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 cybersecurity law as such in England and Wales. Rather, there are numerous statute-based laws, underpinned by the common law. These:

- criminalise interference with computers without authority, including where the 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 significant risk thereof (the Computer Misuse Act 1990 (CMA) as amended by the Serious Crime Act 2015 (SCA));
- criminalise the interception of communications, which includes communications sent or received by computers (the Regulation of Investigatory Powers Act 2000 Part 1 (RIPA)), noting that the RIPA scheme will be replaced by and large by the Investigatory Powers Act 2016 (IPA), which received Royal Assent in November 2016 and is gradually being brought into force from 30 December 2016 onwards;
- impose obligations to protect personal data (rather than data more generally) by the application of security measures (by the Data Protection Act 1998 (DPA), especially within Schedule 1). The Seven Data Protection Principles are that the data is (i) used fairly and lawfully; (ii) used for limited, specifically stated purposes; (iii) used in a way that is adequate, relevant and not excessive; (iv) accurate; (v) kept for no longer than is absolutely necessary; (vi) handled according to people's data protection rights; and (vii) kept safe and secure. A breach of the obligation to keep data secure gives rise to potential criminal sanction, and civil financial penalties can be imposed on the data controller by the Information Commissioner, the UK public official responsible for policing the protection of personal data. Civil remedies are also available to data subjects where there has been a breach of the requirements of the DPA, including where processing by the person controlling the personal data is done in a manner causing, or likely to cause, substantial damage to the data subject;
- criminalise actions amounting to fraud (Fraud Act 2006 (FA)) and infringing intellectual property rights (Copyright, Designs and Patents Act 1988); and
- give rise to actions under the common law, in particular, the tort of negligence, where, if insufficient steps are taken to protect data or information held electronically, the person responsible for loss of the data could be held liable in civil law.

It is important to note that significant changes will be brought about by the implementation of the General Data Protection Regulation (GDPR) and the Network and Information Security Directive agreed by the EU institutions in December 2015 (see question 3 and Update and trends). The Secretary of State for Culture, Media and Sport, Karen Bradley MP, confirmed to the Culture, Media and Sport Select Committee on 24 October 2016 that the GDPR will apply in the UK, notwithstanding 'Brexit'. She stated that 'We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public.'

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

What would otherwise be 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, and in accordance with the authorisation regimes established under RIPA, the Police Act 1997 and the Intelligence Services Act 1994. Again, that scheme will be replaced by the IPA scheme, which provides for more transparent state powers in the electronic surveillance field.

Parliament has not legislated to promote cybersecurity as such, and the offences described have been created in a rather piecemeal approach. The UK government has instead approached the cybersecurity issue by seeking to develop awareness, both in the business sector and among the public more generally, to enhance cybersecurity safeguards against, and mitigate the risks of, cyberattacks. In a speech made on 1 November 2016, Philip Hammond (the new Chancellor of the Exchequer) spoke of the renewal of the five-year National Cyber Security Strategy through which three core pillars are built: to defend, deter and develop. The strategy is underpinned by £1.9 billion of transformational investment and is supported by the new National Cyber Security Centre, based in central London (www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy). The Centre subsumes CERT UK and will provide the next generation of cybersecurity-incident management. This means that when businesses or government bodies, or academic organisations report a significant incident, the Centre will be in a position to bring together and rapidly deploy the full range of technical skills from across government and beyond. The Centre will also link up with law enforcement, help mitigate the impact of incidents, seek to repair the damage and assist in the identification and prosecution of those responsible.

The CMA, which stands as the principal statute implementing the Budapest Convention on Cybercrime, provides for criminal offences based on the notion that if a person (i) 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, then 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 not done by a person 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. What constitutes consent in the cyberworld may be open to argument, but the courts are anxious to limit what might be so regarded. For example, the English Court of Appeal has determined that a distributed denial of service (DDoS)

attack constitutes an action done without consent, despite the suggestion that a computer is designed to receive communications.

The CMA creates further offences where the unauthorised access is sought with a view to committing other offences, for example, 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, penalties are higher, in the latter case 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 of unauthorised access, etc.

The DPA, which implements the EU Data Protection Directive (95/46/EC), requires data controllers to meet the following standard as far as data security is concerned: '[a]ppropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data' (Seventh Data Protection Principle, Schedule 1 DPA). In essence, an organisation must take steps to prevent unauthorised access, as well as accidental loss or damage. Failure to meet these standards can lead to a civil penalty or a criminal sanction (sections 55A and 55 DPA respectively).

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 that process and control data. The DPA applies specifically to personal data, namely, 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 will have to meet the DPA requirements to the extent that they process personal data (and virtually all will do so). Government guidance and publicity was traditionally directed towards the defence sector but is now addressed to all businesses and sectors because of the pervasive nature of the threats and breaches. Guidance, which is extensive and frequently published, and compliance standards tend to be structured around the types of attacks, rather than the industries attacked. There are some examples of sectoral guidance, for example, the Payment Card Industry Data Security Standard (PCI DSS) must be complied with by all organisations that accept, store, transmit or process cardholder data, to decrease payment card fraud. There is no data to suggest that any sector is doing much better than any other. The finance sector, where there is an obvious risk of fraud, may be thought to have considered these matters for longer, and in greater depth, than others. The 2016 PwC Global Economic Crime Survey cites cybercrime as the second most reported economic crime, affecting 32 per cent of organisations. The same survey notes that most organisations are inadequately prepared for cyberattack, with only 37 per cent having a basic cyber-incident response plan in place.

