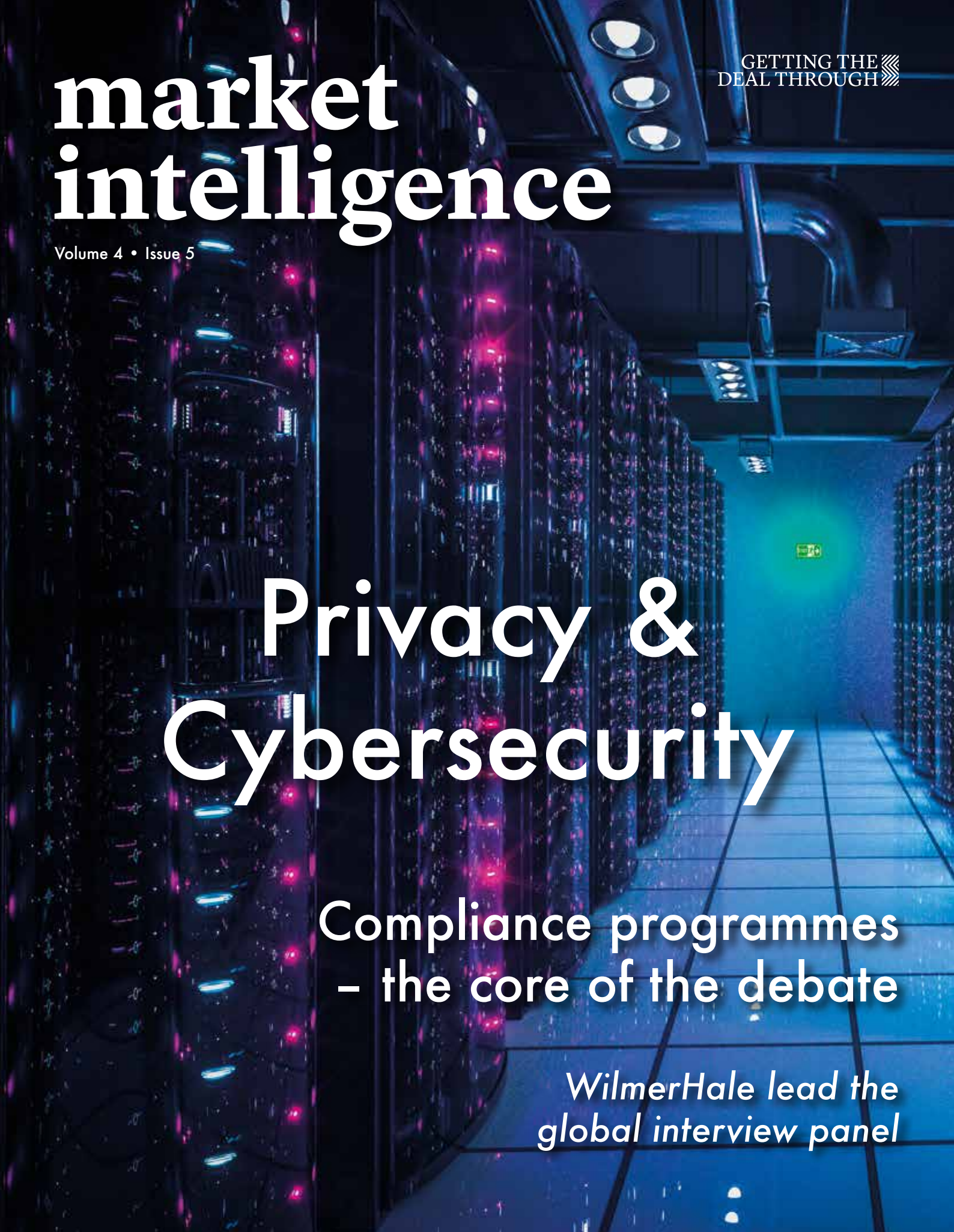


GETTING THE DEAL THROUGH

market intelligence

Volume 4 • Issue 5

Privacy & Cybersecurity

Compliance programmes – the core of the debate

WilmerHale lead the global interview panel

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

Publisher: Gideon Roberton
Senior business development manager: Adam Sargent
adam.sargent@gettingthedealthrough.com
Business development manager: Dan Brennan
dan.brennan@gettingthedealthrough.com
Readership development manager: Rosie Oliver
rose.oliver@gettingthedealthrough.com
Product marketing manager: Kieran Hansen
subscriptions@gettingthedealthrough.com

