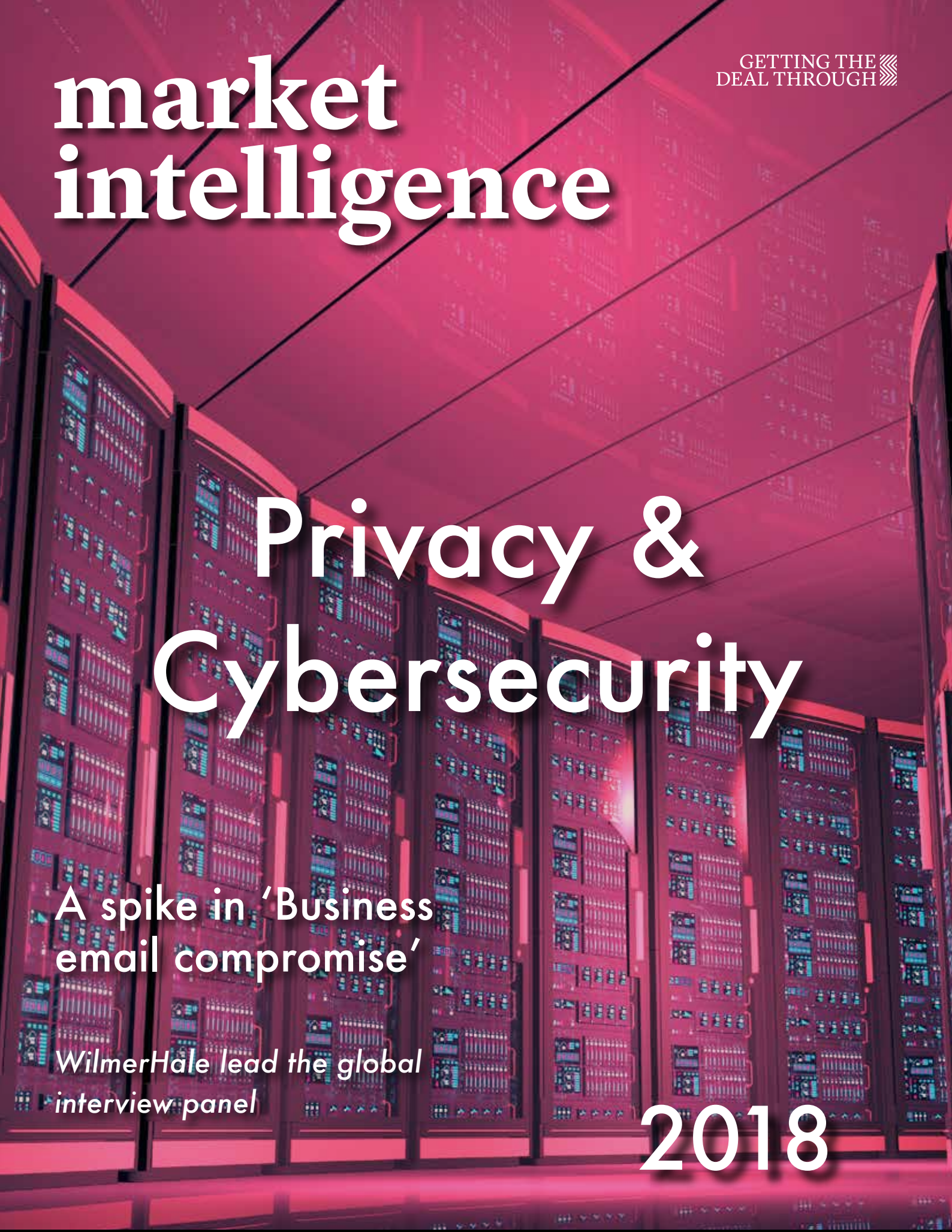

GETTING THE DEAL THROUGH

market intelligence

Privacy & Cybersecurity

A spike in 'Business email compromise'

WilmerHale lead the global interview panel

2018

North America • Asia-Pacific • Europe • Latin America
Regulatory developments • M&A risks • Best practice • Cloud computing

Publisher: Tom Barnes
Senior business development manager: Adam Sargent
adam.sargent@gettingthedealthrough.com
Business development manager: Dan Brennan
dan.brennan@gettingthedealthrough.com
Product marketing manager: Kieran Hansen
subscriptions@gettingthedealthrough.com

Head of production: Adam Myers
Editorial coordinator: Gracie Ford
Subeditor: Janina Godowska
Designer/production editor: Harry Turner

Cover: iStock.com/Maxiphoto

Published by
Law Business Research Ltd
87 Lancaster Road

Law Business Research

London, W11 1QQ, UK
Tel: +44 20 3780 4104
Fax: +44 20 7229 6910

ISBN: 978-1-78915-086-5

GETTING THE DEAL THROUGH

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

market intelligence

Welcome to GTDT: *Market Intelligence*.