Professional regulators are increasingly engaged in the participation of cybersecurity initiatives, at times embedding national strategies and guidance into their own regulatory guidance. The Solicitors Regulation Authority, for example, has encouraged the use of the government's '10 Steps to Cyber Security'.

Failure to protect data adequately may give rise to breaches of regulatory requirements more generally. For example, the Financial Conduct Authority (FCA) has levied penalties for data breaches where they have been found to constitute breaches of FCA Principle 3 to 'take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems' by failing to take reasonable care to establish and maintain systems and controls appropriate to the business, or to counter the risk that a business might be used to further financial crime. Examples of such fines include Think W3 Limited, an online travel services company, being fined £150,000 in 2014 after using insecure coding, which resulted in 1.1 million credit and debit card details being stolen by cybercriminals. A year earlier, the ICO fined Sony £250,000 when the PlayStation Network Platform, containing private information belonging to millions of customers, was breached in a cyberattack. See also question 21.

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

The European Union has and continues to have a key role in setting standards for the United Kingdom.

First, Directive 95/46/EC was designed to protect the privacy of all personal data collected for or about citizens of the EU. This has been given effect in England and Wales by the DPA and affects any organisation that collects or processes personal data (see question 1).

Second, Directive 2013/40/EU on attacks against information systems 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.

Most recently, the EU has been promoting the European Commission's Cyber Security Strategy of 2013. Of the greatest significance, on 15 December 2015, the EU Parliament, Council and Commission agreed the text of the long-anticipated GDPR. This regulation was adopted on 27 April 2016, and will be implemented on 25 May 2018 at the latest, after a two-year transition period. Despite Brexit, the government has confirmed that the GDPR will enter into application in the UK, as the UK will most likely still be a part of the EU on that date. On 7 December 2015, the same three EU institutions had agreed the Network and Information Security Directive, the first EU-wide legislation on cybersecurity in a directive with measures to ensure a high common level of network and information security. In addition, a third measure, a directive concerning data protection in the field of law enforcement, which seeks to maintain the protection of individuals where their data is processed for prevention, detection, investigation and prosecution of crime or to safeguard against and prevent threats to public security has also been agreed by the institutions.

This legislation is the most prescriptive of its kind, and will generally apply to all data controllers and processors established in the EU and processing personal data of subjects who are in the EU. Several key provisions of the GDPR should be noted in the cybersecurity context. The first is a uniform requirement for notification of security breaches. The effects of the requirement for telecommunications providers to notify the supervisory authority of any actual breaches without undue delay under EU Regulation 2013/611/EU will apply under the new Regulation, albeit to a much wider range of organisations. In addition, there is also a requirement to notify the 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 high risk effectively. Second, the Regulation affects both data controllers and data processors. In relation to the latter, it now sets out clear obligations which include the responsibility to implement technical and organisational security measures, appropriate to the specific risks that are present. It also includes the requirement to assist data controllers in any data subject access requests, thus facilitating individuals' access to their personal data. The Regulation further sets out clear provisions for the transfer of data, which is possible with adequate consent, when based on model clauses, or pursuant to an approved code of conduct or an approved certification. The Regulation specifies how consent can be properly obtained and, for the first time, identifies the age of consent in relation to the processing of personal data, which by default is 16 years, unless a member state legislates to allow consent from people as young as 13.

The Regulation sets out detailed rights of individuals in relation to data processing, which includes the right to access your personal data, the right to rectification and the right to erasure of information where, for instance, the information is no longer necessary or consent has been withdrawn and there is no other legal ground. Other rights include the right to data portability, that is, to receive your personal data in a structured and commonly used format and the right to transmit this data to another controller, and the right to object to the processing of information. The scope of these rights can still be restricted on a wide range of grounds, including where there is a need to safeguard national security, defence and public security, for the purpose of preventing, investigating, detecting or prosecuting crime or breach of ethics for regulated professions and for the enforcement of civil claims. Violations of the core principle of the Regulation can result in fines of

up to 4 per cent of the organisation's annual worldwide turnover, or a maximum of €20 million (whichever is highest).

The Network and Information Security Directive, already being described colloquially as the 'Cybersecurity Directive', is primarily concerned with enhancing national cybersecurity capabilities, improving cooperation and applying security and notification requirements both for operators of essential services and for digital service providers. Under the Directive, 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. In terms of cooperation, an EU-wide 'Cooperation Group' will be established in order to facilitate cooperation and information sharing between member states. Both operators of essential services and digital service providers will be under an obligation to notify security incidents to the relevant national supervisory authority; the inevitable national differences in notification obligation remain to be identified. To a certain extent, the Directive leaves the precise definition of 'operators of essential services' and 'digital service platforms', such as e-commerce platforms, search engines and cloud services, to the discretion of member states.