Head of production: Adam Myers
Editorial coordinator: Gracie Ford
Subeditor: Jonathan Allen
Designer/production editor: Tessa Brummitt

Cover: iStock.com/4X-image

Law Business Research

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4104
Fax: +44 20 7229 6910

ISSN: 2515-3749

GETTING THE DEAL THROUGH

Strategic Research Sponsor of the ABA Section of International Law

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

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

market intelligence

Welcome to GTDT: *Market Intelligence*.

This issue focuses on 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 2017

In this issue

iStock.com/alice-photo

PRIVACY & CYBERSECURITY IN THE

UNITED KINGDOM

Michael Drury is a partner at BCL Solicitors LLP. He has unparalleled experience in cybersecurity issues having been the Director of Legal Affairs at GCHQ, the UK government agency charged with advising on IT security and the gathering of signals intelligence, for 15 years. He advised upon the form and implementation of the Regulation of Investigatory Powers Act 2000 and, since entering private practice in 2010, has provided a wide range of information law and cybersecurity advice, and given evidence to the UK Parliament Human Rights Committee about the replacement (and yet to be brought into force) Investigatory Powers Act 2016, on which he has advised companies both large and small.

Julian Hayes is 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 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 co-authored the England and Wales chapter of GTDT *Cybersecurity* 2017.

