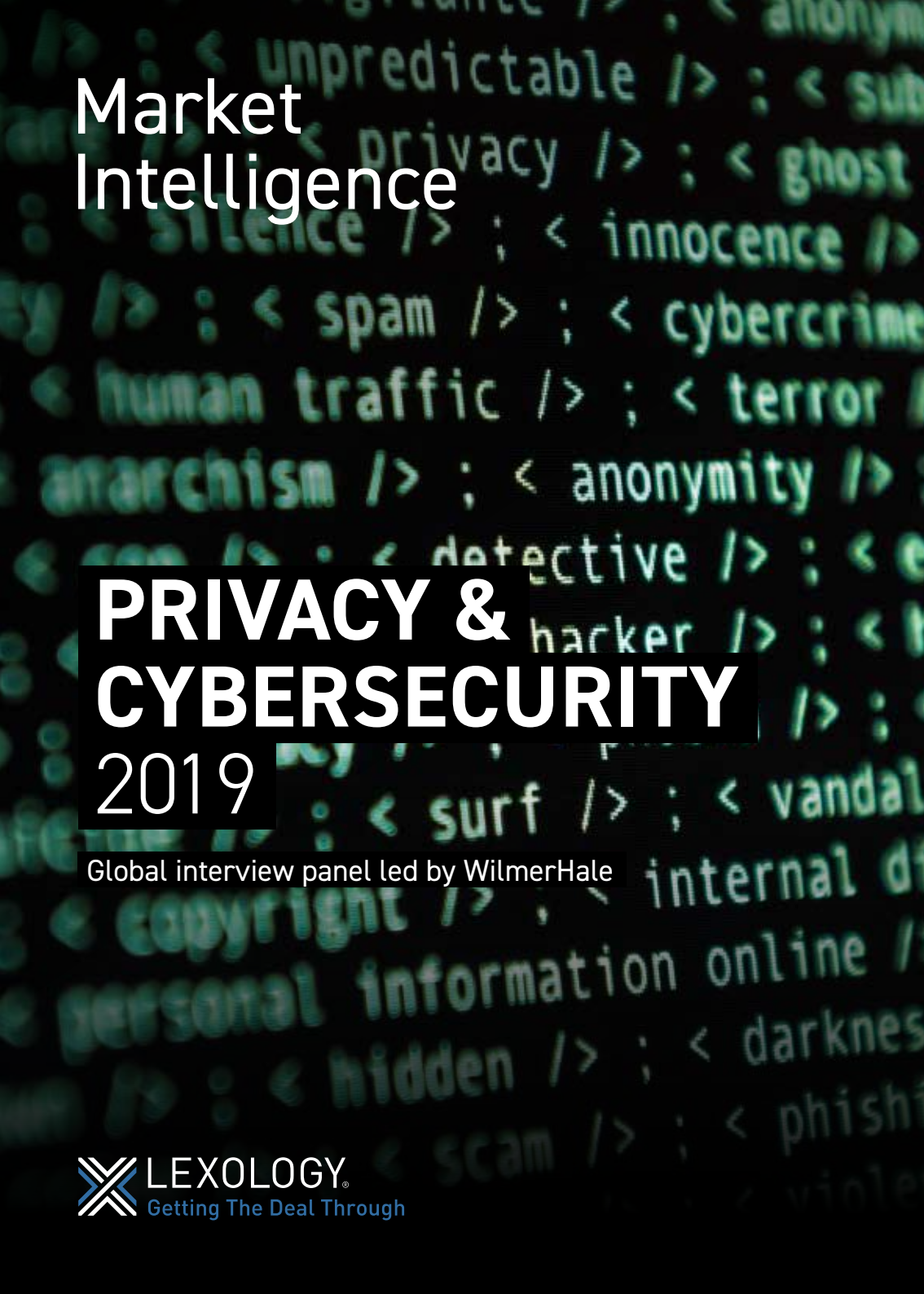
Market
Intelligence
PRIVACY &
CYBERSECURITY
2019
Global interview panel led by WilmerHale
LEXOLOGY
Getting The Deal Through

LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development managers
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Business development manager
Dan Brennan
dan.brennan@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL
Tel: +44 20 3780 4104
Fax: +44 20 7229 6910

Cover photo: iStock.com/CHUYN

ISBN: 978-1-83862-199-5

Printed and distributed by Encompass Print Solutions

Privacy & Cybersecurity 2019

United Kingdom

Michael Drury, partner at BCL Solicitors LLP, has unparalleled experience in cybersecurity issues having been for 15 years the director of legal affairs at the Government Communications Headquarters, the UK government agency charged with advising on IT security and the gathering of signals intelligence. He advised upon the form of and implementation of existing Regulation of Investigatory Powers Act 2000 and, having entered private practice in 2010 and provided a wide range of information law and cybersecurity advice since then (including the GDPR and the Cybersecurity directive), has given evidence to the UK Parliament Human Rights Committee about the replacement Investigatory Powers Act 2016, on which he has advised companies both large and small.