The International Organization for Standardization's ISO 27001:2013 sets out 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.

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 (for more detail, 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.

At present, aside from the general standards, in the Information Communication Technology (ICT) context, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), implementing Directive 2002/58/EC, imposes obligations on a provider of public electronic communications services to take appropriate technical and organisational measures to safeguard the security of that service. The law does not seek to impose a standard as such: a measure shall only be taken to be appropriate if, having regard to the state of technological developments and the cost of implementation, it is proportionate to the risks against which it would safeguard. Administrative financial penalties can be imposed for breaches of the regulation (but they have so far been confined to marketing breaches with which the Regulations are also concerned). Directive 2002/58/EC and, thus, the PECR will be reviewed once the new GDPR has been implemented.

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 whom they represent in accordance with the law (as embodied in the DPA, as well as the Companies Act 2006 and elsewhere). For instance, pursuant to section 174 of the Companies Act 2006, a company director is held to the standard 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 . . .'. This is an objective test, which sits alongside a subjective test of knowledge, skill and experience. Personal liability could, therefore, follow in certain circumstances for breaches where it is found that directors failed to fulfil those standards. The 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, unless all due diligence has been exercised. However, there is no specific law with regard to cybersecurity. Ultimately, data protection liability rests with the organisation in question. The new EU Data Protection requirements will add further layers of corporate responsibility.

5 How does your jurisdiction define cybersecurity and cybercrime?

There are no specific legal definitions of 'cybersecurity' and 'cybercrime' as such: the thinking is certainly dominated by data protection concepts, but has now spread beyond that. The police define cybercrime as the use of any computer network for crime, and the National Crime Agency (NCA) define it as any crime committed through the use of ICT. The work of the National Cyber Security Centre should add further clarity here.

According to the NCA, the most common cyberthreats for businesses are hacking and DDoS. For consumers, they are larger in number: phishing (eg, bogus emails asking for personal details or delivering harmful viruses), webcam manager (taking over your webcam), file hijacking (hijacking files and holding them in ransom), keylogging (recording what you type on your keyboard), screenshot manager (taking screenshots of your computer screen) and ad clicker (directing a computer to click a specific link).

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

There are no minimum protective measures as such, except for compliance with the Seventh Data Protection principle or its equivalents. The standards at the level of law tend to be expressed by what is appropriate, measured against risks. More specific standards may be applied, in particular, implementations of the general standard (see ISO 27001).

See question 3 for the minimum measures likely to be required as a consequence of the GDPR.

See question 2 for reference to PCI DSS applied to cardholder data security.

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

While there are no specific laws or regulations addressing cyberthreats to intellectual property, these are addressed both by criminalising the way in which it would be unlawfully obtained and by criminalising the improper use of intellectual property. One would also have to consider civil liability.

The main purpose behind offences listed in question 1 may perhaps not have been to protect intellectual property, per se, however, in reality, the obtaining of 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 in order 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 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. The section is broad and encompasses a range of activity, including copying, distributing and, simply, communicating work to the public. 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?

Cyberattacks that are directed against the critical national infrastructure will be criminal if they meet the tests set out in the CMA (see question 1). Threats of this nature are also likely to represent threats to the UK's national security and, as such, those making them are liable to come to the attention of the UK's security and intelligence agencies and law enforcement authorities.

The SCA amended the CMA by creating an offence for persons to knowingly use a computer for an unauthorised purpose that causes or creates a significant risk of damage to human welfare, the environment, the economy and the national security of any country (section 3ZA CMA). The infrastructure and sectors this law seeks to protect from 'disruption' include energy, fuel and water, in addition to communication and transport networks and health services (section 3ZA(3)). Offences under this section where there is a significant risk of serious damage to human welfare or national security carry life-term prison sentences (section 3ZA(7)), and 14 years' imprisonment for any other offence under this section.

The CMA provisions for extraterritorial jurisdiction have been extended by the SCA to provide a legal basis to prosecute if there is a 'significant link' to the UK, for example, if the accused is in the UK at the time of the offence or if the affected computer is in the UK. Additionally, a UK national may also be prosecuted where there is no significant link to the UK, provided that the offence is an offence in the country where it took place (section 5 CMA, pursuant to article 12 of the EU Directive 2013/40/EU on attacks against information systems).

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 standard questions of confidentiality. In fact, the government has been actively encouraging effective sharing in order to tackle cyberthreats and improve cybersecurity. The Cybersecurity Information Sharing Partnership (CiSP), a part of CERT-UK (which has since been subsumed by the National Cyber Security Centre; see question 1), was established as a joint industry–government initiative to share information about cyberthreats and vulnerabilities. It includes members across all sectors and organisations, in order to exchange cyberthreat information in real time within a framework that protects confidentiality of shared information. The government has also set up industry-specific spaces, for example, the Retail Cyber Security Forum, to help address effective reporting and information sharing within the industry. It should also be noted that effective sharing of information is one of the aims of the EU Network and Information Security Directive.

