Pending domestic legislative change to introduce a formal mass action procedure and the introduction of the EU Collective Redress Directive, the use of 'test cases' will still predominantly be used for privacy class actions in Ireland. The use of test cases is viewed positively by the courts and parties to litigation. However, as each case is determined on its own merits, there is a risk that subsequent proceedings after the test case could be distinguished by the parties. Nevertheless, typically all parties will look to the decision in the test case to consider how to resolve the remaining cases and parties are more likely to avoid the need for further court hearings on matters with similar factual and legal issues in dispute.

The Supreme Court's decision in *Lloyd v Google* brings the position on representative actions firmly into line with the outcome of the UK government consultation conducted last winter on the possibility of introducing a bespoke procedure for opt-out class actions in the data protection space.

In **Germany**, mass actions are on the rise. They were long alien to German procedural law, but now both the German legislator and the EU legislator are increasingly creating possibilities to bundle claims of numerous plaintiffs into one proceeding. Existing mechanisms in Germany include actions brought by associations or groups acting in the interest of a group of affected individuals or entities. In particular, the "model declaration" action (which was introduced in 2018 and follows the "opt-in" principle) may be an option for cyber-related litigation. Whilst a court cannot award damages to the plaintiffs based on such an action, it can find that claims for damages are in principle justified, meaning that, generally, the plaintiffs may simply proceed to enforce their damages claims in individual proceedings (albeit that each would have to prove his or her individual damage suffered).

In addition, claims may also be bundled based on general rules of the German Code on Civil Procedure. These rules permit multiple parties to sue jointly in certain circumstances involving similar claims or for the court to pull together several individual actions, where they are legally connected or could also have been asserted in a single claim. One example of this model are claims handling platforms pursuing claims against flight operators for delays and cancellations. This model initially has been met with suspicion by the courts, however the German Federal Court of Justice as well as the German legislator have confirmed its legitimacy.

Existing mechanisms in Germany include actions brought by associations or groups acting in the interest of a group of affected individuals or entities. In particular, the "model declaration" action (which was introduced in 2018 and follows the "opt-in" principle) may be an option for cyber-related litigation.

Finally, the implementation of the EU Collective Redress Directive in German law will further strengthen mass actions. When transposing the Directive, the German legislator will need to decide between the coexistence of existing mechanisms and an entirely new mechanism, or an amendment of current provisions so that they meet the Directive's requirements. The scheme for model declaration actions currently comes closest to the scheme envisaged by the Directive. In any case it is expected that mass actions according the new will follow the "opt-in" model.

Spain does not have specific legislation governing class actions, but it does have provisions under consumer protection laws that allow the filing of collective actions in certain circumstances. These collective actions are primarily intended to stop illegal practices and to compensate aggrieved parties with damages.

However, as in many member states, the Spanish vision on mass actions is slightly improving, as courts are accepting more mass actions cases. Those making the most progress are those initiated by Consumer and User Associations. Consequently, claimant law firms are encouraging clients to bring more mass action lawsuits, especially in relation to data protection and cybersecurity matters.

It is expected that the impact of the EU Collective Redress Directive will be significant, and will create the opportunity for the Spanish legislator to change the procedural mechanism to make it easier for mass actions to be commenced. We wait to see what changes this brings.

Future Developments

In the UK, the British Airways group litigation will be closely watched, particularly in terms of the effectiveness of the GLO procedure for managing large-scale litigation. It will also be interesting to follow the consequences of *Lloyd v Google*. Several high-profile claims were stayed pending the Supreme Court's judgment, including against Tik Tok, Facebook and Marriott hotels. The judgment, in conjunction with *Warren v DSG Retail*, may well lead to a general dampening of the claims market in this space, with a greater emphasis on the requirement for data subjects to show material damage or distress on an individualised basis.

It is expected that the impact of the EU Collective Redress Directive will be significant, and will create the opportunity for the Spanish legislator to change the procedural mechanism to make it easier for mass actions to be commenced. We wait to see what changes this brings.

