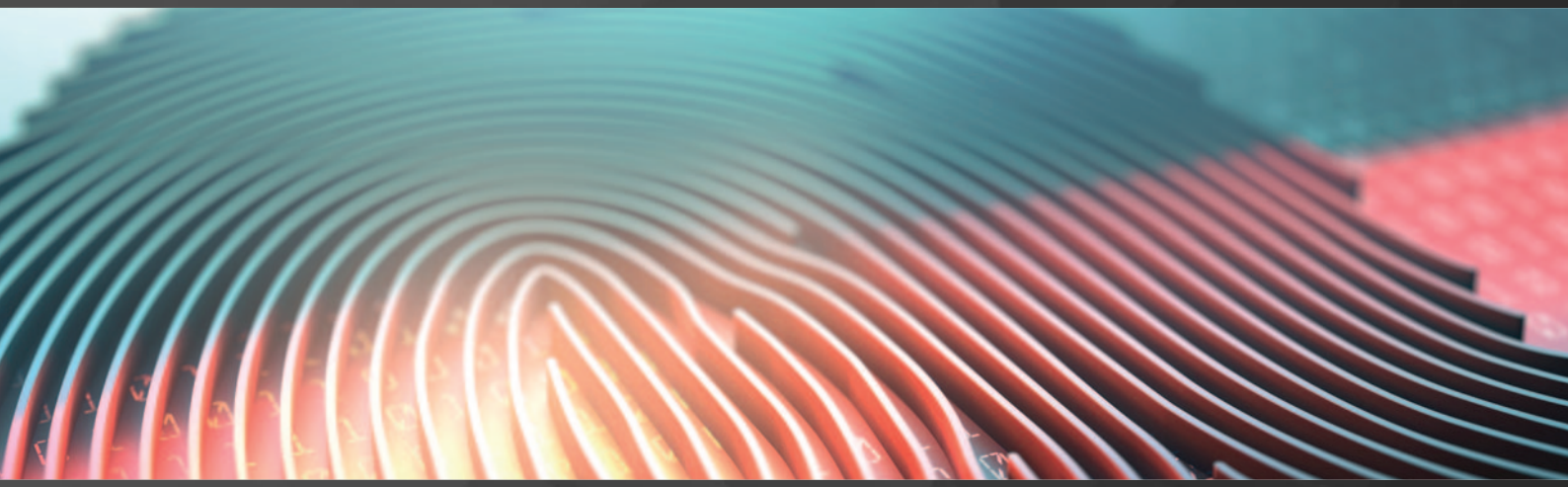
International Comparative Legal Guides



Cybersecurity 2020

A practical cross-border insight into cybersecurity law

Third Edition

Featuring contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Boga & Associates
Christopher & Lee Ong
Cliffe Dekker Hofmeyr
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Faegre Baker Daniels
G+P Law Firm
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.
Iwata Godo
King & Wood Mallesons
Lee & Ko
Lee and Li, Attorneys-at-Law
LEĜA
Lesniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Ropes & Gray
SAMANIEGO LAW
Shardul Amarchand Mangaldas & Co.
Siqueira Castro – Advogados
Sirius Legal
Stehlin & Associés
Synch

ICLG.com

Ireland

Maples Group

Kevin Harnett

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

The Criminal Justice (Offences Relating to Information Systems) Act 2017 (the "2017 Act") came into force on 12 June 2017, giving effect to Directive 2013/40/EU regarding criminal attacks against information systems.

Hacking (i.e. unauthorised access)
Hacking is an offence in Ireland, which, under section 2 of the 2017 Act, occurs when a person who, without lawful authority or reasonable excuse, intentionally accesses an information system by infringing a security measure.

Denial-of-service attacks
Denial-of-service attacks constitute an offence under the 2017 Act, captured under section 3, which provides that it is an offence when a person who, without lawful authority: intentionally hinders or interrupts the functioning of an information system by inputting data on the system; transmits, damages, deletes, alters or suppresses, or causes the deterioration of, data on the system; or renders data on the system inaccessible.

Phishing
Phishing does not, *per se*, constitute a specific offence in Ireland. However, it is possible that the activity would be caught by certain other, more general criminal legislation, depending on the circumstances (for instance, relating to identity theft or identity fraud). In this regard, see below.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infection of IT systems with malware is also an offence, again covered by the 2017 Act. In this regard, section 4 provides that a person who, without lawful authority, intentionally deletes, damages, alters or suppresses, or renders inaccessible, or causes the deterioration of data on an information system commits an offence.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
Possession or use of hardware, software or other tools used to commit cybercrime also constitutes an offence under the 2017 Act (section 6), which occurs when a person who, without lawful authority, intentionally produces, sells, procures for use, imports, distributes, or otherwise makes available, for the purpose of the commission of an offence under the 2017 Act, certain hacking tools. Such tools are described as "(i) any computer programme that is primarily designed or adapted for use in connection with the commission of such an offence, or (ii) any device, computer password, unencryption key or code, or access code, or similar data, by which an information system is capable of being accessed".

