Cybersecurity

Contributing editors
Benjamin A Powell and Jason C Chipman

2019

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2019

Contributing editors
Benjamin A Powell and Jason C Chipman
Wilmer Cutler Pickering Hale and Dorr LLP

Reproduced with permission from Law Business Research Ltd
This article was first published in January 2019
For further information please contact editorial@gettingthedealthrough.com

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

Law Business Research

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2015
Fifth edition
ISBN 978-1-912228-87-4

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

CONTENTS

Global overview 5
Benjamin A Powell, Jason C Chipman and Maury Riggan
Wilmer Cutler Pickering Hale and Dorr LLP

Cyber clouds and silver linings? 7
Edite Ligere

Australia 10
Alex Hutchens
McCullough Robertson

Austria 16
Árpád Geréd
Maybach Görg Lenneis Geréd Rechtsanwälte GmbH

China 22
Vincent Zhang and John Bolin
Jincheng Tongda & Neal

Denmark 28
Tue Goldschmieding
Gorrissen Federspiel

England & Wales 33
Michael Drury and Julian Hayes
BCL Solicitors LLP

France 42
Claire Bernier, Fabrice Aza and Damien Altersitz
ADSTO

Italy 47
Rocco Panetta and Tommaso Mauro
Panetta & Associati Studio Legale

Japan 55
Masaya Hirano and Kazuyasu Shiraishi
TMI Associates

Korea 62
Doil Son and Sun Hee Kim
Yulchon LLC

Malta 67
Olga Finkel and Robert Zammit
WH Partners

Mexico 73
Begoña Cancino
Creel, García-Cuéllar, Aiza y Enríquez, SC

Philippines 78
Rose Marie M King-Dominguez and Ruben P Acebedo II
SyCip Salazar Hernandez & Gatmaitan

Poland 83
Ewa Lejman and Kamila Spalińska
Żyglicka & Partners

Singapore 89
Lim Chong Kin and Shawn Ting
Drew & Napier LLC

Switzerland 97
Michael Isler, Jürg Schneider and Hugh Reeves
Walder Wyss Ltd

Ukraine 103
Julia Semeniy, Sergiy Glushchenko, Yuriy Kotliarov and Sergiy Tsyba
Asters

United States 108
Benjamin A Powell, Jason C Chipman, Leah Schloss and Maury Riggan
Wilmer Cutler Pickering Hale and Dorr LLP

Preface

Cybersecurity 2019

Fifth edition

Getting the Deal Through is delighted to publish the fifth edition of *Cybersecurity*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique **Getting the Deal Through** format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Denmark, Poland, Singapore and a new article on human rights and cybersecurity.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Benjamin A Powell and Jason C Chipman of Wilmer Cutler Pickering Hale and Dorr LLP, for their continued assistance with this volume.

GETTING THE DEAL THROUGH

London
January 2019

England & Wales

Michael Drury and Julian Hayes
BCL Solicitors LLP

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

There is no dedicated comprehensive cybersecurity law as such in England and Wales. Rather, there are numerous statute-based laws, underpinned by the possibility of civil actions in common law. These:

- criminalise unauthorised interference with computers – including where there is an intention is to commit other crimes by means of accessing computers, altering computer programs or producing 'hacking tools', or where the result is one of serious damage to the economy, environment, national security or human welfare, or where there is a significant risk of that (the Computer Misuse Act 1990 (CMA), as amended by the Serious Crime Act 2015 (SCA));
- criminalise the interception of communications – including communications sent or received by computers (the Investigatory Powers Act 2000 Part 1 (IPA));
- impose obligations to protect personal data (rather than data more generally) by the application of security measures. The three key pieces of legislation are the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA), and the Network and Information Systems Regulation 2018 (NISR), which implements the EU's Network and Information Security Directive; and
- criminalise actions amounting to fraud (Fraud Act 2006 (FA)) and infringing intellectual property rights (Copyright, Designs and Patents Act 1988).

It is important to note that significant changes have been brought about by the implementation of the GDPR and the Network and Information Security Directive agreed by the EU institutions in December 2015 (see question 3 and 'Update and trends').

Aside from emphasising in policy the benefits of good cybersecurity, therefore, English law predominantly seeks to encourage cybersecurity by punishing breaches (notably in failures by data controllers and processors to keep personal data secure) rather than by reward.

Acts that would otherwise be considered breaches of law are made lawful where conducted by state agencies principally in the interests of national security, and for the prevention and detection of serious crime, in accordance with the authorisation regimes established under IPA (see question 9), the Police Act 1997 and the Intelligence Services Act 1994.

Parliament has not legislated to promote cybersecurity as such, and the offences described have been created in a rather piecemeal fashion. The UK government has approached the issue of cybersecurity by seeking to raise awareness and to enhance cybersecurity safeguards against (and to mitigate the risks and effects of) cyberattacks. In November 2016, the five-year National Cyber Security Strategy containing three core pillars – to defend against and to deter cyberattacks, and to develop cyberdefence – was approved. The strategy is underpinned by £1.9 billion of transformational investment, more than double the budget of the first such strategy (2011–2016) (www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy). The strategy is supported by the National Cyber Security Centre (NCSC), which, in its 2018 Annual Review, noted that from September 2017 to August 2018, it had handled 557 cyber incidents; removed 138,398 unique phishing sites and issued 134 pieces of cybersecurity guidance. When businesses, government bodies or academic organisations report a significant incident, the NCSC may bring together and deploy the full range of technical skills from across government and beyond. The NCSC also links up with law enforcement, helps mitigate the impact of incidents, seeks to repair the damage and assists in the identification and prosecution of those responsible.

Of fundamental importance, the GDPR applies to personal data processing carried out by organisations operating within the EU and to those operating outside the EU that offer goods or services to individuals in the EU. It does not apply to processing carried out for law enforcement purposes (eg, the police, criminal courts), for national security purposes or to processing by individuals for purely domestic or household activities. Article 5 of the GDPR stipulates that personal data must be processed in accordance with seven principles:

- it must be processed lawfully, fairly and transparently (lawfulness, fairness and transparency);
- it must not be processed in a manner incompatible with the specific, explicit and legitimate purposes for which it was originally collected (purpose limitation);
- it must be limited to what is necessary in relation to the purpose for which it was collected (data minimisation);
- it must be accurate and kept up to date (accuracy);
- it must not be kept for longer than is necessary (storage limitation); and
- it must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality); and
- finally, data controllers must be able to demonstrate compliance with the principles relating to personal data processing (accountability).

A breach of the data processing principles – significantly in the context of security breaches – can lead to the imposition of substantial administrative fines imposed by the Information Commissioner's Office (ICO). The ICO may also prosecute offenders in the criminal courts for offences under the DPA. Those suffering damage (including distress) from breaches of the data protection legislation may also seek compensation from the controller or processor concerned.