This is the 2018 edition of *Privacy and Cybersecurity*.

Getting the Deal Through invites leading practitioners to reflect on evolving legal and regulatory landscapes. Through engaging and analytical interviews, featuring a uniform set of questions to aid in jurisdictional comparison, *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 interesting cases and deals.

Market Intelligence is available in print and online at www.gettingthedealthrough.com/intelligence.

Getting the Deal Through
London
August 2018

Contents

PRIVACY AND CYBERSECURITY IN THE

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 GCHQ, 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 (and yet to be fully brought into force) Investigatory Powers Act 2016, on which he has advised companies both large and small.

Julian Hayes is also a partner at BCL Solicitors LLP, specialising in all aspects of business crime and regulation, advising both individuals and corporates. He has particular expertise in the rapidly developing fields of cyber-crime, data regulation and related litigation, advising leading communications service providers and others in relation to high-profile enquiries by the NCA and others. He advises on the GDPR and Data Protection Act 2018. He co-authored the 2018 edition of the England and Wales chapter of GTDT's publication *Cybersecurity*.

Photo by Benjamin Davies on Unsplash

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

Michael Drury and Julian Hayes: Although the UK is expected to leave the EU in March 2019, the government nevertheless implemented three significant pieces of EU legislation during 2018: the General Data Protection Regulation (GDPR), the EU Law Enforcement Directive (LED) and the Network and Information Security Directive (NIS). Together this legislative trio will bring about the most fundamental change in a generation to the regulatory landscape for UK cybersecurity and data protection (and, the government hopes, enhance the UK's chances of a treaty or EC 'adequacy decision' to safeguard post-Brexit UK–EU data flows).

The GDPR came into force in the UK on 25 May 2018. Although it has direct effect, it should be read in conjunction with the Data Protection Act 2018 (DPA 2018). Applying common standards across the EU, the GDPR aims to modernise European data laws. Of particular relevance to cybersecurity is the integrity and confidentiality principle – the obligation on both data controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Much GDPR terminology and many of its concepts will be familiar from the preceding data protection regime, leading some experts to suggest organisational compliance would be straightforward. However, ensuring contract compliance with the GDPR alone is estimated to have cost FTSE 100 companies approximately £800 million, and as late as March 2018, the UK's Federation of Small Businesses found fewer than 10 per cent of small businesses were fully GDPR-ready.

Oversight of the GDPR in the UK will continue to be undertaken by the Information Commissioner's Office (ICO), backed up by extensive investigative and enforcement powers. Whereas previously breach notification was not mandatory, the GDPR requires notification of personal data breaches to the ICO 'unless it is unlikely to result in a risk for the rights and freedoms of natural persons', and notification of affected individuals themselves where a high risk is likely (as detailed below). Serious GDPR infringements may attract administrative penalties, with failures to comply with the processing principles, with a supervisory order, or to give the ICO access to premises or equipment attracting a potential maximum penalty of €20 million or 4 per cent of global turnover.

The provisions of the LED are enacted through Part 3 of the DPA 2018, which regulates data processing by various authorities (including the Serious Fraud Office, National Crime Agency (NCA), Financial Conduct Authority (FCA), Competition and Markets Authority and the police) for the prevention, investigation, detection or prosecution of criminal offences, execution of criminal penalties and the prevention of threats to public security. Data processing for law enforcement purposes must adhere to six data protection principles that mirror those in the GDPR. Individuals have a number of statutory rights, including to access their personal data, to rectify inaccuracies and to erase them where the relevant criteria are satisfied. Exemptions and restrictions exist where necessary and


Michael Drury


Julian Hayes

Breaches must be notified to the ICO unless they are unlikely to result in a risk for the rights and freedoms of individuals.

proportionate to avoid obstructing or prejudicing an investigation, and to protect public or national security.