Concluding remarks

This year's report has highlighted two key areas: (1) the prevalence and major threat to organisations, irrespective of size and sector, of ransomware and (2) the increasing trend of litigation from individuals whose data has been impacted by a cyber event. Both create a significant risk to organisations, financially and reputationally and serve as a stark reminder of the need for organisations to get cyber-ready and have rehearsed response and recovery plans in place for when an attack inevitably happens.

If 2021 was the year of ransomware, the authors of this report consider that 2022 is likely to be the same. The current threat of ransomware attacks is not going away any time soon. Organisations will find themselves – out of nowhere – thrust into the complex world of managing a business threatening ransom attack. Ultimately, it may well be that governments, policy makers or the insurance industry may step in with measures which go some way to breaking the cyber criminals' business model. Of note, in recent months:

1) There is a discussion in the Netherlands regarding a ban on the payment of ransoms[11]
2) A US led ransomware Task Force set out a number of interesting proposals for combatting ransomware[12]
3) The cyber insurance market is tightening, and this includes proposals to not cover the reimbursement of ransom payments[13]

The debate on introducing further controls or restrictions on the payment of ransoms looks set to continue.

Acknowledgements

Stuart Davey
Partner, London

Stuart advises corporates, insurer clients and their insureds in responding to cyber incidents. This involves managing the breach response process by instructing IT forensics teams, managing regulatory investigations, cooperating with criminal authorities, engaging with credit monitoring services providers and dealing with third party claims arising out of data breaches. Stuart also specialises in resolving disputes arising out of large scale and technically complex IT projects. He advises both suppliers and users of technology, with a focus on dispute resolution and renegotiation of contracts for business process outsourcing and software/systems implementation projects. He is experienced in litigation, arbitration, mediation and other forms of alternative dispute resolution, having advised on one of the UK's largest ever technology arbitrations.

Julia Varley
Senior Associate, London

Julia advises a broad spectrum of clients in relation to all aspects of responding to cyber incidents, regulatory investigations and responding to data subject claims (including mass actions). She has considerable experience advising on ransomware events. Julia also specialises in media disputes and has been involved in a number of leading and high-profile cases in this area.

This paper was also produced with contributions from members of our UK and International Cyber teams, detailed overleaf.

About our cyber team

Pinsent Masons has developed an international cyber practice with specialist lawyers operating across the UK, Ireland, France, Germany, Spain, the Netherlands, UAE, Singapore, Hong Kong, and Australia with market leading expertise. We offer a full range of services from cyber readiness pre-breach services, incident response to regulatory investigation and litigation.

Our dedicated UK Cyber Team

David McIlwaine
Head of Cyber, Partner, London
+44 (0)20 7490 6224
+44 (0)7956 569 887
david.mcilwaine@pinsentmasons.com

Laura Gillespie
Partner, Belfast
+44 (0)2890 894 885
+44 (0)7918 721 998
laura.gillespie@pinsentmasons.com

Stuart Davey
Partner, London
+44 (0)20 7490 6179
+44 (0)7585 996 312
stuart.davey@pinsentmasons.com

James McBurney
Partner, Leeds
+44 (0)113 368 7770
+44 (0)7500 604 939
james.mcburney@pinsentmasons.com

Andrew Sackey
Partner, London
+44 (0)20 7490 9373
+44 (0)7771 387 667
andrew.sackey@pinsentmasons.com

Anna Flanagan
Senior Associate, Belfast
+44 (0)2890 894 887
+44 (0)7824 483 060
anna.flanagan@pinsentmasons.com

Julia Varley
Senior Associate, London
+44 (0)20 7418 8159
+44 (0)7771 822 861
julia.varley@pinsentmasons.com

Mastane Williamson
Associate, London
+44 (0)20 7054 2692
+44 (0)7880 134 898
mastane.williamson@pinsentmasons.com

Anna Conquest
Associate, London
+44 (0)20 7490 6393
+44 (0)7774 431 434
anna.conquest@pinsentmasons.com

Meghan Kirk
Associate, Belfast
+44 (0)2890 894 944
+44 (0)7342 069 285
meghan.kirk@pinsentmasons.com