The DPA enacts the EU's Law Enforcement Directive, which regulates the processing of data by various authorities such as the Serious Fraud Office, the Financial Conduct Authority (FCA) and the National Crime Agency (NCA). In addition, the DPA complements and amplifies the provisions of the GDPR.

NISR applies to operators of essential services (OES) (eg, water, transport and energy) and relevant digital service providers (RDSPs) (eg, online search engines available to the public, online markets and cloud computing services). NISR requires appropriate and proportionate technical and organisational measures to manage risk of disruption. Incidents that 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, operators are also strongly encouraged to contact the NCSC.

In terms of the principal criminal law deterrent, the CMA, implementing the Budapest Convention on cybercrime, provides for criminal offences on the basis that: (i) a person causes a computer to perform any function with intent to secure access to any program or data held in any computer or to enable any such access to be secured; (ii) the access he or she intends to secure or to enable to be secured is unauthorised; and (iii) he or she knows at the time when he or she causes the computer to perform the function that this is the case, he or she is guilty of an offence. Such offences are punishable by imprisonment, some carrying a maximum sentence of life imprisonment where the attack causes or creates a significant risk of serious damage to human welfare or national security.

Securing access to a computer or a program encompasses many different actions. 'Computer' is not defined in the CMA. Access is said to be unauthorised if done by a person other than one who has responsibility for the computer and is entitled to determine whether the act may be done, or is done without the consent of such a person.

The CMA creates further offences where unauthorised access is sought with a view to committing other offences (eg, theft or fraud), or to impair the operation of a computer, which would include the implanting of viruses or spyware and DDoS attacks. In such cases, the penalty can be up to 10 years' imprisonment. The CMA also criminalises the obtaining, making, adapting, supplying or offering of articles to be used in committing the CMA offences.

Subject to particular statutory defences, the DPA criminalises certain behaviour in relation to personal data, including knowingly or recklessly obtaining or disclosing it without the consent of the controller (blagging). It is also an offence to retain personal data without the consent of the controller from whom it was obtained; to offer or sell 'blagged' personal data; to 're-identify' personal data that has been de-identified (ie, processed in such a manner that, without more, it can no longer be attributed to a particular data subject) without the controller's consent; or to process such re-identified data. Other criminal offences are dealt with under the relevant questions below.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Cybersecurity laws and regulations affect all businesses and organisations processing or controlling data. The GDPR applies specifically to personal data, that is data from which a living person can be identified. As such, cybersecurity laws and regulations affect all sectors of the economy.

Presently, there are no specific sectoral laws (except, to some extent, for the providers of public communications services – see question 3), but businesses of any size must meet the GDPR requirements to the extent that they process personal data. Extensive guidance is now addressed to all businesses and sectors because of the pervasive nature of the threats. It tends to be structured around the types of attacks, rather than the industries. There are some examples of sectoral guidance, for example, the Payment Card Industry Data Security Standard (PCI DSS), which must be complied with by all organisations that accept, store, transmit or process cardholder data. The finance sector, where there is an obvious risk of fraud, may be thought to have considered cybersecurity matters for longer, and in greater depth, than other sectors. Cybercrime is now the UK's number one fraud, according to the 2018 PWC Global Economic Crime Survey, with 25 per cent of all participating UK organisations reporting experience of cybercrime within the past two years. There are encouraging signs that UK organisations are taking greater care to minimise the risk of cybercrime (and minimising the harm when it occurs). A higher number of UK firms than the global average now have cybersecurity programmes in place. However, surveys indicate the UK still lags behind the global average in the use of advanced technology such as predictive analytics and machine learning to identify cyber-enabled fraud.

Professional bodies and regulators are increasingly engaged in cybersecurity initiatives, at times embedding national strategies and guidance into their own regulatory guidance. The Law Society contributed to the NCSC's 2018 report on cyberthreats to the UK legal sector (https://www.ncsc.gov.uk/legalthreat) and its website includes a page dedicated to practical cybersecurity advice, educational webinars and endorsed partner products and services to help mitigate cybersecurity threats. In the financial sector, the FCA has prioritised cybersecurity through 'soft guidance' measures, including senior-level speeches on the subject, while simultaneously emphasising the regulatory obligation to report material cybersecurity incidents under Principle 11 of the FCA Handbook.

Failure to protect data adequately may give rise to breaches of regulatory requirements. The FCA has levied penalties for data breaches where they have been found to constitute breaches of FCA Principle 3, that is, the obligation to take reasonable care to organise and control a regulated entity's affairs responsibly and effectively with adequate risk management systems. In October 2018, the FCA imposed a fine of £16.4 million on Tesco Bank for failures to protect its customers against a cyber attack in November 2016 when, over a 48-hour period, cyberattackers stole £2.26 million from current account holders using 'virtual cards' to undertake thousands of unauthorised debit card transactions. Significantly, data breach reports to the FCA more than tripled during 2017. Despite this, the FCA has expressed suspicion that there remains a material under-reporting of successful cyberattacks in the financial sector (https://www.fca.org.uk/news/speeches/effective-global-regulation-capital-markets).

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Although the United Kingdom voted to leave the European Union on 23 June 2016, the subsequent years have witnessed the government implementing several far-reaching pieces of European legislation that will fundamentally alter the regulatory landscape for UK cybersecurity and data protection: the GDPR, the Law Enforcement Directive and the NISR. By doing so, the government's clear aim is to ensure that the UK's cyber and data protection laws are as closely aligned as possible to those of the EU, thus removing potential obstacles to the UK obtaining a data protection 'adequacy decision' from the EU post the transition withdrawal period and Brexit, enabling unimpeded data-flows between the UK and the EU. Indeed, the government's draft EU withdrawal agreement, announced on 14 November 2018, specifically states that, during the proposed 21-month transition period, the European Commission will begin its adequacy considerations and that, until such a decision is reached, the EU's data protection laws will continue to apply in the UK. Thereafter, the UK is committed to maintaining 'essential equivalence' to the EU in respect of data protection. As a result, European Union has, and will continue to have, a key role in setting standards for the UK.

Regulation (EU) 2016/679 (the GDPR) is directly applicable in UK, and took effect in the UK on 25 May 2018: it governs the treatment of personal data throughout the EU (see question 1). Several of its key provisions should be noted in the cybersecurity context. The first is a uniform requirement for notification of security breaches (see questions 16 and 24). There is also a requirement to notify the affected data subjects if a 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 high risk effectively. Second, the GDPR affects both data controllers and processors. It includes the obligation to implement technical and organisational security measures, appropriate to the specific risks that are present.