To the extent that, in the context of sharing cyberthreat information, personal data forms part of that information, then obviously the requirements of the DPA must be met (see below).

Sections 19-21 of the Counter-Terrorism Act 2008 allow state authorities to share material intercepted under RIPA or other national security sensitive information with other intelligence services and also private entities if in pursuance of national security or the prevention of serious crime. Section 19 absolves any individual or entity for breach of confidentiality provided the threshold has been met where it is sharing information for national security purposes or for the prevention of serious crime.

There are limitations on the capacity to share 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, notably from a telecommunications service provider, it is a criminal offence for a person in that service provider or for a public official to fail to keep secret the existence and content of the warrant or authorisation. Any information from that source therefore needs to be desourced. Other information from government bodies can be shared as long as it is compatible with their own statutory foundations (if any) and the requirements of the Human Rights Act 1998. That position will be maintained under the IPA 2016.

Article 8 of the ECHR (the right to privacy and freedom of correspondence) given effect in England through the Human Rights Act 1998, 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, and 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 (and others).

The DPA (see also question 1) regulates the use of 'personal data', that is, data from which a living individual can be identified that is retained on a computer (section 1(1)) and places duties on those persons responsible, known as 'data controllers', for processing that data (section 4(4)). Every data controller must comply with the data protection principles (set out in Part 1, Schedule 1), which ensure that personal data is obtained for a specific purpose and shall not be processed in any manner incompatible with that purpose (Part 1(2)), including by keeping the data secure.

It is an offence for any person knowingly or recklessly to obtain, disclose or procure the disclosure of personal data, in addition to selling or offering to sell data that has been unlawfully obtained pursuant to section 55. Offences of this nature currently carry punishments by way of fines only. A civil penalty regime enforced by the Information Commission under section 55A DPA allows a civil monetary penalty of up to £500,000 (at the time of writing) to be imposed on a data controller guilty of serious breaches, as a means of encouraging good practice in the handling of personal data. The Parliamentary Justice Committee has considered proposals to amend the DPA further to include custodial sentences for the section 55 criminal offence, but none are presently available. Power to amend section 55 DPA was introduced in the Criminal Justice and Immigration Act 2008, but (at the time of writing) has not yet been implemented.

Further protection as to privacy is provided by RIPA, which makes it an offence for persons intentionally and without lawful authority to intercept any communication in the course of its transmission (section 1(1) and (2)) unless such conduct is permissible by way of a warrant issued by the Secretary of State in matters of national security, serious crime prevention, or in the safeguarding of the UK economy (section 5). Monitoring such communications is lawful if done by the provider of a telecommunications service, and it takes place for purposes connected with the provision or operation of that service, or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services (section 3).

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 set out exceptions where, in connection with the carrying on of a private or public sector business, the monitoring of communications will be authorised, for example, to establish the existence of facts or ascertain compliance with regulatory practices, and where such conduct is in the interests of national security or crime prevention. Interception upon these bases will not, therefore, contravene RIPA, even though they do not amount to exemptions from the DPA. Again, monitoring communications for the purposes of lawful business will be permitted under the IPA regime (when it is implemented).

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 in England and Wales. It is also an offence to use or obtain for use articles in order to commit either of the first two offences mentioned. See also questions 1 and 8.

The unauthorised interception of information (eg, through 'phone hacking') is covered by RIPA. A prison term of up to two years is provided for offenders under section 1(7)(a). The offence and the punishment to be applied will remain under the IPA 2016.

As above, section 55 DPA creates an offence of unlawfully obtaining and processing personal data. As an illustration of the sentences previously imposed, in February 2015, an online holiday insurance company was fined £175,000 by the ICO because of the IT security failings that resulted in the use of credit cards of 5,000 customers.

All 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.

References to criminal offences are to be found in questions 1, 8 and 9.

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

The DPA principles also apply to cloud computing services, most notably the Seventh, which specifies that an organisation must take steps to prevent unauthorised access as well as accidental loss of, or damage to, personal data (see question 1). The responsibility of 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 and is essentially treated as a data controller. The responsibility exists whether the data is being held or is in transit, and lies in mitigating security risks to ensure end-to-end security. This involves undertaking the necessary checks on the cloud service provider (by someone with appropriate technical expertise) to ensure it provides sufficient guarantees and takes reasonable steps to ensure compliance with the DPA. It should be noted that although responsibility in mitigating risks lies both in the holding and the transfer of data, most issues and penalties have, so far, been with regard to data in transit. It should also be noted that the new Cybersecurity Directive will also apply to cloud-computing services, and will, thus, impose further obligations; for instance, the requirement to notify the national supervisory authority of any cybersecurity incidents.

The EU Regulation (see question 3) places responsibility not only on the data controller but also on the data processor for a range of obligations and liabilities. It imposes certain additional rules on data processors, such as restrictions on international data transfers and further duties. These proposals are treated with caution and apprehension by commentators, who are concerned this will force cloud computing and other service providers out of the EU.