Michael Drury

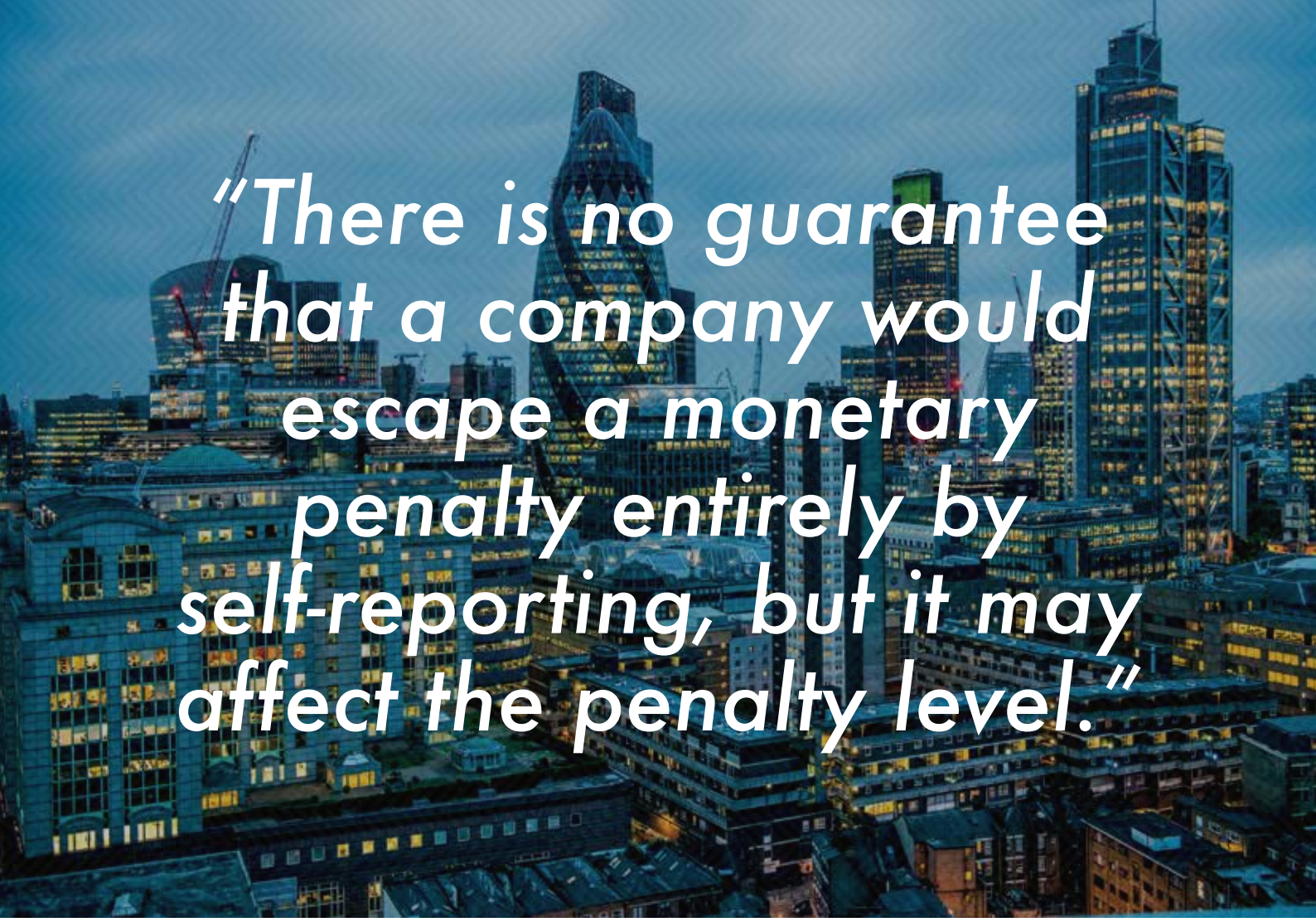
Julian Hayes

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

Michael Drury & Julian Hayes: Notwithstanding Brexit, both the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NISD) represent the most important upcoming UK regulatory developments in cybersecurity. Both are due to be implemented in May 2018 and will have wide-reaching implications for UK businesses.

The GDPR will have direct effect in the UK from 25 May 2018 and aims to modernise European data protection laws in line with rapidly increasing technological possibilities and cybersecurity threats. The new Regulation has extensive jurisdictional scope, affecting any business offering goods and services to EU citizens regardless of where it is located. Several key provisions should be noted in the cybersecurity context. The first is a uniform requirement for notification of security breaches including notification to affected data subjects if the breach is likely to result in a high risk to the rights and freedoms of individuals, unless the organisation had applied appropriate security measures either before or after the breach to counteract this risk. Second, the Regulation affects both data controllers and data processors. In relation to the latter, it now sets out clear obligations that include the responsibility to implement technical and organisational security measures, appropriate to the specific risks that exist. It also includes the requirement to assist data controllers with data subject access requests, facilitating individuals' access to their personal data. Once adopted, violations of the core principles of the Regulation could result in fines of up to 4 per cent of an organisation's annual worldwide turnover, or a maximum of €20 million (whichever is highest).

The NISD is primarily concerned with enhancing national cybersecurity capabilities, improving cooperation and applying security and notification requirements both for essential service operators and digital service providers. Under the NISD, member states must adopt a national network and information security strategy in line with EU law and designate a national supervisory authority and computer security incident response teams to handle risks and incidents. An EU-wide 'cooperation group' will be established to facilitate cooperation and information sharing. Both essential service operators and digital service providers will be obliged to notify security incidents to the relevant national supervisory authority. To a certain extent, the NISD leaves the precise definition of 'operators of essential services' and 'digital service platforms', such as e-commerce platforms, search engines and cloud services, to member state discretion.