The GDPR sets out detailed rights of individuals in relation to data processing, which includes the right to access personal data, the right to rectification and the right to erasure of information where, for instance, it is no longer necessary for it to be held or consent has been withdrawn and there is no other legal ground for its retention.

Directive (EU) 2016/680 (the Law Enforcement Directive) is transposed into UK law in Part 3 of the DPA and relates to the processing of personal data for law enforcement purposes (the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties). It complements the GDPR and sets out the principles with which data controllers must comply when processing personal data.

Directive (EU) 2016/1148 ('security of network and information systems') is implemented in the UK by means of NISR. It specifies a high common level of security of network and information systems across the EU. NISR applies to OES and RDSPs and its primary focus is cybersecurity.

In addition, Directive 2013/40/EU aimed to create a unified approach to the types of and punishments for cyber offences through the EU. The Directive was given effect in the UK by the SCA, which amended the CMA to include new and extend existing offences,

and increased the maximum penalty for some cyber offences to life imprisonment.

Finally, Directive 2002/58/EC is implemented in the United Kingdom by the Privacy and Electronic Communications Regulations 2003 (PECR), which impose obligations on providers of public electronic communications services to take appropriate technical and organisational measures to safeguard the security of their services.

At a non-governmental level, the International Organization for Standardization's ISO 27001:2013 sets out information security standards, including requirements for the assessment and treatment of risks tailored to the needs of an organisation, as well as generic requirements applicable to all organisations. It includes standards of leadership and commitment to information security management by senior management, requirements for planning action, implementation and evaluation, and sets out requirements for resources, competence and awareness as well as proper communication and documentation of arising issues. ISO 27000:2016 provides an overview of information security management systems, and terms and definitions commonly used in the Information Security Management System family of standards.

The ISO has not been formally adopted as a legal requirement to meet government standards, and is, in fact, insufficient to meet the 'UK Cyber Essential and Cyber Essentials PLUS' certificates (see question 13). The Cyber Essentials scheme does, however, recommend the ISO to executive management, as supporting standards in addition to its own. Further, although there has been no formal adoption of these standards, if an organisation does adopt and apply them to its data operations, this would give comfort that in the event of a civil suit, civil penalty or even in the event of a prosecution for a DPA offence, the organisation should be able to advance an arguable defence (see question 9).

How the UK will continue to participate with international bodies concerned with cybersecurity post-Brexit has been the subject of considerable debate. In a speech in November 2018, the CEO of the NCSC stated that the UK's departure from the EU would not have an impact on levels of UK–EU cybersecurity and cooperation and that the UK government's clear instruction was to continue to work with EU counterparts unconditionally. This reflects the sentiment expressed in the government's 2017 policy paper, 'Foreign policy, defence and development – a future partnership paper', which recognised cyberthreats know no international boundaries, and set as its aim a 'deep security partnership' with the EU (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643924/Foreign_policy_defence_and_development_paper.pdf). It is hoped that, post-Brexit, the UK will continue to participate as a 'third country' in EU cybersecurity bodies such as the European Union Agency for Network and Information Security (https://www.enisa.europa.eu/about-enisa) and the NIS Co-operation Group.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Responsible personnel and directors have the normal obligations to act in the interests of those corporate bodies that they represent (as embodied in the DPA, as well as the Companies Act 2006 (CA) and elsewhere). For instance, section 174 of the CA 2006 requires a company director to attain the standards of 'a reasonably diligent person with . . . the general knowledge, skill and experience that may reasonably be expected of a person carrying out the functions carried out by the director in relation to the company . . .'. Personal liability could follow in certain circumstances for breaches where it is found that directors failed to meet those standards. Section 198 DPA also provides for liability of directors and officers for certain offences committed with the consent of, or that are attributable to the negligence of, the director. Article 82 GDPR provides for liability of data controllers and processors for breaches of their GDPR obligations. These obligations require the processing of personal data in a manner ensuring appropriate security, including protection against unauthorised or unlawful processing (article 5(1)(f) GDPR).

Ultimately, data protection liability rests with the organisation in question, but the above will have a significant impact on company directors and officers, who are likely to be held increasingly accountable for inadequate cybersecurity.

5 How does your jurisdiction define cybersecurity and cybercrime?

Cybersecurity and cybercrime are hard to define. Cybercrime, for example, could mean anything from an individual being targeted by an email scam to a state-sponsored attack against another state's infrastructure (or anything between these two extremes). There are no specific legal definitions for 'cybersecurity' and 'cybercrime'; the thinking is certainly dominated by data protection concepts, but has now spread beyond that. For the latter, the clearest definition is provided in the government's National Cyber Security Strategy, which states that it consists of two interrelated forms of criminal activity: cyber-dependent crimes that can only be committed through Information and Communications Technology (ICT) and cyber-enabled crimes that are traditional crimes 'scaled-up' by the use of ICT.

According to the NCA, common cyberthreats for businesses remain hacking and DDoS attacks. For consumers, they are larger in number: phishing, webcam manager, file hijacking, keylogging, screenshot manager and ad clicker.

The NCSC defines a cybersecurity incident as a breach of a system's security policy to affect its integrity or availability and the unauthorised access or attempted access to a system. Commonly occurring incidents falling within the first category include attempts to gain unauthorised access to a system or data, malicious disruption and denial of service. By contrast, significant cybersecurity incidents are those that impact on the UK's national security or economic well-being.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Given the variety and complexity of the UK economy, a 'one-size-fits-all' approach to cybersecurity would be impractical. The legislation therefore adopts a risk-based approach rather than prescribing specific measures. The GDPR, for example, requires entities falling within its scope to process personal data in a manner that 'ensures appropriate security'. Similarly, NISR requires OES to take 'appropriate and proportionate technical and organisational measures' to manage risks posed to the security of the systems on which they rely.

It is a matter for regulated entities to determine how best to achieve such standards, taking into account technological advances and matters such as implementation cost, risk and the potential impact of a security breach.

See question 2 in relation to PCI-DSS applied to cardholder data security.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Although there are no specific laws or regulations addressing cyberthreats to intellectual property, these are addressed by both criminalising the way in which it would be unlawfully obtained and by criminalising its improper use.

The purpose behind the offences listed in question 1 may perhaps not have been to protect intellectual property, per se. Nonetheless, obtaining intellectual property by means of cyberattack would be covered by many of the offences under the CMA and the FA, notably fraud by false representation, given that the offence covers any act whereby an individual dishonestly makes false representations to make a gain or cause a loss. This can include purporting to be the person to whom the data relates or belongs.