Julian Hayes is also a partner at BCL Solicitors LLP, specialises in data protection law, business crime and regulation, advising both individuals and corporates. He has particular expertise in the rapidly developing fields of cybercrime, data regulation and related litigation, advising leading communications service providers and others in relation to high-profile enquiries by the National Crime Agency and others. He advises on the GDPR and Data Protection Act 2018. He is a contributor to *The Guide to Cyber Investigations*, published by *Global Investigations Review*.

Photo: unsplash.com/@bruneljohnson

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

Following the UK's implementation of the General Data Protection Regulation (GDPR), the EU Law Enforcement Directive and the Network Information Security Directive during 2018, it might have been expected that the pace of regulatory change in the sphere of cybersecurity would abate. However, the UK's proposed departure from the European Union has ensured that legislators continue to train their sight on national cybersecurity regulation.

In preparation for Brexit, 2019 has already seen the publication of several Statutory Instruments relating to electronic data including the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (the Data Protection Amendment Regulations) and the Network and Information Systems (Amendment etc) (EU Exit) Regulations 2019 (the NIS Amendment).

Although not yet in force, the Data Protection Amendment Regulations correct legislative deficiencies caused by the UK's withdrawal from the EU with a view to ensuring that the legal framework for data protection within the UK continues to function smoothly after Brexit. No doubt hopeful of an EU adequacy decision to maintain post-Brexit UK–EU data flows, the UK government is essentially seeking continuity with the current regime. However, this may entail cost implications for business; for example, it has been confirmed that, in the event that the UK departs the EU without an agreement, data controllers processing UK personal data outside the UK would be required to appoint a representative within the UK as a point of contact for the UK's supervisory authority, the Information Commissioner's Office (ICO). The Data Protection Amendment Regulations will come into force 20 days after the UK formally leaves the EU.

The NIS Amendment amends those provisions of the Network and Information Systems Regulations 2018 (NIS) made redundant by the UK's withdrawal from the EU. The NIS Amendment removes obligations on the regulatory authorities and the National Cyber Security Centre (NCSC) to liaise, cooperate and share information with the European Commission and authorities in other member states. It also revokes Regulation (EU) No. 526/2013, which establishes and confers functions on the EU Agency for Network and Information Security (ENISA). The UK will, however, seek to agree continued third country participation in ENISA in line with existing third country agreements. Again, the NIS Amendment will come into force 20 days after the UK leaves the EU.

In a seeming contradiction of the nation's preparations for Brexit, the government recently implemented the EU Regulation on ENISA and Cyber Security Certification

(EU Regulation) (the ENISA Regulation), which came into force in the UK on 27 June 2019. The ENISA Regulation:

- strengthens the role of ENISA and provides it with a permanent mandate in order to give it a stronger and more central role; and
- sets up a framework to govern voluntary European cybersecurity certification schemes with a view to increasing trust and security of information, communications technology products and services and address existing fragmentation in the certification landscape to reduce costs and administrative burdens for companies, and to strengthen the digital single market.

EU Exit Guidance notes that the ENISA Regulation does not introduce any directly operational cybersecurity certification schemes, so there should be no operational implications for industry arising as a direct result of future cyber-related EU Regulations following the UK's departure from the EU.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The GDPR imposes strict reporting requirements and tough sanctions for failure to report where the obligation arises under article 33 of the GDPR. It is, therefore, vital that controllers fully understand what constitutes a data breach and are aware of their reporting duties.

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. Breaches include both hostile external activities (eg, ransomware attacks) and accidental internal incidents (eg, loss of digital devices containing personal data or missent emails).

In the first 12 months of the GDPR coming into force, the ICO saw a 400 per cent increase in the number of breach reports, though only 0.5 per cent of these led to the imposition of an improvement plan or a civil penalty. Perhaps with these statistics in mind, the regulator has introduced an online self-assessment tool to help controllers decide whether a breach report is necessary (https://ico.org.uk/for-organisations/report-a-breach/pdb-assessment/y).