Identity theft or identity fraud (e.g. in connection with access devices)
Although there is no precise, standalone offence of identity theft or identity fraud in this jurisdiction, it can nonetheless potentially be captured by the more general offence referred to as "making a gain or causing a loss by deception" (as contained in section 6 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (the "2001 Act")). This occurs where a person who dishonestly, with the intention of making a gain for himself or herself or another, or of causing loss to another, by any deception induces another to do or refrain from doing an act. In addition, sections 25, 26 and 27 of the 2001 Act cover specific forgery offences.

Separately, under section 8 of the 2017 Act, identity theft or fraud is an aggravating factor when it comes to sentencing, in relation to "denial-of-service attack" or "infection of IT systems" offences. This is described in broad terms as being a misuse of the personal data of another person with the aim of gaining the trust of a third party, thereby causing prejudice to that person.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft is covered by the relatively broad offence of "unlawful use of a computer", as provided for in section 9 of the 2001 Act. This occurs where a person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Section 5 of the 2017 Act creates the offence of "intercepting the transmission of data without lawful authority", which occurs when a person who, without lawful authority, intentionally intercepts any transmission (other than a public transmission) of data to, from or within an information system (including any electromagnetic emission from such an information system carrying such data). This is a broad provision which potentially covers other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

With regard to penalties, in relation to offences under the 2017 Act, the penalties range from maximum imprisonment of one year and a maximum fine of €5,000 for charges brought "summarily" (i.e., for less serious offences), to a maximum of five years' imprisonment (10 years in the case of denial-of-service attacks) and an unlimited fine for more serious offences. The above offences under the 2001 Act are only tried in the Circuit Court, with "making a gain or causing a loss by deception" carrying a maximum penalty of five years' imprisonment and an unlimited fine, and forgery and "unlawful use of a computer" offences carrying a maximum of 10 years and an unlimited fine.

Owing to the relatively recent implementation of the 2017 Act, there have been very few (if any) prosecutions of note under this particular legislation to date. That said, Ireland's first successful prosecution for hacking took place in July 2013 on foot of charges under the Criminal Damage Act 1991. The prosecution followed a collaborative investigation between the Irish Garda Bureau of Fraud and the FBI, and involved the hacking of a major political party's website during the run-up to a national election.

There have also been a number of relatively high-profile denial-of-service attacks on large national websites over the last couple of years (those of certain governmental departments and the national lottery, to name a few), which are currently the subject of ongoing investigations. These investigations may lead to some element of prosecution under the 2017 Act in the near future.

Failure by an organisation to implement cybersecurity measures

There is no particular offence in this jurisdiction directly linked to a failure by an organisation to implement cybersecurity measures. That said, and in specific relation to personal data concerning individuals, section 71 of the Data Protection Act 2018 (the "**DPA**") provides that controllers must ensure that data is "processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against (a) unauthorised access or unlawful processing, and (b) accidental loss, destruction or damage".

The Data Protection Commission (the "**DPC**") may, under its statutory powers, notify an organisation that it is deemed to have breached these obligations, and further issue an enforcement notice in this respect. It is then an offence for any controller or processor to, without reasonable excuse, fail or refuse to comply with such a notice. The maximum fine imposable in this regard is €250,000 or imprisonment for a term not exceeding five years.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All of the above offences under the 2017 Act have certain extraterritorial application, and so offenders may therefore be tried in Ireland, so long as they have not already been convicted or acquitted abroad in respect of the same act, and the relevant act was committed:

(a) by the person in Ireland in relation to an information system outside of the country;
(b) by the person outside of the country in relation to an information system in Ireland; or
(c) by the person outside of the country in relation to an information system also outside of the country, if:
    (i) that person is an Irish citizen, a person ordinarily resident in Ireland, or a company established or existing under Irish law; and
    (ii) the act is an offence under the law of the place where it was committed.

Although broader concepts such as, for instance, the "European arrest warrant" may be of relevance for Irish prosecutors, none of the above-mentioned offences under the 2001 Act carry, in and of themselves, extraterritorial application.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Each of the above offences under the 2017 Act contain the ingredient that it was committed without "lawful authority", which is defined as either "with the authority of the owner of the system", "with the authority of a right holder of the system", or "as permitted by law". Accordingly, prosecution of these offences will require, necessarily, that such authority or lawful permission was absent.

In addition, the offence relating to "hacking" carries a further qualification, i.e., where the person or company had a "reasonable excuse". This term is, however, not defined under the 2017 Act, and so its precise application will depend on future judicial interpretation.