The use of the data that has been misappropriated will often also be criminal. Section 107 of the Copyright Designs and Patents Act 1988 establishes a range of offences committed by those who for commercial purposes infringe copyright by making or dealing with infringing articles when they know or have reason to believe they are infringing. This is likely to catch individuals threatening intellectual property using cyber methodologies. Punishments for offences under this section vary in their maximum sentences, with the most severe offences carrying a maximum sentence of 10 years' imprisonment and a fine.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Critical national infrastructure and sectors providing essential services are likely to fall within the definition of an OES under NISR (see question 1). As such, they must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential services rely, and take appropriate and proportionate measures to prevent and minimise the impact of security incidents affecting those systems. Penalty notices may be imposed on the relevant competent authority where a particular OES fails to achieve to these standards.

Where attacks do take place, perpetrators may be prosecuted under the CMA for knowingly using a computer for an unauthorised purpose that causes or creates a significant risk of damage to human welfare, the environment, the economy or national security of any country (section 3ZA CMA). The infrastructure and sectors that this law seeks to protect from 'disruption' include food, energy, fuel and water, in addition to communication and transport networks and health services. Offences under this section where there is a significant risk of serious damage to human welfare or national security carry maximum sentences of life imprisonment (with 14 years' imprisonment for any other offence under this section).

Despite the precautionary measures required by NISR, the NCSC has warned that bad state actors are showing an increased appetite for attacks on critical sectors, often targeting vulnerabilities exposed through legacy industrial control systems that, though increasingly networked, were not designed with cybersecurity in mind.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

There is nothing restricting private entities from sharing cyberthreat information, subject to compliance with the GDPR and standard confidentiality considerations. In fact, the government actively encourages effective sharing to tackle cyberthreats and improve cybersecurity. The Cybersecurity Information Sharing Partnership (CiSP) was established as a joint industry–government initiative to share information about cyberthreats and vulnerabilities. It includes members across all sectors and organisations, and facilitates the exchange of cyberthreat information in real time within a framework that protects confidentiality of shared information. More localised information-sharing schemes include the Cyber Griffin initiative, set up by the City of London Police (CoLP) to help people working in the City by offering briefings on current cybercrime threats and teaching effective defence skills. Recognising that cyberthreats are international, efforts are also under way to coordinate cross-border information sharing: for example, CoLP also promotes the Global Cyber Alliance, including the Quad9 initiative, which uses threat intelligence from leading cybersecurity companies to keep participants safe from sites containing known malware.

Sections 19–21 of the Counter-Terrorism Act 2008 allow state authorities to share intercepted material or other national security-sensitive information with other intelligence services and also private entities if in pursuit of national security or the prevention of serious crime. Section 19 absolves any individual or entity of liability for breach of confidentiality where it is sharing information for national security purposes or for the prevention of serious crime. Similar provisions exist under section 7 of the Crime and Courts Act 2013 for disclosure to the NCA.

There are limitations on sharing information obtained by interception. Where a government agency has, under warrant, intercepted communications in the interests of national security or for the prevention of serious crime it is a criminal offence under the IPA for a person in that service provider or for a public official to divulge the existence and content of the warrant or authorisation. Other information from government bodies can be shared provided it is compatible with their own statutory foundations (if any) and the requirements of the Human Rights Act 1998 (HRA).

Article 8 of the European Convention on Human Rights (the right to privacy and freedom of correspondence) given effect through the HRA, pervades this entire area, insofar as privacy might be infringed by domestic public authorities, and limitations to that right must be in accordance with law, proportionate and necessary only for the purposes prescribed in article 8(2), that is in the interests of national security or to prevent or detect crime.

Under the GDPR, every data controller must identify a lawful basis for 'processing' personal data. Processing is a broad term encompassing almost anything involving the data, including its disclosure.

Lawful processing necessitates that one or more of the conditions in GDPR article 6(1)(a)(f) applies (see question 1).

Subject to statutory defences, it is a criminal offence under the DPA for any person knowingly or recklessly, and without the consent of the data controller, to obtain, disclose or procure the disclosure of personal data, or to retain it without the data controller's consent after obtaining it. Similarly, it is an offence to sell or offer personal data for sale where it was obtained illegally under the DPA. Prosecutions would normally be brought by the ICO but those convicted of such offences may only be fined. However, demonstrating an increasingly assertive prosecutorial stance, in November 2018, the ICO successfully prosecuted an individual for unauthorised access to personal data under section 1 CMA, which carries a potential custodial sentence. Afterwards, the ICO stated, 'Members of the public and organisations can be assured that we will push the boundaries and use any tool at our disposal to protect their rights.'

In addition to the ability to prosecute, the ICO has a range of regulatory tools at its disposal, including enforcement and 'stop now' notices (such as that imposed on Canadian firm AggregateIQ Data Services Ltd in October 2018 for illegally processing the personal data of UK citizens) and the imposition of potentially severe monetary penalties for GDPR breaches (see questions 23 and 24).

Where a private party is connected to civil proceedings (but is not directly involved), disclosure of information (eg, personal data) may be possible by an application to the court for a *Norwich Pharmacal* order. Unless there is a need for secrecy or urgency, an application should be made on notice to the respondent and the draft order should specify the information being sought, which may also impose a 'gagging order' to restrain the respondent from informing anyone about the application.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The CMA prohibits unauthorised access to computer material or data (ie, hacking (section 1)). It is also an offence to carry out unauthorised acts designed to impair computer systems, which include the deployment of Trojan horses or worms (section 3). The latter offence can carry a prison sentence of up to 10 years and an unlimited fine on conviction in the Crown Court. It is also an offence to use or obtain for use articles to commit either of the first two offences mentioned. (See also questions 1 and 8.)

The unlawful interception of information is governed by the IPA. The framework is contained in Part 1 of the IPA and the offence of unlawful interception is contained in section 3. The maximum punishment for breaching this provision is contained in section 3(6)(c); namely two years' imprisonment and a fine.

The offence of unlawfully obtaining personal data is now found in section 170 DPA 2018 (see question 9).

These offences can be committed by a corporation, where liability can be attributed to such a legal person through the actions of its directors and officers and those who are senior enough to bind the corporation.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

According to the International Data Corporation, the worldwide market for cloud computing services is expected to grow from US$67 billion in 2015 to US$162 billion in 2020 as the need increases for businesses and individuals to manage and store large amounts of data.

Cloud computing enables convenient on-demand network access to a shared pool of configurable resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Moving data to a cloud hosting environment therefore represents a way businesses can efficiently store and access the vast amounts of data they control. However, with that comes data security and privacy concerns.

The responsibility for ensuring adequate protection ultimately lies with the data controller, namely, the original holder or owner of the data. The same responsibility is also placed on the data processor,

namely, the cloud service provider, where it has gained sufficient control over the manner in which the data is processed; it is essentially treated as a data controller. The responsibility exists whether the data is being held or is in transit. Mitigating risk involves undertaking checks on a cloud service provider (by someone with appropriate technical expertise) to ensure it provides sufficient guarantees and takes reasonable steps to ensure GDPR compliance.