Lisa McGrady
Solicitor, Belfast
+44 (0)2890 894 861
+44 (0)7769 935 932
lisa.mcgrady@pinsentmasons.com

Rebecca Townsend
Solicitor (Scotland), London
+44 (0)20 7667 0187
+44 (0)7918 372 316
rebecca.townsend@pinsentmasons.com

Lottie Peach
Solicitor, London
+44 (0)20 7418 7068
+44 (0)7585 103 046
lottie.peach@pinsentmasons.com

Aisling Taggart
Paralegal, Belfast
+44 (0)2890 894 916
+44 (0)7979 962 343
aisling.taggart@pinsentmasons.com

Toby Coughlin
Solicitor, London
+44 (0)20 7054 2573
+44 (0)7775 676 285
toby.coughlin@pinsentmasons.com

Shanelle Mattu
Paralegal, London
+44 (0)20 7490 6594
+44 (0)7557 184 119
shanelle.mattu@pinsentmasons.com

Christian Toon
Chief Information Security Officer, Birmingham
+44 (0)121 623 8648
+44 (0)7552 888 030
christian.toon@pinsentmasons.com

Our global key Cyber contacts

Andreas Carney
Partner, Dublin
+353 1 553 8603
+353 87 187 9584
andreas.carney@pinsentmasons.com

Ann Henry
Partner, Dublin
+353 1 553 8618
+353 87 323 5937
ann.henry@pinsentmasons.com

Annabelle Richard
Partner, Paris
+33 1 53 53 02 23
+33 6 21 17 64 05
annabelle.richard@pinsentmasons.com

Melina Wolman
Partner, Paris
+33 1 53 53 01 64
+33 6 21 17 64 27
melina.wolman@pinsentmasons.com

Paloma Bru
Partner, Madrid
+34 910 484 033
+34 608 641 384
paloma.bru@pinsentmasons.com

Stephan Appt
Partner, Munich
+49 89 203043 561
+49 174 333 28 56
stephan.appt@pinsentmasons.com

Kirsten Wolgast
Partner, Munich
+49 89 203043 579
+49 174 233 85 24
kirsten.wolgast@pinsentmasons.com

Damian Crosse
Partner, Dubai
+971 4 373 9749
+971 50 240 1068
damian.crosse@pinsentmasons.com

Luke Tapp
Partner, Dubai
+971 4 373 9750
+971 50 649 5245
luke.tapp@pinsentmasons.com

Tom Bicknell
Partner, Dubai
+971 4 373 9636
+971 56 403 8136
tom.bicknell@pinsentmasons.com

Paul Haswell
Partner, Hong Kong
+852 2294 3315
+852 5964 2050
paul.haswell@pinsentmasons.com

Bryan Tan
Partner, Singapore
+65 6305 8490
+65 8798 0985
bryan.tan@pinsentmasons.com

Alexander Shepherd
Partner, Singapore
+65 6309 5669
+65 9241 6141
alexander.shepherd@pinsentmasons.com

Andre Walter
Head of Data Law Solutions (Netherlands), Amsterdam
+31 20 7977 712
+31 655 415 810
andre.walter@pinsentmasons.com

References

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[2] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[3] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

[4] https://www.bailii.org/uk/cases/UKSC/2021/50.html

[5] Lloyd v Google was decided under the Data Protection Act 1998

[6] https://www.bailii.org/ew/cases/EWCA/Civ/2013/333.html

[7] https://www.bailii.org/ew/cases/EWHC/Ch/2015/1482.html#Gulati, https://www.bailii.org/ew/cases/EWCA/Civ/2015/1291.html