Data controllers must consider reporting when they become aware of a data breach. The European Data Protection Board (EDPA) defines 'awareness' as having a reasonable degree of certainty that personal data has been compromised through a security incident. Controllers must implement appropriate technical and organisational measures (eg, reporting policies) to ensure they learn of security incidents that jeopardise personal data in time.

Once data controllers are aware that personal data has been lost, they must take steps to control the breach, assess whether their notification obligations are triggered and notify the ICO where necessary as soon as possible, normally within 72 hours. Similarly, outsourced data processors must notify data breaches to data controllers (who retain overall responsibility for breaches) without undue delay.

Breaches must be notified to the ICO unless they are unlikely to result in a risk for the rights and freedoms of individuals. The primary focus of this assessment exercise is on the data subjects whose personal data has been compromised; the recommended 'if in doubt' position is to notify the ICO.

Where there is likely to be a high risk to the rights and freedoms of individuals as a result of the breach, the data controller must also notify the affected individual without undue delay so they can take precautionary steps (eg, changing passwords). Direct notification to individuals is unnecessary where the lost data is securely encrypted, where remedial measures mean the perceived high risk is unlikely to

"In the first 12 months of the GDPR coming into force, the ICO saw a 400 per cent increase in the number of breach reports."

eventuate or where individual notification would involve disproportionate effort and a general public communication would suffice.

The ICO website gives some assistance on assessing risk, but WP29 (the forerunner of the EDPA) issued more detailed – and still current – guidance in its Guidelines on Personal Breach Notification under Regulation 2016/679 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052). Risk should be assessed by reference to its severity and likelihood. Relevant factors include the type of breach, the nature, sensitivity and volume of personal data affected, the number of individuals affected and the ease with which individuals can be identified from it. Where the lost data reveals an individual's ethnic origin, political views, details of their health, criminal convictions or offences, the data controller should assume the damage is likely to occur, increasing the likelihood that notification must be given.

Where supervisory authority notification is necessary, it can be given by phone or online. The Information Commissioner described the ICO's reporting expectation as, 'Tell it all, tell it fast and tell the truth'. However, phased reporting is permissible where not all the information is yet available.

Photo: unsplash.com/@heftiba

The ICO reminds service providers (eg, telecoms providers or internet service providers) that they should report breaches to the ICO within 24 hours under the Privacy and Electronic Communications (EC Directive) Regulations 2003 rather than the GDPR. Similarly, digital service providers should notify the ICO of breaches under the NIS provisions. Those subject to further regulatory obligations (eg, the Financial Conduct Authority (FCA) or Solicitors Regulation Authority (SRA)) should consider whether a data breach triggers a reporting requirement to those regulatory bodies. Finally, where criminal activity is suspected, data controllers may consider reporting the matter to the police via the Action Fraud website (https://www.actionfraud.police.uk/report_fraud). Careful records should be made documenting the personal data breach.

Apart from the adverse publicity attendant on high profile breaches, failure to notify the ICO of a notifiable data breach can attract a maximum fine of up to €10 million or 2 per cent of global turnover in the preceding financial year (whichever is the greater). The ICO's Regulatory Action Policy (https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf) suggests that failure to self-report is likely to increase any penalty imposed. Further, the GDPR gives any person who suffers damage or distress as a result of a data breach the right to pursue the data controller or processor for compensation.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

All organisations will suffer a data security incident at some stage, jeopardising privacy, business continuity and reputation, as well as exposing them to potential regulatory penalties and litigation. Advance planning is the key to navigating such hazards. Increasingly, organisations are developing cybersecurity and incident response plans to mitigate the risks. Such policies are a means of demonstrating to the ICO that an organisation takes seriously its obligations as a data controller to implement appropriate measures, ensuring that its data processing is GDPR-compliant. If a breach occurs, the ICO is likely to request a copy of an organisation's data protection policy and may check staff familiarity with it. According to some reports, between 2017 and 2018, 90 per cent of breach reports to the ICO arose as a result of employee error. Given this, staff training is essential to ensure everyone recognises, understands and avoids the risks, is aware of their individual responsibility for data security, knows how to report breaches and is encouraged to do so. Indeed, the organisational measures implemented by a data controller, self-reporting and the level of co-operation shown towards the ICO once a breach is

reported are all considerations in determining whether a penalty notice should be imposed and, if so, its level.