> *"There is no guarantee that a company would escape a monetary penalty entirely by self-reporting, but it may affect the penalty level."*

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 personal data breach is the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. Electronic service providers like telecoms providers and internet service providers under the Privacy and Electronic Communications Regulations 2003 are obliged to notify the Information Commissioner's Office (ICO) within 24 hours of detecting a breach. Additionally, in May 2017, the Financial Conduct Authority (FCA) published guidance confirming that regulated firms must report 'material' data breaches under their Principle 11 obligations. That said, there is currently no general legal obligation under the Data Protection Act (DPA) for data controllers to report breaches to the ICO. However, the regulator believes data controllers should report serious breaches. 'Serious' is undefined, though ICO guidance suggests that key determiners include potential detriment to an individual (including emotional distress), the volume of the personal data loss, and its sensitivity. ICO guidance suggests that, where a company is unsure whether to report, the presumption should be to do so.

Once notified, the ICO has several options, ranging from taking no further action to requiring the company to take remedial steps or serving a monetary penalty notice of up to £500,000 if a company had deliberately or negligently failed to provide an appropriate level of data security. The ICO has released detailed guidance about issuing monetary penalties that are more likely if the ICO wants to set an example, where a company failed to take reasonable precautionary steps such as implementing adequate information policies and procedures or did not provide adequate staff training. There is no guarantee that a company would escape a monetary penalty entirely by self-reporting, but it may affect the penalty level, as would the vulnerability of the individuals affected, whether a company's senior management was involved, and a company's size and financial resources. In light of these, a self-reporting decision under the DPA regime requires careful prior consideration and breach reporting is rare; a survey by the Department of Culture, Media and Sport (DCMS) in April 2017 found that just 26 per cent of the most serious UK incidents were externally reported to entities other than companies' own cybersecurity providers.

Once the GDPR comes into force, a company's discretion over reporting data breaches will be curtailed; all personal data breaches will be reportable without delay and within 72 hours of

becoming aware of them, unless the breach is unlikely to jeopardise the rights and freedoms of natural persons. Breach reports will have to contain specific information, including the nature of the breach, the likely consequences and the measures taken to address it. Piecemeal disclosure will be permitted if not all the information is immediately available. Data processors (eg, outsourced data storage firms) will be similarly required to report data breaches to the company (as the data controller) without delay.

Where personal data breaches are likely to threaten the rights and freedoms of the data subject, the controller or processor will normally also be obliged to inform the data subject without undue delay, including advising on the likely consequences and the measures taken by the company to mitigate the risks. However, highlighting the potential significance of cybersecurity policies and incident response management plans, communication with the individual data subjects affected will not be required where the data controller had implemented appropriate technical measures (including encryption) and organisational protection, where it has taken subsequent steps to ensure the threat to data subjects as a result of the breach is unlikely to eventuate, and if it would involve disproportionate effort and a general public communication to inform the public would suffice.

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

MD & JH: The overriding issue for companies in the event of a data breach is damage limitation, both for those whose personal data has been compromised and for the company itself. That process begins well before an incident takes place, however, as advance planning is key in identifying and stemming a data breach, avoiding or minimising subsequent regulatory penalties, mitigating any civil claims that arise, protecting the company's brand and reputation, and defraying the costs resulting from an incident. Carefully thought-out cybersecurity policies are crucial. However, according to a DCMS survey in April 2017, only 33 per cent of UK firms currently have a formal policy covering cybersecurity risk. That figure is likely to rise as cybersecurity incidents become more commonplace and awareness of the potential penalties under the GDPR increases. If a serious incident occurs, having such a policy should help demonstrate to the regulator, data subjects and a potentially hostile media that the organisation had taken all reasonable steps to mitigate the risk.

While a cybersecurity policy should include technical matters such as antivirus software use, patch and security update downloads as well as backup recovery plans, a company would also be well advised to implement regular staff training to try to prevent situations arising in the first place. Eighty-five per cent of data breaches are said to arise from within organisations themselves as a result of, for example, laptops stolen from an office, inadvertent email disclosure of customer details or accidentally leaving sensitive documents on public transport. Adequate training should be undertaken to ensure staff recognise, understand and avoid the risks, as well as knowing what to do and who to alert in the event of a breach so that, should an incident occur, a company can accurately assess the situation and take immediate steps to minimise the harm.