The NIS provisions are enacted by means of the Network and Information Systems Regulation 2018 (in force from 10 May 2018) and are applicable to operators of essential services (eg, water, transport and energy) and digital service providers above a certain size and turnover (eg, online search engines available to the public, online markets and cloud computing services). Using a non-prescriptive approach, NIS aims to establish a pan-European level of security for critical infrastructure providers by requiring appropriate and proportionate technical and organisational measures to manage risk. Incidents which have a significant impact on the continuity of an essential service must be notified to the applicable competent authority. Where incidents are suspected of having a cybersecurity element, as well as notifying the competent authority, operators are strongly encouraged to contact the UK's National Cyber Security Centre (NCSC).

GTDT: 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?

MD & JH: 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 mis-sent emails).

Pre-GDPR, notification of serious data breaches to the ICO was not obligatory. A November 2017 DCMS survey found, for example, only 29 per cent of businesses had reported their most disruptive cyber breach to anyone other than an outside contractor in the preceding 12 months. The GDPR regime radically changes the legal position, imposing strict new reporting requirements and tough sanctions for non-compliance to enforce the 'integrity and confidentiality' principle.

Data controllers must consider reporting when they become aware of a data breach. WP29 (now the European Data Protection Board), 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 which jeopardise personal data in a timely manner.

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 he or she 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 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 has given more detailed guidance in its Guidelines on Personal Breach Notification under Regulation 2016/679 (https://iapp.org/media/pdf/resource_center/WP29-Breach-notification_02-2018.pdf). 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 has 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.

The ICO reminds communications service providers that they should continue to report breaches within 24 hours under the Privacy and Electronic Communications 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 FCA or 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 and the steps taken.

The consequences for failure to comply with these requirements can be severe. 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 draft Regulatory Action Plan 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.

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

MD & JH: 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. With 85 per cent of data breaches within an organisation said to arise as a result of employee error, 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.

When a data breach occurs, a data controller has several immediate priorities: containing the

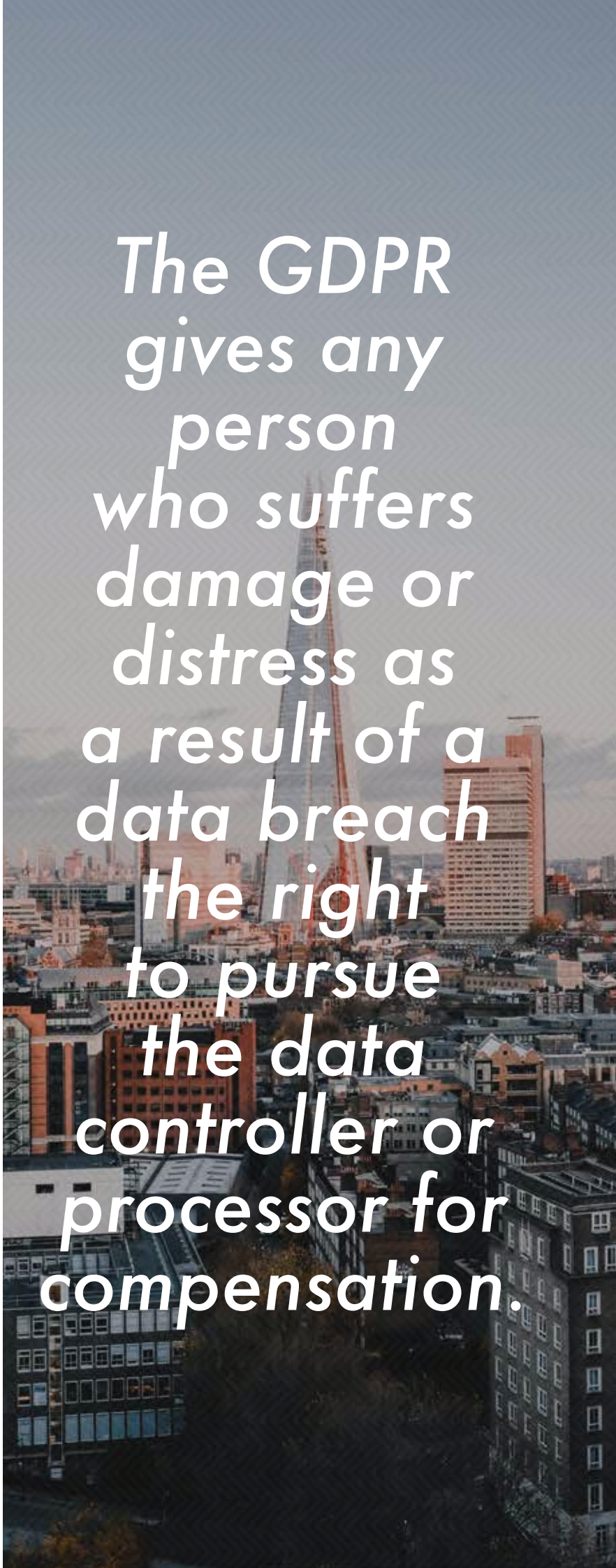

Photo by Aaron Gilmore on Unsplash

Photo by Veliko Karachiviev on Unsplash

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 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 that result 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, though many organisations still hope to rely on general insurance policies that are often silent on cyber coverage. In 2017, the UK's insurance regulator, the Prudential Regulatory Authority, directed insurers to be clearer about whether cyber risk is covered in general policies.