[8] https://www.bailii.org/ew/cases/EWHC/QB/2016/2217.html

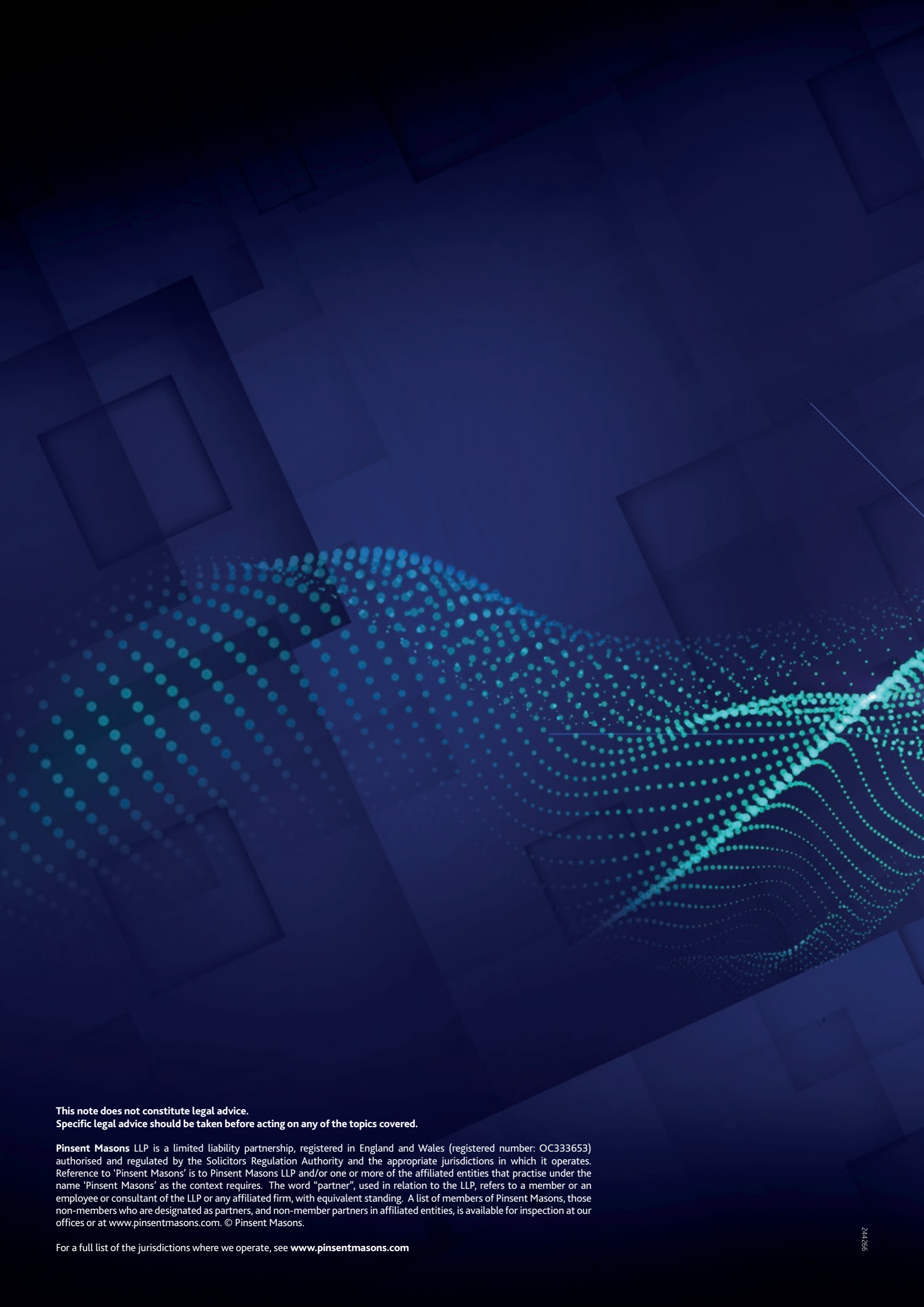
[9] https://www.bailii.org/ew/cases/EWHC/QB/2021/2168.html

[10] A number of claims brought against British Airways have apparently settled.

[11] https://www.pinsentmasons.com/out-law/news/dutch-government-considering-ban-on-ransom-payments-by-insurers

[12] https://securityandtechnology.org/ransomwaretaskforce/report/

[13] https://www.insurancejournal.com/news/international/2021/05/09/613255.htm



244266