NISR applies to cloud computing services and imposes further obligations on OES (see questions 1, 8 and 27).

Further guidance has also 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).

Just like internal IT systems, cloud hosting environments are also susceptible to server meltdowns. A 2017 example occurred when Amazon Web Services, the United States' largest cloud computing company, suffered a major outage affecting many major businesses such as Airbnb, Netflix and Spotify, with Apple services such as Apple Music also affected. It is, however, debatable whether local server provision is more secure than cloud storage.

As cloud-based storage expands and the technology improves, the general consensus is that cloud, is in fact, more secure. The reasons for this include: the dissemination of data across multiple locations – cloud providers typically store at least three copies of every piece of data in separate locations meaning that all three locations would have to fail simultaneously for the data to be lost; the ability to essentially remove the threat of an employee or anybody physically removing a hard drive; the ability to create specific access credentials thereby controlling who in the entity sees what; and the improved chances of recovering data held in multiple locations.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

As the EU has harmonised cybersecurity laws and regulations across member states, organisations throughout Europe are likely to have very similar standards and obligations to those in the UK. That said, variations are likely to remain with some countries regarding GDPR standards as the baseline in data protection and others seeing it as the 'gold standard'. However, third country organisations processing or storing personal data of any EU subjects outside the EU are likely to be prevented from doing business in the UK or with UK individuals if their own national security requirements and regulations are inadequate. In other words, they must offer protection 'essentially equivalent' to that existing within the EU (following the *Max Schrems* case in the European Court of Justice) (see questions 3 and 11).

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Although much guidance has been issued by governmental bodies, ultimately, it has been left to organisations themselves how they achieve the legal standards expected of them in respect of cybersecurity (see question 6).

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 cyberattack, 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 sectoral-specific guidance such as the Payment Card Industry Data Security Standard, ISO/IEC 27001, published in 2013, enforcing tight controls surrounding the storage, transmission and processing of cardholder data handled by business. In addition, BS 10012:2017 provides a GDPR-compliant personal information management system available to organisations seeking to achieve best standards.

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 and https://www.fca.org.uk/publication/documents/cyber-security-infographic.pdf). These 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 cybersecurity. Additionally, the ICO's Regulatory Action Policy (awaiting parliamentary approval) suggests adherence to such codes will be considered when the regulator decides whether and by how much to penalise an organisation for a data breach.

14 How does the government incentivise organisations to improve their cybersecurity?

In December 2016, the government published its Cybersecurity Regulation and Incentives Review, which in part addressed incentives to boost cyber risk management across the wider economy. After widespread stakeholder consultation, the review concluded that, without wishing to overburden business, increased regulatory requirements should be matched by a wider uplift in support and information. An option that garnered considerable support from stakeholders was the introduction of an 'official' cyber health check, which would demonstrate the appropriateness and sufficiency of an organisation's security measures. Though many private organisations contributing to the review also enthusiastically sought financial incentives to improve cybersecurity, the government pointed out that basic rate tax relief was already available for business expenditure in this area and the potential cost to government of enhanced tax relief would be high.

Notwithstanding financial constraints, one of the 2017/2018 objectives of the government's Innovate UK scheme, which offers investment in micro, small and medium-sized business projects, was the encouragement of smart and resilient infrastructure fit for the digital revolution. Additionally, the government's 'G-Cloud' framework on the digital marketplace enables public sector authorities to invite private sector organisations to provide cloud-hosting, software and support without the need to resort to a formal tender process. The NCSC now offers reassurance by certificating expertise, products and services offered for sale to end users (https://www.ncsc.gov.uk/marketplace). Organisations bidding for central government contracts have needed to be 'Cyber Essentials' certified since 1 October 2014.

See also question 13.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

There is no equivalent of the IT Industry Council 'Cybersecurity Principles for Industry and Government' which appeared in the US. However, the Confederation of British Industry has sought to raise awareness of data security issues amongst its members, publishing the results of its survey 'Building Trust in the Digital Economy' (www.cbi.org.uk/index.cfm/_api/render/file/?method=inline&fileID=FFA34BD4-686F-4AEB-953DB1588A4D3764) in September 2018, hosting an annual cybersecurity conference in partnership with leading governmental bodies in the field, including the NCSC and ICO, and making a podcast available containing best practice advice on becoming cyber secure (www.cbi.org.uk/news/podcast-cybersecurity/). In addition, industry regulators will often direct those seeking cybersecurity advice to government sources such as the '10 Steps to Cyber Security'.

See questions 13 and 14.

16 Are there generally recommended best practices and procedures for responding to breaches?

Under the GDPR, data controllers must normally report personal data breaches to the ICO without undue delay and within 72 hours of becoming aware of them unless there is unlikely to a risk to the rights and freedoms of natural persons. Where the data breach results in a high risk to those rights and freedoms, the data controller must also inform the relevant data subject without undue delay. Under the PECR, which apply to organisations sending electronic marketing to the public,

organisations such as telecoms providers and internet service providers are obliged to notify the ICO within 24 hours of detecting a breach.

Notification may be made to the regulator by telephone during normal office hours or online (https://ico.org.uk/for-organisations/report-a-breach/). The online forms indicate the information that the ICO expects to be provided by those making such reports. Incidents that are notifiable to the ICO under NISR (see question 27) may also be made to the ICO via these methods.

In addition to ICO reporting obligations, in May 2017, the FCA published guidance confirming that regulated firms must report 'material' data breaches under their Principle 11 obligations.

Despite the increased stringency of reporting obligations, there is no single source of best practice for responding to data breaches. Instead, multiple sources of public and private, national and overseas guidance exists. Reflecting the often overlapping nature of such guidance, joint advice is increasingly offered such as the GDPR Security Outcomes guidance from the NCSC and ICO (https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes). This includes sections on avoiding, and planning for, breaches.

Carefully thought-out cybersecurity policies and rehearsal are crucial, particularly given the time constraints for reporting to the ICO. However, according to the 2018 Cyber Security Breaches Survey commissioned by the Department of Culture, Media and Sport (DCMS), only 27 per cent of UK businesses currently have a formal policy. That figure is likely to rise as cybersecurity incidents become more commonplace and awareness of the potential penalties under the GDPR increases through regulatory action. Though 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. Adequate training should be undertaken to ensure staff recognise, understand and avoid the risks, as well as know 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.

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 Human Resources, as well as external advisers (eg, forensic experts, lawyers and PR consultants) as necessary. Such external consultants should ideally be identified before an incident occurs.

In the event of an incident, best practice suggests that 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, as well as the likely implications for both data subjects and the organisation.