Further guidance has been published by the UK's Information Commissioner's Office 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' through the European Cloud Computing Strategy and, in due course, cloud providers may well shoulder their own protection obligations, rather than solely the data controllers (see http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy).

One of the difficulties is that the location of cloud computing service users is generally less well controlled and controllable. In a survey in June 2014, 75 per cent of consumers using social media on mobile devices stated they were automatically logged in from their personal devices, as were 23 per cent of mobile banking users. As a result, in addition to the application of the Cyber Essentials scheme (see question 13), additional precautions, such as a two-factor authentication, are greatly encouraged. There is a plethora of guidance, including the report from the ICO mentioned above, as well as the ISO27001:2013 Information Security Management (see question 3).

As cloud computing often involves the movement of data to a 'cheaper jurisdiction' the user may not be aware of the physical location where it is stored. Personal data can only be transferred to a country outside the EEA if that country is on the Commission's authorised list of countries that provide adequate protection for personal data. The DPA permits organisations to transfer data to a non-EEA location where the organisation demonstrates that they meet the Binding Corporate Rules and satisfies the requirements of the 'Article 29 Working Party' (see https://ico.org.uk/for_organisations/data_protection/overseas/binding_corporate_rules). It is important to note that the GDPR will replace the Article 29 Working Party with the 'European Data Protection Board' (EDPB), which is set to play a very significant role in data protection compliance as a body central to the formation of guidance, approval of codes of practice and certification schemes and, crucially, as the appellate body for GDPR disputes. Like the Article 29 Working Party, the EDPB will be comprised of regulators from each EU member state (among others). The Safe Harbour Agreement between EU states and the United States, stating that the US did fulfil the necessary requirements for organisations to be permitted to transfer data, was held to be invalid by the European Court of Justice in October 2015 (*Max Schrems* case). The Safe Harbour agreement has since been replaced by the EU–US Privacy Shield transatlantic data transfer framework. However, there are current proceedings issued by Digital Rights Ireland and La Quadrature du Net challenging the European Commission's approval of the adequacy decision of the Privacy Shield framework. In proceedings that formally began on 16 September 2016, Digital Rights Ireland sought, among other things, a declaration from the CJEU that the relevant implementing decision be declared null and void on the grounds that the Commission made a 'manifest error of assessment' in determining that the Privacy Shield framework provided an adequate level of protection for personal data transferred between the EU and US. Digital Rights Ireland argues that the privacy principles included in the Framework are 'international commitments' that are not binding on the United States. It raised concern that, by virtue of the Foreign Services Intelligence Act, US public authorities will still have 'secret access' to the content of electronic communications. It is unclear how long it will take the CJEU to determine these cases, and so in the interim period Privacy Shield will remain in force, although the Privacy Shield agreement specifically included a joint EU–US review of the Framework after its first 12 months in operation. It can be anticipated that this review may provide a further forum for the raising of objections to the Framework.

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 is attempting to harmonise cybersecurity laws and regulations across member states, organisations in other EU states are likely to have very similar standards and obligations. However foreign 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 security requirements and regulations are not "adequate", that is, they must offer protection 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?

Yes. Much guidance has been issued by the UK government but ultimately the decision as to the level of security to be put in place remains an issue for organisations based on their assessment of risk to themselves and their customers underpinned by the legal requirements.

In implementing the UK government's Cyber Security Strategy (see question 18) the government has worked with industry to develop the Cyber Essentials scheme (www.gov.uk/government/publications/cyber-essentials-scheme-overview), which aims to give organisations a clear baseline to aim to protect themselves against the most common cyberthreats. Independent assurance schemes are available to demonstrate that the organisation in question has taken a considered approach and has met a government-approved standard, with a view to this giving a competitive edge over others who have not.

Other schemes include Cyber Streetwise (www.cyberstreetwise.com) and Get Safe Online (www.getsafeonline.org), which provide basic advice for individuals and businesses.

The government has tried to make it easier for organisations to improve cybersecurity. An example is to be seen in the launch of the Cyber Governance Health Check, which is a free service providing a confidential, tailored report for large organisations, enabling them to see what changes should be made. This has also enabled the government to aggregate data on how companies are performing.

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

The government recently released a new scheme, Innovate UK, to encourage small businesses to improve their cybersecurity. Through this scheme it offers micro, small and medium-sized businesses up to £5,000 for specialist advice on how to boost their cybersecurity.

Organisations bidding for central government contracts will need to be 'Cyber Essentials' certified.

In 2012, the UK government launched 'G-Cloud' so that public sector authorities could invite private sector organisations to carry out work without the need to resort to a formal tender process. Its success has resulted in the rebranding of this cloud service to the 'Digital Marketplace' (www.digitalmarketplace.service.gov.uk) together with the establishment of the Government Digital Services division of

the Cabinet Office to assist the public sector in easily, securely and cost-effectively engaging the private sector, which must explain how their services meet the Cloud Security Principles in the procurement framework.

In November 2015, the government, through the policing organisation Ipsos MORI, launched a telephone survey seeking businesses' views on cybersecurity to provide up-to-date findings on their approaches, help organisations learn more about issues that businesses like theirs are likely to face, and inform government policy on cybersecurity and how they need to work with businesses to improve this area.