Depending on the nature and extent of the data breach, an underprepared company risks being paralysed by hesitation in the event of a serious incident. To guard against this, and limit damage as far as possible, a company's cybersecurity policy should incorporate an incident response management plan, identifying who should handle the incident and the steps that should be taken. Internally, a senior member of the company should ideally take control, enlisting the assistance of in-house counsel, the IT department and HR, as well as external advisers as necessary.

The first priority must be to ascertain and record precisely what has occurred, who was involved and what data has been lost. A proper assessment can then be made of the nature and seriousness of the data breach, whether it is ongoing, how it can be stopped, and the likely implications for both data subjects and the company. Having done this, a reasoned assessment can be made about whether the ICO should be notified, and whether and how data subjects affected should be informed so they may take precautionary measures and mitigate any financial losses arising. Consideration should also be given to whether any contractual or professional notification obligations arise. For example, authorised firms should consider notifying the FCA and law firms should consider informing the Solicitors Regulation Authority. If necessary, sensible remedial measures can also be implemented within the company such as reviewing remote working practices, modifying data access and changing passwords.

If a company believes it has been the victim of crime, it may – and often will – decide to inform the police, and will consider whether any ensuing harm could be prevented by seeking injunctive relief.

Simultaneously, once news of a data breach gets out, a company may face questions from its staff and possibly external sources. The alacrity with which the company can investigate the incident, close it down and implement remedial measures will dictate the degree of reassurance that can be given to staff and the various external stakeholders concerned.

As the 2015 TalkTalk 'data hack' demonstrates, apart from reputational damage, the regulatory penalties arising from a data breach can be very serious. Added to these are the inevitable management costs and potential civil claims arising against a company. Underpinning any prudent cybersecurity policy, therefore, is cyber liability insurance to offset the potential expense of the incident. As of April 2017, however, only 38 per cent of UK companies said they had specific cover for this risk; many rely on general policies that are likely to be tightened up by insurers as a result. Historically, specific cyber liability insurance has been more common in jurisdictions with mandatory reporting of data breaches. As the GDPR implementation date draws nearer, more UK companies are likely to seek such cover to mitigate the financial risk associated with data incidents.

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

MD & JH: There is some mandatory specific sectoral guidance on cybersecurity, such as the Payment Card Industry Data Security Standard applicable to organisations handling payment cardholder data. More generally, in 2012, the government published its '10 Steps to Cyber Security' and, in 2013, 'Small businesses: what you need to know about cyber security', which both set out straightforward measures that organisations could take to improve cybersecurity preparedness. Subsequently, after identifying ongoing vulnerabilities, the government formulated its Cyber Essentials Scheme, which recommends that all organisations implement five basic controls to protect against cyberattack, including creating effective boundary firewalls, ensuring an appropriate level of system access and ensuring use of the latest supported application versions and patches. Those achieving these standards may then apply for accreditation under the Assurance Framework envisaged by the Scheme. All suppliers bidding for government contracts involving sensitive and personal data handling must be compliant with the Cyber Essentials controls (as of 1 October 2014). Despite this, the scale of the task to raise awareness became clear when figures released in April 2017 suggested that only 3 per cent of UK businesses had implemented the Cyber Essentials basic standard across their business.

Other sources of best practice advice include the Home Office Cyber Aware campaign (formerly Cyber Streetwise), the FCA's *Good Cyber Security – Foundations*, the ICO's *A Practical Guide to IT Security,* and guidance published on the National Cyber Security website and information available on Get Safe Online. Helpfully, the government has pulled much of this guidance together on one web page: www.gov.uk/government/collections/cyber-security-guidance-for-business.

Additionally, the government has published a non-technical Cyber Governance Health Check questionnaire aimed at FTSE 350 companies, enabling them to see what cybersecurity changes may be needed.