When a data breach occurs, a data controller has several immediate priorities: containing the breach, identifying the personal data involved, assessing the risk to those affected and notifying the ICO and data subjects (if necessary). A well-rehearsed incident response plan helps achieve these objectives, ideally with the help of an incident response team (IRT) led by a senior individual. Other IRT members might include representatives of an organisation's IT, business management and corporate communications departments. External consultants (eg, forensic experts, lawyers and PR advisers) should ideally be identified before an incident occurs.

As well as potential notification obligations under the data protection legislation, the IRT should also consider whether any contractual or professional regulatory obligations arise as a result of a data breach. For example, under Principle 11 of the FCA Handbook, regulated firms must notify it of 'material cyber incidents' (ie, those resulting in significant data loss) affecting a large number of customers or resulting in unauthorised access to or malicious software present on information and communications systems. Additionally, where a company believes it has been the victim of crime, it may – and often will – inform the police and should consider whether it could prevent any harm arising from the breach by seeking injunctive relief.

During both simulation exercises and genuine incidents, the IRT should record all the steps that it takes and its reasons for doing so to learn from its experience and later justify its decision-making to regulators and external stakeholders as necessary.

The costs of a data breach are potentially significant so organisations should ensure adequate insurance cover. The high-profile NotPetya malware and WannaCry ransomware attacks have prompted companies to seek specific cyber insurance cover, though many organisations still hope to rely on general insurance policies that are often silent on cyber coverage. However, the UK's increased exposure to cyber risk has given rise to a proliferation of 'affirmative' (ie, bespoke) cyber policies. The insurance regulator, the Prudential Regulatory Authority (PRA), has recently highlighted the risk of non-affirmation policies which are silent on coverage of cyber risk, which can give rise to disputes between insurers and the insured. The PRA has asked for insurers to develop a 'silent cyber' action plan by the middle of 2019.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

There is no single source of best practice cybersecurity guidance in the United Kingdom. Instead, multiple sources of national guidance on cybersecurity

"High-profile NotPetya malware and WannaCry ransomware attacks have prompted companies to seek specific cyber insurance cover."

preparedness exist. The disparate sources of guidance reflect the variety of UK authorities with responsibility for cybersecurity (NCSC, ICO, National Crime Agency (NCA) Cyber Crime Unit and National Fraud Intelligence Bureau) and industry-specific regulators whose responsibilities are affected by cyber risk.

The well-known '10 Steps to Cyber Security' (https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security), formerly issued by the government, was withdrawn on 13 December 2018 and is now issued by the widely respected NCSC whose website contains a wealth of guidance on cybersecurity issues. 'The 10 Steps to Cyber Security' is complemented by 'Common Cyber Attacks: Reducing the Impact', which sets out security and process controls organisations may establish to protect against online risk. The Cyber Essentials Scheme also recommends organisations implement five basic controls to protect against cyberattacks, including the creation of effective firewalls and the use of the latest supported application versions and patches. Additional useful information is available from the NCSC's 'Cyber Security: Small Business Guide', the cross-governmental Cyber Aware campaign, the ICO's 2016 publication 'A Practical Guide to IT Security' and the Action Fraud website of the National Fraud and Cyber Crime Reporting Centre. The NCSC's website also contains helpful pages on specific IT security issues, including protecting against ransomware, phishing attacks and email security. At a non-governmental level, there is some mandatory sector-specific guidance such as the Payment Card Industry Data Security Standard and the ISO/IEC 2700 group of standards for the security of information security management systems and BS 10012:2017, which provides a GDPR-compliant personal information management system. Reflecting the significance of the financial sector for the UK economy, the FCA is increasingly active in relation to the dissemination of cybersecurity information (https://www.fca.org.uk/publication/research/cyber-security-industry-insights.pdf). In June 2019, the Bank of England published a report on the future of the financial system that, while acknowledging that coordination between the private sector and regulators had made progress towards mitigating risk, nevertheless recognised the ever-present threat and need for even greater cooperation in the event of a major cyber incident. Such efforts have been supported by the CBEST framework designed to test the cyber resilience of systemically important financial institutions through bespoke vulnerability-testing. Where industry codes exist, adhering to them may demonstrate compliance with a data controller's obligation to maintain appropriate security. Additionally, the ICO's Regulatory Action Policy suggests abiding by them will be considered when the regulator decides whether and by how much to penalise an organisation for a data breach. The ENISA Regulation implemented in the UK despite imminent Brexit envisages that the EU Cyber Security Agency will become a future information hub with responsibility for promoting and sharing best cybersecurity practice.