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' as has appeared in the US. In the UK, guidance appears piecemeal and is issued by individual companies. In addition, industry regulators will often point to and suggest use of government report and advice, such as the 'Ten Steps to Cyber Security'.

See further, questions 13, 14 and 27.

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

Best practice in this area is still under development and will be fact-specific. In the event of the loss of personal data obvious steps need to be taken to rectify the situation so as to seek to recover the 'lost' data and put in place measures to ensure there is no recurrence.

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

There are no government requirements and no incentives as such, however, the government has tried to encourage the sharing of information about cyberthreats (see question 9). The government's encouragement towards 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 2011, the UK government issued an overarching UK Cyber Security Strategy (www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf), which seeks to put the UK in a position where:

> *law enforcement is tackling cyber criminals; citizens [including businesses] know what to do to protect themselves; effective cyber security is seen as a positive for UK businesses; a thriving cyber security sector has been established; public services online are secure and resilient; and the threats to [the UK] national infrastructure and national security have been confronted.*

More recently, the UK government acknowledged that, although its 2011 Cyber Security Strategy had delivered substantial improvements to UK cybersecurity, its approach had not achieved the scale and pace of change required to stay ahead of the fast-moving threat. As a result, in November 2016, a new National Cyber Security Strategy was published for 2016 to 2021 (www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021). Like its predecessor, the new strategy recognises that the significant role played by businesses and organisations in the UK's national response to cyberthreats will be effective.

A Cyber Growth Partnership (CGP), which is a joint initiative between industry, academia and government, aims to boost the UK's global market position in cybersecurity products and services. Under that, a new Cyber Security Suppliers scheme has been developed, whereby businesses can show that they supply cybersecurity products and services to the UK government and use the government logo in their marketing material. The intention is to provide assurance to the private sector of the efficacy and operability of cyberdefence products. For instance, in 2015 as part of the CGP, the UK Trade and Investment and the Department for Culture, Media and Sport set up a Cyber Demonstration Centre to support growth of this sector and be used to showcase services or products offered to various industries. Also, in 2016, the Department for Culture, Media and Sport funded a competition to find the UK's most innovative small cybersecurity company, with the shortlisted companies going through to compete at the Infosecurity Europe Conference.

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

Yes, in principle, insurance cover is available to mitigate cybersecurity risks as with any other risks. Unsurprisingly, the market is often considered generally underdeveloped given that the scale of risk to be insured against is uncertain on the basis that the risk of a cybersecurity breach and its detection (if it has occurred) and the assessment of the loss arising from a breach are difficult for brokers and underwriters to assess. Nevertheless, as the incidences of cybersecurity breaches increase and the potential liabilities on business increase, demand for such insurance is likely to increase.

The UK government has recently been working with the insurance sector in order to highlight the important role of cybersecurity insurance and in an attempt to make the UK 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 working group focusing on how cyber insurance can both mitigate damage caused by cyberattacks and encourage better cybersecurity by offering premiums for cyber-secure organisations released a report in March 2015 (www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf). This report 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, but only 10 per cent of UK companies actually had cyber insurance protection (as at March 2015). The report further provides a thorough assessment of the risks of and potential losses deriving from cyberattacks, as well as serious encouragement of the Cyber Essential scheme.

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 National Crime Agency, which has a dedicated cybercrime unit (www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit). As with other crimes, criminal cases would have to satisfy the criteria that would allow prosecution by the Crown Prosecution Service: a reasonable prospect of success and being in the public interest. In November 2015, the government announced a comprehensive programme including a National Cyber Centre, the country's first 'cyberforce'. The National Cyber Security Centre became operational in October 2016 and acts as a coordinating organisation.

The Information Commissioner enforces the DPA in both criminal and civil jurisdictions (https://ico.org.uk/what_we_cover/taking_action/dp_pecr).

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

In addition to enforcement by regulatory authorities, the DPA also makes provision for individuals to claim compensation in civil courts for damage and distress suffered as a result of data protection breaches.

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

Update and trends

Five events from 2016 carrying through to 2017 will dominate the UK cybersecurity field in the coming year: (i) Brexit and the effect it will have on EU law; (ii) the clear timetable for the implementation of the GDPR in May 2018; (iii) the replacement of the present RIPA and DRIPA regime with a new one under the Investigatory Powers Act 2016 governing electronic surveillance in the UK; (iv) steps towards implementing the Network and Information Security Directive (the Cybersecurity Directive), which must come into force throughout Europe by May 2018; and (v) as an adjunct to the Cybersecurity Directive, the establishment of the National Cyber Security Centre with a view to providing greater clarity in the renewed UK national cybersecurity policy and coordinating cybersecurity action.

A few things are certain when one considers cybersecurity in the Brexit context. Brexit will not take effect before the implementation of the GDPR in May 2018. As above, the UK government is committed to implementing the GDPR by the required date. This would be done either by way of Regulations made under the European Communities Act 1972 or through new primary legislation. Either way, amendment to the Data Protection Act 1998 seems inevitable. Whether this will take place in 2017 or in the first half of 2018 remains uncertain.