Despite (or perhaps because of) this plethora of guidance, the government's National Cyber Security Strategy 2016–2021 acknowledged that the majority of UK businesses and individuals were still not properly managing cyber risk. It's possible that the harsher penalty regime under the GDPR and the requirements of those providing cyber risk insurance policies will focus minds and encourage organisations to adopt the best practice guidance available.

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: According to International Data Corporation, the worldwide market for cloud computing services will grow from US$67 billion in 2015 to US$162 billion in 2020 as demand increases for large-scale data storage and management. Moving to a cloud hosting environment represents a way in which businesses can efficiently store and access the vast amounts of data they control.

Entrusting a third party with data that businesses control is a decision that should not be taken lightly, however. When deciding which cloud computing service to use, someone with the appropriate technical expertise should undertake the necessary checks on the provider to ensure that they provide sufficient guarantees and comply with the relevant regulations. The GDPR places responsibility not only on the cloud computing provider as a 'data processor' but also on the original holder or owner of the data as a 'data controller' (with whom responsibility ultimately rests). Responsibility is also placed on the data processor, namely, the cloud hosting environment, which has gained sufficient control over the manner in which the data is processed.

The major data security and privacy concern is that the location of cloud computing service users is generally less well controlled. Indeed cloud computing often involves the movement of data to a 'cheaper jurisdiction' and so the user may not be aware of the physical location where they are stored. Personal data can only be transferred to a non-EEA country if it is on the Commission's authorised list of nations providing adequate personal data protection. The DPA permits organisations to transfer data to a non-EEA location where organisations demonstrate that they meet the Binding Corporate Rules and satisfy the requirements of the Article 29 Working Party (WP29). It is important to note that the GDPR will replace WP29 with the European Data Protection Board, which is set to play a very significant

THE INSIDE TRACK

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

The prime requirement is for the lead lawyer to understand the technical issues sufficiently to be able to translate them into steps that make sense, both to the executives of the client and other lawyers, and more specifically in sometimes opaque information and criminal law contexts. The best lawyers have strong communication skills enabling them to intercede with and explain matters to technical experts and management, as well as with regulators and law enforcement bodies. Anticipatory judgement – being able to answer 'what next?' – is key.

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

Information law rarely mandates specific solutions. Rather the data protection principles provide required outcomes; how they are achieved is a function of guidance from the authorities, quite limited (but complex) case law, and the lawyer's skill and judgement in arriving at a solution that works practically, protects the client's interests and meets the legal requirements. In short, it is still the adviser's judgement that is of real value. The number of incidents and the still-developing roles of the NCA, NCSC and ICO in this field make working with the authorities a real test for any lawyer.

How is the privacy landscape changing in your jurisdiction?

It is, or should be, all about the GDPR and the need for data controllers and processors to understand and implement processes to meet the greater demands that the Regulation brings and that need to be in place by May 2018. Despite the statistics that demonstrate cybersecurity does not have the priority it ought to have, the 2017 ransomware attacks have the potential to provide the catalyst for real change in both the private and public sectors that good government policy and professional advice have seemingly failed thus far to achieve.

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

The 'weaponising' of ransomware through its joinder with self-replicating worms – seen in the recent 'WannaCry' attack – arguably represents a change in the way such assaults on companies are carried out. Attacks of this type will continue and, in some ways, large IT estates are more at risk given the complexities of legacy and imported systems that have not been the subject of scrutiny in the way that is now coming to be regarded as standard. Accompanied by an increased desire on the part of the ICO to investigate and punish data security failures, the danger to all institutions is that they will not simply be regarded as victims, as perhaps they should be, but malefactors themselves.

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

role in data protection compliance, including guidance formulation, codes of practice approval, certification schemes, and as the appellate body for GDPR disputes.

Just like internal IT systems, cloud hosting environments are also susceptible to server meltdowns. By way of example, an incident occurred in early 2017 when Amazon Web Services, the United States' largest cloud computing company, suffered a major outage affecting many major businesses including Airbnb, Netflix, Spotify and Apple Music. In order to safeguard against such occurrences, best practice suggests backing up data separately and also ensuring that cloud hosting environments have a comprehensive back-up system.