Having done this, a reasoned assessment can be made about whether the GDPR reporting threshold has been reached, 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 solicitors' firms should consider informing the Solicitors Regulation Authority (SRA). 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 decide to inform the police, the NCA or the NCSC 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, necessitating a coordinated media response.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Encouraging organisations to report attacks is seen as key to combatting such incidents. There are no government requirements or incentives as such, although the government has tried to promote the sharing of information about cyberthreats through CiSP (see question 9). The UK authorities have also set up the ActionFraud website for reporting online fraud, scams and extortion. Cyber incidents may be reported directly to the NCSC where they impact on the UK's national security, economic well-being, affecting a large proportion of the UK population or jeopardise the continued operation of an organisation. Statutory measures to encourage cyberthreat information include the 'information gateways' in the Counter Terrorism Act 2008 and the Crown and Courts Act 2013, albeit where personal data is provided via these gateways, compliance with the DPA is still required (see question 9). The encouragement of collaboration is evidenced by the ICO's 'Protecting personal data in online services: learning from the mistakes of others' report (https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf).

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

In November 2016, the National Cyber Security Strategy up to 2021 (www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 acknowledged the transformation that digital connectivity was bringing about for both public and private enterprise but emphasised the significant role played by businesses and organisations in the UK's national response to cyberthreats.

Recognising the importance of partnership between government and private sector in the development of cybersecurity standards, the NCSC's website has a dedicated partnership page listing efforts aimed at developing cross-sector cybersecurity capabilities within the UK. Included are details of educational bursaries and work placements to nurture the future cybersecurity workforce, educational events aimed at existing cybersecurity professionals, and the Industry 100 initiative to facilitate close collaboration with private sector talent in the field of cybersecurity by encouraging part-time secondment to the NCSC to promote the exchange of knowledge and expertise.

On the industry side, 'techUK', represents more than 950 commercial entities involved in the cyber-sphere, including FTSE 100 companies, small and medium-sized enterprises and start-ups. The body works with key stakeholders to inform debate about the future development and application of technologies. As part of the Cyber Growth Partnership, a joint initiative between industry, academia and government that aims to boost the UK's global market position in cybersecurity products and services, techUK promotes the Cyber Exchange, enabling participants across industry, academia and government to interact on issues arising in cybersecurity. Recognising the underrepresentation of women in the cybersecurity sector, techUK has also launched an initiative to promote and encourage the involvement of women in this heavily male-dominated field.

In conjunction with industry, the DCMS has developed the Cyber Security Suppliers scheme whereby businesses can advertise that they supply cybersecurity products and services to the UK government and use the government's logo in their marketing material. The intention is to provide assurance to the private sector of the efficacy and operability of cyber-defence products.

In 2017, DCMS launched its Digital Skills Partnership (DSP) through which UK government, businesses, charities and voluntary organisations joined forces to give people of all ages the opportunity to boost their online know-how by offering free training in areas such as basic online skills through to cybersecurity and coding. DSP has set itself four priorities: increasing digital skills provision, developing local or regional partnerships, assisting small businesses and charities to digitally upskill their employees, and supporting educationalists in the field of computing.

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

In principle, insurance cover is available to mitigate cybersecurity risks. Although, the market is often considered underdeveloped. As a result of the potential risk exposure and the shortage of actuarial data resulting from underreporting, insurers have been cautious to provide policies. Nevertheless, as incidents and consequences of cybersecurity breaches increase, demand for such insurance is also increasing, particularly given the mandatory reporting requirements under the GDPR.

The UK government has been working with the insurance sector for some time to highlight the importance of cybersecurity insurance

in an attempt to bolster the UK's reputation as a world centre for cybersecurity insurance. On 5 November 2014, they issued a joint statement (www.gov.uk/government/uploads/system/uploads/attachment_data/file/371036/Cyber_Insurance_Joint_Statement_5_November_2014.pdf), emphasising the 'strong role' of cyber insurance in mitigating cyber risks, specifically in relation to 'malicious attacks'.

A government report in 2015 noted the gap in awareness of the use of insurance, evidenced by the large number of firms unaware that insurance was even available; around 50 per cent of CEOs believed their companies have some form of coverage in place. As of April 2017, however, only 38 per cent of UK companies said they had specific insurance cover for cyber risk, with many continuing to rely on general insurance policies. Companies may find that, as breaches become more commonplace, insurers will restrict reliance on such general policies.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

In terms of cyberattacks, the law enforcement body with prime responsibility for investigations is the NCA, which has a dedicated cybercrime unit (www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit). As with other crimes, the criteria that would allow prosecution by the Crown Prosecution Service – a reasonable prospect of success and it being in the public interest – apply to cybercrimes. The NCSC takes on the role of protecting critical services from cyberattacks, managing major incidents and improving underlying security through technology and advice. The NCSC has a staff of 740 and a budget of £285 million for 2016–2021. It also supplements its workforce with secondees from the private sector. Despite the widespread admiration the NCSC has attracted in its first two years of operation, commentators have noted the risk that its resources will become overstretched as demand grows for its expertise and assistance. The ICO enforces the DPA and the GDPR in the civil jurisdiction, and the DPA in the criminal sphere (https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/).

Where national security is at risk, the UK's security and intelligence agencies will be involved.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The powers of the authorities to monitor and investigate for criminal offences under the CMA are the same as those in respect of criminal investigations generally. Material can be obtained by the NCA or the police through court orders (and searches without notice can be carried out with the appropriate permissions). Covert surveillance and interception are also possible, again with the necessary permissions having been obtained under the IPA (and its predecessor the Regulation of Investigatory Powers Act 2000, in relation to physical evidence). Intercept evidence is generally not admissible in criminal proceedings in England.

The ICO's role and powers are set out in Parts 5 and 6 of the DPA. The types of regulatory action in which the ICO engages are described in its Regulatory Action Policy. Those activities include conducting assessments of compliance with data protection legislation, issuing urgent information notices to data controllers and processors, issuing assessment notices requiring data controllers and processors to permit an assessment of compliance with data protection legislation, issuing reprimands and enforcement notices and administering fines by way of penalty notices. Significantly, the ICO also has the power to prosecute criminal breaches of the data protection legislation, and the indications are that it is showing a greater willingness to do so. The principal criminal offences in this regard relate to the unlawful obtaining of personal data (section 170 DPA), although it is showing increasing willingness to prosecute under alternative legislation where possible (see question 9). The ICO's powers of entry and inspection are set out in DPA, schedule 15. It is a criminal offence to obstruct a person executing an ICO warrant.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

There have been very few prosecutions for cyberattacks. A November 2018 prosecution of those responsible for the 2015 attack on TalkTalk ended in prison sentences for two 'hackers'. Such prosecutions are rare. In fact, figures from the Office for National Statistics show a decrease of prosecutions under the CMA. However, this is likely to change given the increasingly prevalent threat. In 2016, the NCA published a CyberCrime Assessment outlining the immediate threats to UK businesses, noting that the growth of cybercrime was outstripping the UK's collective response and noted that under-reporting of incidents hampered the efforts of law enforcement to understand the operating methods of cybercriminals and take effective counter-measures. The NCA and NCSC worked together to produce a video report on 'The cyber threat to UK business 2017–2018 report' (https://www.ncsc.gov.uk/threats. The report states that 5.7 million businesses in the UK are at risk from cybercrime. The report discusses the effects of the recent WannaCry, Uber and Moller Maersk cyberattacks, and suggests that, by the end of 2018, the internet of things will connect 11 billion gadgets with all the potential vulnerability that this entails.