In practice, Brexit will not permit the UK to abandon the EU data protection regime entirely or, in reality, at all. A very similar, if not identical, regime to that under the GDPR and associated 'cyber' EU directives will have to continue to exist within the UK. The nature of the UK's future relationship with the EU will necessitate transfers of personal data from the EU to the UK. Given that any non-EU country to which EU personal data is transferred must provide personal data protection essentially equivalent to that of the EU for such a transfer to be compatible with EU law, UK law will have to provide such equivalence. On the basis of the legal requirement for implementation of the GDPR and other Directives, UK law will reflect those requirements by the date of Brexit.

There would seem to be little point, post-Brexit, in seeking to amend the law recently put in place to remove protections to data or data subject rights where the maintenance of those is a necessary requirement to permit EU member states and institutions to continue to transfer data as a function of their relationship with the UK. What is likely to be necessary is an equivalent – perhaps in lesser form – of the US–EU Privacy Shield arrangements agreed earlier in 2016 as a replacement for the preceding Safe Harbour arrangements that were struck down in the *Max Schrems* case in October 2015. Whether Privacy Shield will provide a suitable template for future EU–UK data transfers remains unclear, given that privacy campaigners are already challenging it in the courts and in the light of a potentially testing joint US–European review later in 2017. It should be remembered that cybersecurity has its roots in the need to protect personal data, exemplified in the Seventh Data Protection Principle.

Fundamentally, what is apparent is that the principles set out in EU law, whether in the form of the GDPR or the Cybersecurity Directive are sensible, agreed by the UK, consistent with the UK's own national cybersecurity policy and represent the protections and necessary legal drivers to achieve good cybersecurity outcomes, whether for government, institutions or individuals. Put another way, the cybersecurity requirement survives Brexit, whether or not the requirement is met in legal terms through EU legislation or domestic legislation having essentially the same effect; the EU Regulation and Directives provide a ready-made legal version of a 'commercial off-the-shelf solution'.

Moreover, if it really is the case that 'Britain is open for business' and is to champion free trade outside the EU, the cybersecurity requirement, and a suite of laws to encourage that by means of control and regulation of data, remains an immutable requirement.

After almost a year of debate, the Investigatory Powers Act 2016 (IPA) received Royal Assent on 29 November 2016. Although dates for its full commencement are not known at the time of writing, its data retention provisions (Part 4 of the IPA) were brought into force on 30 December 2016 to ensure continued data retention post the demise of DRIPA the following day. How the government will respond to the challenges to generalised data retention as a result of the CJEU judgment in *Watson & Ors* remains, at the time of writing, unclear. It is noteworthy that the vulnerability of communications data retained under the IPA has been identified by some commentators as being of some concern, notwithstanding the previous legislation contained very similar data retention provisions.

Significantly, and highly exceptionally, given the national security and law enforcement context in which communications data retention operates, the UK's Information Commissioner will be given responsibility for auditing compliance in relation to integrity, security and destruction of data retained under the data retention regime.

The best estimate is that, retention of communications data aside, the IPA will be implemented in Q2 2017, but this timetable is not certain.

In essence, the IPA seeks to provide a comprehensive scheme for the use of investigatory powers by public authorities to obtain communications and communications data, undertake electronic surveillance more generally (including hacking) and access personal data held in large datasets. The scheme is intended to ensure that the requirements of the Human Rights Act 1998 (and through that the European Convention on Human Rights) and EU law, where applicable, are met. These powers essentially cover five areas of activity: (i) interception warrants (specific and bulk); (ii) obtaining communications data (including bulk acquisition warrants); (iii) retention of communications data; (iv) equipment interference including bulk equipment interference; and (v) using bulk personal datasets (eg, the electoral roll and lists of all UK passport holders).

Like the GDPR, the Cybersecurity Directive must come into force by May 2018, and, therefore, before the UK's departure from the EU. Perhaps less well-known than the GDPR, the Cybersecurity Directive will, as mentioned above, principally affect operators of critical national infrastructure, including in the energy, transport, health, trading and digital sectors. All such providers of essential national services – identified by a set of criteria in the Directive – will be obliged to take appropriate and proportionate security measures around their networks and IT systems, as well as giving timely notification to the competent authority of incidents having a significant impact on the continuity of the services provided by them. As minds turn to the likely post-Brexit data security landscape, and the long-term need for essential equivalence of data protection, awareness and preparations for compliance with the requirements of the Cybersecurity Directive are likely to increase.

Finally, 2016 saw the publication of an enhanced National Cyber Security Strategy and the setting up and commencement of operations of the National Cyber Security Centre. Having a policy body with specific and particular responsibility for these issues at the centre of UK government can only be a good thing. The proof of the pudding here will be in the eating: 2017 will be a demanding year for the new Centre. The will is there for it to succeed, as are the resources, despite the government's very real financial constraints.

interception are also possible, again with the necessary permissions having been obtained. It should be noted that intercept evidence is generally not admissible in criminal proceedings in England.