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

MD & JH: There is no single source of best practice cybersecurity guidance in the UK. Instead, multiple sources of national guidance on cybersecurity preparedness exist. If these were not enough, a recent survey also suggested some businesses are consulting overseas sources such as the US Federal Computer Security Program Managers' Forum for guidance. The disparate sources of guidance reflect the variety of UK authorities with responsibility for cybersecurity (NCSC, ICO, NCA Cyber Crime Unit and National Fraud Intelligence Bureau) and industry-specific regulators whose responsibilities are affected by cyber risk.

Despite this crowded field, joint advice is increasingly on offer (eg, 'GDPR Security Outcomes' offered by the NCSC and ICO) and even joint campaigns between government

and industry bodies (eg, 'The Devil's in the Detail' campaign led by ActionFraud, the Telecommunications UK Fraud Forum and Financial Fraud UK to promote measures against information theft).

In 2016, the government updated its '10 Steps to Cyber Security', which is now complemented by 'Common Cyber Attacks: Reducing the Impact' setting out security and process controls organisations may establish to protect against online risk. The Cyber Essentials Scheme also recommends all organisations implement five basic controls to protect against cyber attack, 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 ActionFraud 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 there is also ISO/IEC 27001 published in 2013 which aims to reflect best practice for information security management, and BS 10012:2017 providing a GDPR-compliant personal information management system. Recently, the FCA has prioritised cybersecurity through senior-level speeches to raise industry awareness and publishing guidance on cybersecurity (https://www.fca.org.uk/firms/cyber-resilience). These 'soft guidance' measures have been supported by the CBEST framework designed to test the cyber-resilience of systemically important financial institutions through bespoke vulnerability-testing. Foreshadowing future guidance, in July 2018, the Bank of England, FCA and Prudential Regulation Authority issued a joint discussion paper to generate a debate about regulatory expectations of the operational resilience of firms and financial market infrastructures.

Where industry codes exist, adhering to them may demonstrate compliance with a data controller's obligation to maintain appropriate security. Additionally, the ICO's draft 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.

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

MD & JH: In 2018, the cloud computing market was estimated to be worth US$287.8 billion worldwide. 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 exists. 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 (DDoS) 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'.

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'.

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 it is stored. Personal data can only be transferred to a non-EEA country if it is on the EC'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.

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

MD & JH: The difficulty for the UK government in addressing serious cybersecurity threats and criminal activity stems from determining just what comprises 'serious cybersecurity threats

THE INSIDE TRACK

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

The key attribute is being able to synthesise an analysis of complex and often undeveloped law, which in large part will be an exercise in legal risk management as much as pure interpretation, with a sufficient understanding of the technology both in terms of what has happened and how it can be used to mitigate damage. An appreciation of the wider business drivers – crucially the effect of a cyber incident on market share, customer service and, ultimately, reputation – is also fundamental.

Ultimately, advising on cyber security is not something that lawyers can do in isolation. So the ability to work as part of a cross-disciplinary team and see the law as only part, if nonetheless a very important part, of the development of sound cyber security practice and crisis management – if matters come to that – is essential.

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

The newness of the 2018 regime in English law presents fascinating challenges. Although firmly rooted in the previous EU driven regime, there is sufficient change, especially in the new specific cyber-related Network and Information Systems Regulation and the investigation and enforcement regime, to allow real legal creativity. Coupled with an activist ICO, the challenges for businesses, even in respect of what might formerly have been thought of a 'minor' incidents, are significant. And cyber law professionals will be in more demand than ever.

Necessarily the complexities produced by forthcoming Brexit also provide unique legal challenges which will be never less than fascinating. Although the future may be obscured by the fog shrouding what any Brexit deal will eventually look like – whether it will be hard or soft – the need to provide sound advice within a system that maintains the necessary degree of equivalence with EU law will require a far from isolationist legal approach.

How is the privacy landscape changing in your jurisdiction?