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

The global cloud computing market is forecast to reach US$623.3 billion by 2023. Its exponential growth reflects its attractiveness for efficiently storing and accessing vast amounts of data.

If the transition to the cloud is conducted with care, it can improve IT security. However, myriad financial, legal and compliance risks exist. The threats, risks and vulnerabilities for cloud-hosting environments are largely the same as traditional data-hosting environments in the form of data breaches, denial of service attacks and system vulnerabilities. When choosing a cloud computing service, someone with the appropriate technical expertise should undertake the necessary checks to ensure sufficient guarantees and compliance with the relevant regulations. The GDPR places responsibility on both the cloud computing provider as a 'data processor' and on the original holder or owner of the data as a 'data controller'.

Photo: unsplash.com/@samuelzeller

The major data security and privacy concern is the lack of control over the location of cloud computing service providers. Cloud computing often involves movement of data to a cheaper jurisdiction so the user may not be aware where the data is stored. Personal data can only be transferred to a non-European Economic Area (EEA) country if it is on the European Commission's authorised list of nations providing adequate personal data protection. Organisations may transfer data to non-EEA locations only where they demonstrate that they meet the Binding Corporate Rules and satisfy the requirements established by WP29. Users need to be alive to these issues.

Just like internal IT systems, cloud hosting environments are susceptible to server meltdowns. To safeguard against such occurrences, best practice suggests backing up data separately and ensuring that cloud hosting environments have a comprehensive back-up system themselves.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The scale of cybersecurity threats and cybercrime in the UK's complex economy varies enormously, from phishing scams through to sophisticated, state-sponsored attempts to disrupt critical national infrastructure such as the energy, health, finance and food sectors. The scope of activities that could fall into that category is wide and the threats evolve at a rapid pace. Acknowledging the many benefits that internet-based technologies have brought, the UK's National Cyber Security Strategy 2016–2021 notes cybercriminals and hostile state-sponsored groups are enlarging their ambitions and expanding their stratagems to take advantage of online opportunities. Ranged against this multiplicity of external and internal threats are a number of government agencies including the NCA, the cybercrime units of police Regional Organised Crime Units, Action Fraud run by the City of London Police, the ICO, the NCSC, the Centre for the Protection of National Infrastructure and the security services, each with different remits and functions. Reflecting the boundary-less nature of cyberthreats, these agencies work closely with each other and with their overseas counterparts such as the Europol and the Netherlands-based European Cybercrime Centre, the FBI and the Australian Cyber Security Centre.

The government has broadly pursued a three-pronged strategy in tackling current and emerging cyberthreats: providing advice to improve cybersecurity, increasing statutory and regulatory reporting obligations, and promoting information sharing about emerging threats. A lead player in the UK authority's approach has been the NCSC. Backed by the expertise and resources available to Government Communications Headquarters (GCHQ), the NCSC is intended as a single point of

"The government has broadly pursued a three-pronged strategy in tackling current and emerging cyberthreats."

contact in relation to cybersecurity incidents, aiming to provide authoritative cybersecurity advice to manage cyber incidents and to mitigate their effects. Information-sharing about threats by those experiencing them is seen as key to tackling cyberthreats and preventing them spiralling out of control. However, under-reporting of cybercrime is seen as a significant problem, with the NCA estimating only 3 per cent of cyberattacks are reported to the police, often through fear of regulatory action or business disruption resulting from investigations by law enforcement. To address under-reporting, the NCSC confirmed in April 2019 it would not automatically report data breaches to the ICO and the NCA has given similar public indications. Later in the year the NCA will roll out a bespoke online platform to make it more straightforward for businesses to report cybercrime and which will direct the report to the appropriate agency.

Other measures to promote the sharing of cyberthreat information include statutory 'information gateways' in the Counter Terrorism Act 2008 and Crime and Courts Act 2013 that absolve an individual or entity of liability in respect of disclosure to the UK intelligence services or NCA. Additionally, the government has established organisation-focused information sharing forums including the Cybersecurity Information Sharing Partnership and the Retail Cyber Security Forum to facilitate the early sectoral dissemination of information on cyberthreats, vulnerabilities and remediation.