In data protection terms, the Information Commissioner may serve information notices requiring organisations to: provide the Information Commissioner's Office with specified information within a certain time period; issue undertakings committing an organisation to a particular course of action in order to improve its compliance; serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law; and serve assessment notices to conduct compulsory audits to assess whether an organisation's processing of personal data follows good practice.

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

There have been very few prosecutions of those responsible for cyberattacks. This is likely a consequence of the lack of a dedicated, well-resourced investigative unit, the prime purpose of which is the investigation and prosecution of cybercrime, however, that may change given the creation of the NCA Cyber Crime Unit. 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 countermeasures. In December 2015, the Metropolitan Police Commissioner, announced the creation of a task force of 500 police officers to deal specifically with cybercrime. The evidential difficulties of proving a

criminal offence to the requisite standard are likely to be great, especially given the likely problems in proving the origin of an attack and identifying a particular person or organisation responsible.

Most attention has been given to the Information Commissioner's powers under section 55A DPA, although even under those powers, there have been few prosecutions: 13 prosecutions undertaken, of which 10 resulted in a criminal conviction and four cautions in 2014–2015. The power to impose financial penalties was put in force in April 2010. Between that date and November 2015, the ICO levied fines totalling £783,500, in relation to cybersecurity incidents (which may not be regarded as a significant figure in overall terms). A £250,000 fine was levied on Sony in January 2013 where it failed to put in place on its Network Platform adequate security measures, which meant personal data of a large number of individuals was lost in a (criminal) cyberattack on its network. In August 2014, the Ministry of Justice was fined £180,000 for failing to encrypt data concerning prisoners under its control. In November 2015, a penalty of £200,000 was imposed on the Crown Prosecution Service after laptops containing videos of police interviews were stolen from a private film studio (seemingly on the basis that the laptops were not encrypted).

A more recent example is the cyberattack on the telecoms company, TalkTalk. Following an in-depth investigation by the ICO, it was found that an attack on the company in October 2015 could have been prevented if TalkTalk had taken basic steps to protect customers' information. The attacker accessed the personal data of 156,959 customers including their names, addresses, dates of birth, phone numbers and email addresses. In 15,656 cases, the attacker also had access to bank account details and sort codes. Following the failings of TalkTalk in securing the data, the ICO issued them with a record £400,000 fine (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/) Furthermore, Yahoo have recently discovered a major cyberattack where more than 1 billion user accounts were compromised, making it the biggest cybersecurity breach ever recorded. In December 2016, the ICO issued a statement in response to the security breach. The expectation of the ICO is that any formal investigation will be handled by US and European authorities, but they will continue discussions with Yahoo to ensure 'the data protection interests of UK customers are considered'.

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

Currently, civil actions under section 55A DPA can lead to penalties of up to £500,000. However, under the forthcoming GDPR, there are two categories of offence, both with different penalties. Article 83 sets out the two categories of offence. 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 are individual offences related to child consent and transparency of information and communication. 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 data processing, non-compliance with a notice issued by the Information Commissioner and transfer of data to a third party. It is important to note that the lists of offences in both categories are not exhaustive and so these categories may be expanded upon in the future. The huge increase in potential fines provides greater impetus for businesses to both comply with the GDPR provisions 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?

Generally there are no such reporting requirements, although a failure to report may well be considered an aggravating factor in the event action is taken by the Information Commissioner under section 55A DPA. This will obviously be subject to change when the General Data Protection Regulation comes into force (see question 3).

For public and electronic communications providers, there is a duty under the PECR to submit breach notifications to the ICO. Failure to do so can incur a fine of £1,000.

In 2016, the ICO published guidance on the steps that businesses should take to prepare for the reporting obligations that will apply when the GDPR comes into force in the UK, including implementing a breach reporting procedure.

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

Actions can be taken under the DPA for breaches of the principles including the obligation for a data controller to apply appropriate measures to keep data secure. Alternatively, normal civil law torts will apply, of which the most relevant are actions in breach of confidence and negligence (for failing to keep data secure).

Threat detection and reporting

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

There are currently no set policies or procedures in law or pursuant to government policy that must be implemented. However, good practice would dictate that policies do exist and are implemented, and the lack of policies would almost inevitably give rise to a breach of the DPA and lead to enforcement action from the Information Commissioner (see questions 21, 22 and 24).

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

Although there is no legal obligation on an organisation to record cyber-incidents, and while there is general mention of the importance of incident management, the recording of incidents or threats is not included in the Cyber Essentials accreditation or the government guide on 'Ten Steps to Cyber Security' (www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf). It is, however, suggested in the ISO:27001

BCL BurtonCopeland

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

'control objectives' as a way of logging and monitoring an organisation's cyberspace.

It should be noted that this will change when the GDPR and the Network and Information Security Directive come into force (see question 3) when obligations will be imposed to keep record of any breaches of the Regulation.

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

There are 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 his 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 GCHQ (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.

When the GDPR comes into effect in May 2018, all cybersecurity breaches will have to be notified to the national supervisory authority. 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.