At present, the English legal position remains extremely fluid. There is a new intrusive surveillance regime just implemented with extant challenges both in the Strasbourg Court and in the domestic courts to the old regime, which nonetheless have the potential to influence even the very existence of the new laws and certainly their interpretation given the similarities between the old and new legislation.

The boundaries of personal privacy defined in data protection and the rights of the data subject to demand, to know and be told what is happening to their data have just been considerably expanded by the EU and in UK primary legislation. Those principled changes, with the data subject being at the centre of things, will not suffer as a result of Brexit whatever its stamp.

Finally, in the realm of personal privacy the limits to which Article 8 of the European convention of Human Rights can be relied upon to protect individuals from state action – with a parasitic growth in privacy protection in the purely private sphere – seem far from settled and there is surely further room for reliance on those rights.

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

Although 'WannaCry' may seem like ancient history in terms of threats, the theft of data – even where good practice is followed – will remain a key concern, especially if associated with a threat to embarrass or damage data controllers or subjects if a ransom is not paid. Important though it is to defend against such attacks through good cyber practice and adherence to the data protection principles, the underlying threat remains the pre-eminent one: the inadvertent loss of data through technical weakness or human error without the actions of a malefactor. To that extent nothing has changed and one can see how the investigative and enforcement regime will continue to target – and be harsher toward – those whose basic protections, both physical and technological, are judged inadequate, as against those who are the victims of sophisticated and unauthorised incursions.

We are now entering a new world where 'data harvesting' through the use of apps applied to social media in particular, with less than clear capabilities matched by equally opaque terms and conditions, represents a real threat not only to an individual's privacy but, seemingly, broader democratic processes. These must constitute cybersecurity incidents, at least as far as the operators of social media platforms are concerned. We will surely see the creation of a new paradigm in terms of the care such providers take to prevent such incidents.

Michael Drury and Julian Hayes
BCL Solicitors LLP
London
www.bcl.com

and criminal activity'. The scope of activities that could fall into that category is wide and threats evolve at a rapid pace. The word 'serious' connotes 'excessive harm'. 'Harm', for businesses, is likely to be defined in strict financial terms whereas for public bodies, 'harm' is likely to be determined in terms of a broader threat to the nation or the simple fact of data loss. Notwithstanding the struggles associated with tackling cybersecurity threats, the UK government is taking steps to confront the issue.

In July 2018, the Lord Chancellor announced a new court (expected to be completed in 2025) specifically designed to tackle cybercrime, fraud, and economic crime. Regarding hostile state-sponsored groups the UK's National Cyber Security Strategy 2016–2021 notes that these are expanding their stratagems to take advantage of online opportunities. Consequently, this is likely to increase extremism, threatening the UK and its interests.

As such, the government has pursued a three-pronged strategy, in tackling current and emerging cyber threats: 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 GCHQ, NCSC aims to provide authoritative cybersecurity advice to manage cyber incidents and to mitigate their effects.

In April 2018, in conjunction with the NCA, the NCSC published its 2017–2018 report on the cyber threat to UK businesses, explaining the modus operandi of pivotal cyber incidents such as the WannaCry ransomware attack and noting trends such as the increase in DDoS and ransomware attacks throughout the year. In the same month, the NCSC launched CYBERUK 2018, attended by specialists from across government, industry and law enforcement. There, it was announced that, against the backdrop of the GDPR implementation and NIS, the NCSC and law enforcement are implementing a new cyber incident prioritisation framework. NCSC incident responders now classify attacks into six categories to improve consistency around incident response and better use resources – ultimately aiming for better victim support.

Other measures to promote the sharing of cyber threat 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 cyber threats, vulnerabilities and remediation.

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

MD & JH: 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). Despite these statistics, a recent survey of 214 businesses including financial institutions, investors and legal services providers, found that 78 per cent of respondents believed that cybersecurity is not analysed in great depth during the M&A due diligence process.

Given the nature of M&A work and the financial risks at stake, privacy and data security issues should be seen as paramount. 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 boardroom.

However, while the GDPR has brought about some degree of certainty in this area, the regulatory framework remains unclear, resulting in legal advisers not having a clear set of rules against which to assess potential M&A targets.

In the first instance, more comprehensive due diligence work is required. 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 company's data security policy and internal IT systems. Due diligence should look at how the target company gathers data and personal information, how it uses and stores those data (including the use of cloud services), whether it encrypts data, whether it destroys them 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.

Also available online

www.gettingthedealthrough.com

ISBN: 978-1-78915-086-5