The NCSC, along with the Law Society, produced a 2018 report entitled, 'The cyber threat to UK legal sector', with the most common being: phishing; data breaches; ransomware and supply chain compromise, such as the exploitation of third party data stores or software providers. The report discusses several factors that make law firms an attractive target, namely the possession of sensitive client information and significant funds. According to the SRA, over £11 million of client money was stolen by means of cybercrime in 2016 – 2017 (https://www.ncsc.gov.uk/threats).

In July 2018, the Ministry of Justice announced plans to build a new flagship cybercrime court in London. Expected to be completed by 2025, the premises will house 18 court rooms and it is hoped will expedite the legal process as regards data protection issues.

For the ICO's enforcement powers, see question 21.

For companies that receive a monetary penalty, the scrutiny does not stop after an initial fine. TalkTalk, for example, which was fined a record £400,000 in 2015 for a 2014 data breach, was fined a further £100,000 in 2017 after it failed to look after its customers' data and risked it falling into the hands of scammers and fraudsters (https://ico.org.uk/action-weve-taken/enforcement/talktalk-telecom-group-plc-august-2017/). More recently, in October 2018, Facebook was fined £500,000 under section 55A DPA 1998, for the unfair processing of personal information between 2007 and 2014. However, under the new GDPR and DPA 2018, the maximum fine could have been much larger, namely, €20 million or up to 4 per cent of the company's global turnover (https://ico.org.uk/action-weve-taken/enforcement/facebook-ireland-ltd/).

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Article 83 of GDPR, sets out two categories of offence, both with different penalties. The first category carries a maximum penalty of up to 2 per cent of a business' global annual turnover or €10 million, whichever is the greater. Included in this first category is a failure to take adequate security measures to protect personal data. Also included in this category are failure to comply with record-keeping obligations, failure to designate a data protection officer when required to do so and failure to cooperate with the ICO. The second category of offence carries a maximum penalty of up to 4 per cent of a business' global annual turnover or €20 million, whichever is greater. Within this category are individual offences related to the processing principles, the right of data subjects and obstruction of the ICO. The lists of offences in both categories are not exhaustive and may be expanded in the future.

The ICO's Regulatory Action Policy suggests that the heaviest penalties will be imposed on organisations that repeatedly and wilfully transgress their obligations and where formal regulatory action would serve as a deterrent to others. When deciding on the level of the penalty imposed, the ICO will take into account aggravating factors (eg, whether an organisation has made any financial gain as a result of the failure to report – see question 24) and mitigating factors. Deliberate failure, the involvement of vulnerable victims or a poor regulatory history are likely to increase the size of the penalty imposed.

Prior to the implementation of the GDPR, the ICO went to considerable effort to reassure data controllers about the future use of its powers to impose enlarged fines under the Regulation. It remains to be seen whether the increasing media prominence of data issues will be reflected in the level of fines imposed for breaches of the obligations on

Update and trends

Brexit

Cybersecurity, as with other elements of UK law and policy, is dominated by one question: 'what will happen post-Brexit?' The astute questioner asks a more highly developed question: 'what will happen in the period of transitional arrangements and what will happen in the period after Brexit finally takes place (whenever that is)?' As at the date of writing, none of this is completely certain, to say the least, as it depends upon the outcome of Parliament's consideration of the UK–EU agreed Withdrawal Agreement and Political Declaration that accompanies it. Given the parliamentary arithmetic, it is not clear whether and the present 'deal' will survive and whether the UK is entering 'hard Brexit' territory.

If a deal on the present terms is approved by Parliament – and the EU has made it clear that those are the only terms for withdrawal in an agreed manner – the following are clear as far as data protection is concerned, and cybersecurity too given that the law relating to cybersecurity is to a great extent (one could argue nearly exclusively) a function of or sister of EU data protection law:

- EU law will continue to apply generally in the UK during the transition period (although the status of the ICO, and thereby its influence, is not yet settled); and
- post-transition and into full Brexit, there is an assumption that an adequacy decision will have been negotiated to allow data flows as between the UK and the EU unhindered (with negotiation of that decision taking place during the transitional period).

Of course, the adequacy decision, though simple in theory, is threatened by yet further *Schrems* litigation – challenging the contractual bases upon which adequacy decisions concerning data transfers rest – and the need to consider the vexed question of the protection against potential interference by the UK's police, intelligence and security agencies especially in the light of the *Big Brother and others* judgment in the European Court of Human Rights.

Whichever way one looks at it, the cybersecurity requirements set in EU law will have to continue if an adequacy decision is to be obtained, given that data security is a central tenet of the data protection. So, not only is cybersecurity effectively going to be a legal requirement in a post-Brexit world, whatever that looks like, but of equivalent standard to that demanded in EU law, even if solely under UK law, having such standards makes both practical and good business sense.

Guidance and more

The outpouring of guidance has continued and accelerated, much of which is referred to in the answers above. That is a function of having the dedicated NCSC leading on policy and causing everybody in the public sector and across regulators to raise their game. There can really be no excuse for any institution, large or small, not at least to have contemplated its own cybersecurity requirements and vulnerabilities and to have taken action to ensure action and amelioration of risk. The existence and increasing availability of guidance and information underscores that the real trick to having adequate cybersecurity in place is to ensure that both technical and organisational elements of a business are combined. The law provides a helpful reminder of the basic minimum standards and potential cost in terms of administrative or even criminal action should adequate consideration not have been given to the cybersecurity issue.

Yet more guidance is anticipated over the coming year, in particular from regulators but with the NCSC playing a key role in ensuring that the UK's national policy is supported by the actions of individuals and businesses alike.

Enhanced enforcement

Although the enforcement actions of the ICO for those who have failed to provide adequate data security have not yet reflected the increased penalty regime following the implementation of the GDPR in May 2018, there has been considerable activity by the ICO in bringing administrative proceedings in respect of data breaches in the period before the GDPR. This has resulted in large fines by any standards even under that previous Data Protection Act 1998 regime, with an apparently increased emphasis on tech companies as the subject of regulatory action, opposed to the traditional concentration on the missteps of public authorities as far as data loss is concerned. This has seen penalties levied against Facebook and more recently Uber where, in the latter case, combined financial penalties from the ICO and its Dutch equivalent were close to £1 million. That was in respect of a data breach in which the details of 57 million customers and drivers were accessed in 2016. Uber appears to have been blackmailed and paid the hackers US$100,000 to destroy the data before it told the data subjects concerned.