Another specific data security concern is the potential difficulty in encrypting data in a cloud hosting environment. Given the difficulties (and it is noteworthy that some providers are delivering and marketing security solutions) the presumption should be that cloud hosting environments are insecure and vulnerable to hackers who can access the data held there.

Further guidance has been published by the ICO on the use of cloud computing (see https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf). In 2012, the European Commission published 'Unleashing the Potential of Cloud Computing in Europe' (see http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy).

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

MD & JH: Acknowledging the many benefits that internet-based technologies have brought, the UK's National Cyber Security Strategy 2016–2021 notes that cyber criminals and hostile state-sponsored groups are enlarging their ambitions and expanding their stratagems to take advantage of online opportunities. Although the current technical capability of terrorist groups is considered low, this is also likely to increase

as a computer literate generation engages in extremism, threatening the UK and its interests.

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 National Cyber Security Centre (NCSC), which opened in February 2017. 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 March 2017, in conjunction with the NCA, NCSC published its 2016–2017 report on the cyberthreat to UK businesses, explaining the modus operandi of pivotal cyber incidents during 2016, including the hacking of the Democratic Party during the US presidential election, identifying emerging cyberthreat trends and providing advice on what businesses can do to fight back. Encouraging victims to report attacks is seen as a key component of the fightback, allowing the authorities to understand the true extent of cybercrime, investigate its perpetrators and improve future response. The UK authorities have set up the Action Fraud website for reporting online fraud, scams or extortion, while cyber incidents that may impact the UK's national security or economic wellbeing, affect a large portion of the UK population or jeopardise the continued operation of an organisation may be reported directly to NCSC.

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.

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

MD & JH: Given the nature of M&A work and the financial risks at stake, companies should be vigilant in the way they handle the data they control. Similarly, the lawyers and advisers involved must also be alert to data security issues given their professional obligations. The *Verizon/Yahoo!* deal, which closed in early 2017, is the paradigm example of how deals can be jeopardised through companies adopting a lax cybersecurity stance. After reaching a deal to sell Yahoo!'s core web business, it transpired that at least 500 million account details had been stolen in 2014. After Yahoo! announced the breach, Verizon said that it had only been informed of the scope of the breach two days earlier and wanted to reduce its original offer by US$1 billion. Eventually, the sale price was discounted by US$350 million and Yahoo! were severely criticised.

As the amounts 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 safeguard against grave consequences such as those seen in *Verizon/Yahoo!*. Scrutiny of the target company's data security policy and internal IT systems is a prerequisite. Such an investigation 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, and whether it destroys them and, if so, how. Specific enquiries about data breaches – known or suspected – are necessary. As a buyer, a company should first ensure that the target company actually has a comprehensive data security programme with sufficient technical security measures to protect personal information and sensitive personal information relating to clients, customers and employees. Companies should also carry out regular data risk assessments.

In M&A deals, there is the strong likelihood that a buyer's data security programme will differ somewhat from the target company. In this scenario, the two programmes should be aligned so that data protection is streamlined. Cross-border acquisitions present particular difficulties and information law requirements under EU and non-EU regimes must be understood and any conflicts resolved; seeking jurisdiction-specific advice is essential. Such alignment will bring about change so the companies involved will be under an obligation to forewarn their customers or clients of this. In some circumstances it may be necessary to gain affirmative consent from customers and employees before making changes to the data policies, particularly if the buyer company intends to use the data of the target company in a manner inconsistent with the target company's policy. On this particular topic, the ICO has issued guidance via the Data Sharing Code.

The consequences for acquirers failing to perform thorough cyber due diligence can be severe. In 2014, the online travel site TripAdvisor acquired tour booking company Viator for US$200 million. The transaction closed in mid-August 2014 and, approximately two weeks later, Viator announced it was subject to a data breach and that the personal details and credit card information for up to 1.4 million customers was compromised. As a consequence, TripAdvisor's stock fell by 5 per cent.

Also available online

www.gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law