In recognition of the increasingly hostile online environment, with malign state actors seeking to disrupt critical national infrastructure and interfere in democratic events, the NCSC has developed the means of tracking the most threatening attack groups and techniques of countering them. In a further effort to deter cyberthreats from states and criminal gangs, in May 2019 the government was instrumental in developing a new coordinated EU sanctions regime targeted at those responsible for actual and attempted hostile cyberattacks, including the imposition of travel bans, asset-freezing and the prohibition of funding to those listed. Sanctions may also be imposed on persons or entities associated with listed individuals.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

'Avoid the data lemon'; as the theory goes, in a market where the buyer has less knowledge about the product than the seller, the buyer risks buying a lemon (US slang for a bad car). The effect of a serious cybersecurity breach on a company's share price can be significant (in high-profile examples, AOL and TalkTalk saw respective drops of 23.56 per cent and 14.55 per cent in the month after breaches). As recently as 2014, a survey of 214 businesses including financial institutions,

Photo: unsplash.com/@charlpost

investors and legal services providers, found that 78 per cent of respondents believed that cybersecurity was not analysed in great depth during the M&A due diligence process. That situation may now be changing and given the nature of M&A work and the financial risks at stake, privacy and data security issues should be seen as paramount. Indeed, some commentators now identify good privacy policies as a means of attracting potential investment.

Today, the issue of cybersecurity in the context of M&A must be assessed in the same way as other risks that undermine corporate value. Indeed, to safeguard against risks associated with data security issues, many businesses are appointing chief privacy officers, reflecting the escalation of data privacy issues to the board-room. However, while the GDPR has brought about some degree of certainty in this area, the regulatory framework can be unclear, such that legal advisers lack a clear set of rules against which to assess potential M&A targets. As the volume of personal and customer data kept by companies increases, traditional due diligence is becoming inadequate. Further 'e-due diligence' is a way in which companies can scrutinise the target organisation's data security policy and internal IT systems. Due diligence should look at how the target gathers data and personal information, how

it uses and stores that data (including the use of cloud services), whether it encrypts data, whether it destroys it and, if so, how. Specific enquiries about data breaches are necessary. However, the way in which companies factor risks arising from data and security issues should not stop at the pre-merger or acquisition stage. One way to mitigate data security risks is through warranties and indemnification against both past and future breaches within the share purchase agreement. From a GDPR perspective, companies need to address how existing consents given by data subjects will affect not only the integration of the acquirer and the target, but also of the future of the merged businesses. This final point envisages the example of a US company acquiring another company that processes the personal data of EU citizens. If the acquiring company, operating from a 'third country', intends to transfer this personal data outside the EU, it should consider its potential obligations under Chapter 5 GDPR.

Michael Drury
mdrury@bcl.com

Julian Hayes
jhayes@bcl.com

BCL Solicitors LLP
London
www.bcl.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Key is being able to synthesise an analysis of complex and developing law, which will be an exercise in legal risk management as much as interpretation, with sufficient understanding of the technology both in terms of what has happened and how it can be used to mitigate damage. An appreciation of wider business drivers is fundamental.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

This is an area where the law remains in flux: there is no dedicated set of cybersecurity laws. Rather, one has to deal with a complex and challenging amalgam of legislation.

How is the privacy landscape changing in your jurisdiction?

With the UK as a 'third country' post-Brexit, there will have to be equivalent UK laws to the EU regime to continue to permit data transfers between the UK and the rest of Europe. That will necessarily involve a legislative change. In the criminal justice context, the Crime (Overseas Production Orders) Act 2019 should begin to have real impact on law enforcement once the overarching US–UK framework agreement is ratified. There are also seminal legal challenges to the UK electronic surveillance regime over the obtaining of bulk data by the UK Security and Intelligence Agencies and Law Enforcement Authorities.

Recent fines imposed on British Airways and Marriott Hotels for serious data breaches demonstrate the ICO's increasing willingness to flex its muscles, challenging heavyweight targets using its GDPR powers.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

All companies remain vulnerable – the fact that 'WannaCry' slips further into the past does not mean that ransomware attacks are less prevalent. However, targeted attacks are on the rise in the form of 'spear phishing'.

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by WilmerHale, this *Privacy & Cybersecurity* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals.

Regulatory developments
M&A risks
Best practice
Cloud hosting

ISBN 978-1-83862-199-5