Even the tightest security has potential failure points and the drive to protect data has controversially given rise to 'bug bounties' – organisations inviting hackers to test their defences in return for reward to identify and plug cyber weaknesses. Despite such measures, one can predict a continuing litany of data breaches and ever more substantial fines as post-May 2018 incidents fall under the regulator's gaze. We still await the case in which it is suggested that security requirements were adequate and that it would be wrong to impose penalties, given that no system is invulnerable to attack. As with the *Uber* example, the highest penalties will be reserved for those where it is not simply a question of a flaw in the data security process but where the reaction is not immediate and strictly according to the GDPR requirements and those of the relevant regulator.

All of this does, however, illustrate the ongoing tension between reporting and then being punished for doing so. This is thrown into even sharper relief when considering what happens to those who have exploited security weaknesses. In the case of the 2015 TalkTalk data breach – which was another case of attempted blackmail – the overall cost to the corporate was assessed to have been £77 million (including a £400,000 penalty from the ICO). Those responsible, at least in part, for the data breach, were sentenced in November 2018. Two individuals each received a sentence of 12 months or less. Although these authors would not generally encourage 'tougher sentences', which seems to be the response to any social wrong, the disproportionality between the punishments visited on the attacker and the attacked (even where the attacked might be said to be at fault) is striking.

AI

This is one dog that has yet to bark in terms of its effect on cybersecurity policy and law. And there is simply not much law in the artificial intelligence space. As far as the UK government is concerned, plainly the starting point is (https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf) the House of Lords Report from the Select Committee on AI of April 2018 and in particular the government's response to the House of Lords Report of June 2018 (https://www.parliament.uk/documents/lords-committees/Artificial-Intelligence/AI-Government-Response2.pdf. There is clearly a crossover here and we expect the cybersecurity debate to move into the AI space. At present, the concept that AI is bound to have vulnerabilities is clear. What is not clear is whether the present perception that data protection law is a reasonable point of departure for consideration of a legal regime applicable to AI is the correct one.

data controllers. Nevertheless, the huge increase in potential penalties provides strong impetus for businesses both to comply with the GDPR and be generally more proactive against cybersecurity threats.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Under the GDPR, failure to notify the ICO of reportable personal data breaches risks the imposition of an administrative fine of up to €10 million or 2 per cent of group annual turnover (whichever is the higher).

Under NISR, failure by an OES or RDSP to notify its competent authority of a NIS incident may lead to the imposition of severe financial penalties (up to £17 million) in the worst-case scenarios where the material contravention risked causing or has caused an immediate threat to life or significant impact on the UK economy.

Under PECR, personal data breaches must be notified to the ICO without undue delay and within 24 hours. Failure to do so may result in a fixed penalty of £1,000, though more serious breaches can lead to the imposition of heavier monetary penalties.

Despite the ICO's long-standing powers to impose financial penalties, a request under the Freedom of Information Act in mid-2018 revealed that, although the regulator had levied fines totalling £17.8 million since 2010, only £9.7 million of that had been collected, calling into question the deterrent effect of the ICO's powers.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Data subjects may lodge complaints to the ICO where breaches of the GDPR or DPA occurred in respect of their personal data (section 165 DPA). Although the ICO cannot award compensation, a finding by the regulator that a breach has occurred could then be used in any subsequent civil proceedings brought by the aggrieved data subject. That said, a finding by the ICO that there has been a breach is not a prerequisite of a civil claim and a data subject may bring proceedings against a data controller or processor where damage (including distress) can be proved.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

While the NCSC and ICO offer advice on cybersecurity, there are no prescribed policies or procedures in law or regulation that organisations must implement to protect data or IT systems. Instead, organisations must achieve the technical and organisational security standards expected of them under the applicable legislation using the plethora of cybersecurity advice available from governmental and industry bodies. The ability to demonstrate the steps taken to achieve such standards is a key element of the GDPR and NISR and failure to provide them may lead to regulatory action or exacerbate any penalties imposed as a result of a cyber incident.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Apart from the practical utility for organisations of maintaining records to identify systemic issues and improve standards, as part of the overarching GDPR accountability obligation (see question 1), data controllers must maintain records of personal data breaches even where no reporting obligation arises under articles 33 and 34. No particular format is prescribed for such records, though they must contain the facts relating to each data breach, its effect and remedial action taken. The ICO requires that similar information is recorded by network and service providers regulated by PECR in the event of a personal data breach. In the event that a reportable data breach takes place, the ICO may demand to see a data controller's records.

Under NISR, OES and RDSPs must maintain records evidencing the appropriate and proportionate technical and organisational measures taken to manage risks to their systems. In the event of a security incident involving a personal data breach, as well as notifying their respective competent authorities, OES and RDSPs must also notify the ICO and be able to provide documentation demonstrating compliance with their security obligations as well as prescribed details about the incident itself.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

There are currently no rules in England, except for public electronic communications service providers. Under Regulation 5A PECR, these communication service providers must notify the ICO of any personal data breaches. In 2015 (up to 19 November), 143 breaches were reported under this Regulation (see questions 3 and 24). Although there is no legal obligation on data controllers to report breaches of security that result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to her attention. Further, the UK government has taken action to make the reporting procedure simple and straightforward by establishing integrated reporting tools.

There are numerous ways to report cybersecurity breaches, fine-tuned to meet the needs of specific organisations. For government agencies and other public bodies, the two organisations are CESG (originally Communications-Electronics Security Group) the information security arm of Government Communications Headquarters and GOVCERT, the CERT for government and public sector bodies. For private companies and organisations, the two main reporting agencies are the National Cyber Crime Unit (a part of the NCA), and 'Action Fraud', an online national fraud reporting centre. The Cyber Incident Response scheme also exists, which provides access to industry expertise.

Since the GDPR came into effect in May 2018, all cybersecurity breaches must be notified to the national supervisory authority and that notifiable breach reporting to the national supervisory body will be mandatory within 72 hours of an organisation becoming aware of it and, in serious cases, public notification will be required.

29 What is the timeline for reporting to the authorities?

See question 28.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

See question 28.

BCL Solicitors LLP

Michael Drury **mdrury@bcl.com**
Julian Hayes **jhayes@bcl.com**

51 Lincoln's Inn Fields
London
WC2A 3LZ
United Kingdom

Tel: +44 207 430 2277
Fax: +44 207 430 1101
www.bcl.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-912228-87-4