In addition, if a company is charged with any of the above 2017 Act offences where the offence was committed by an employee for the benefit of that company, it will be a defence for that company that it took "all reasonable steps and exercised all due diligence" to avoid the offence taking place.

Separately, it can be expected that judges will continue to take established factors into account when considering the appropriate penalty on foot of a conviction of a cybersecurity-related crime (e.g., remorse, amends, cooperation with investigators, criminal history, and extent of damage).

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

It is, for instance, an offence under section 8 of the Offences against the State (Amendment) Act 1998 to "collect, record or possess information which is of such a nature that it is likely to be useful in the commission by members of any unlawful organisation of serious offences generally or any particular kind of serious offence". The term "serious offence" would encompass any of the above-mentioned offences (apart from failure to comply with an enforcement notice issued by the DPC), so long as the act in question is one which involves "serious loss of or damage to property or a serious risk of any such loss…or damage". The maximum sentence for this offence includes an unlimited fine and 10 years' imprisonment. To date, there does not appear to have been any prosecutions of note which have combined this particular offence with acts of cybercrime.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Apart from the above-referenced statutes in respect of criminal activity, Applicable Laws include the following:

- Data Protection: The DPA governs the manner in which personal data is collected and processed in Ireland. The DPA

requires that controllers take "appropriate security measures" against unauthorised access, alteration, disclosure or destruction of data, in particular where the processing involves transmission of data over a network. The DPA adopted the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**") to Irish law in May 2018.

- e-Privacy: The e-Privacy Regulations 2011 (S.I. 336 of 2011), which implemented the e-Privacy Directive 2002/58/EC (as amended by Directives 2006/24/EC and 2009/136/EC) (the "**e-Privacy Regulations**"), regulate the manner in which providers of publicly available telecommunications networks or services handle personal data and require providers to take appropriate technical and organisational measures to safeguard the security of its services and report Incidents. It was intended that a revised EU e-Privacy Regulation be introduced in May 2018 to replace the existing e-Privacy Directive and e-Privacy Regulations, expanding the current regime to cover all businesses which provide online communication services. That new regulation is still in draft form and at the date of writing has not yet been finalised.
- Payments Services: The new Payments Services Directive II (Directive 2015/2366/EU), was transposed by the European Union (Payment Services) Regulations 2018 (S.I. 6 of 2018) (the "**Payment Services Regulations**") on 12 January 2018, and introduced regulatory technical standards (which were published by the European Banking Authority) to ensure "strong customer authentication" and payment service providers will be required to inform the national competent authority in the case of major operational or security Incidents. Providers must also notify customers if any Incident impacts the financial interests of its payment service users. The Payment Services Regulations superseded the previous regime which was introduced in 2009.
- The Security of Network and Information Systems Directive 2016/1148/EU (the "**NISD**") was transposed into Irish law in September 2018 under S.I. 360/2018 and is known as the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 ("**NISD Regulations**"). The NISD seeks to harmonise cybersecurity capabilities and achieve a common level of network and information systems security across the EU by increasing cooperation amongst EU Member States, improving national capabilities and introducing security measures and Incident reporting obligations for certain operators of essential services.
- Other: If there is a security breach which results in the dissemination of inaccurate information, persons about whom the inaccurate data relates may seek a remedy under the Defamation Act 2009. Similarly, if information was provided in confidence and such information was leaked, there may be an action under common law for breach of confidence or negligence, in the event that a duty of care is found to have been owed.

See also sections 1 and 5.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

As noted above, the NISD was transposed into Irish law in September 2018 under the NISD Regulations. The NISD is also the subject of Commission Implementing Regulation (EU) 2018/151, which specifies further elements to be taken into account when identifying measures to ensure security of network and information systems. Publicly available telecommunications networks and services are governed by the e-Privacy Regulations outlined at question 2.1 above.

We do not believe that the implementing legislation exceeds the requirements of the NISD in any material way.

The Department of Communications, Climate Action and Environment ("**DCCAE**")) published the National Cyber Security Strategy 2015–2017, which provides a mandate for the National Cyber Security Centre to engage in activities to protect critical information infrastructure. In March 2019 the Government opened a public consultation designed to consider what a new, replacement strategy should focus on. That public consultation has now closed and a new National Cyber Security Strategy is expected shortly. As matters stand, the DCCAE together with the Government Taskforce on Emergency Planning and the Office of Emergency Planning in the Department of Defence operate as lead government departments for emergency situations relating to, inter alia, critical infrastructure.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the DPA, controllers are required to take appropriate measures, as outlined in questions 1.1 and 2.1 above. The DPA does not detail specific security measures to be undertaken but in determining appropriate measures, a controller may have regard to the state of technological development and the cost of implementing the measures. Controllers must ensure that the measures provide a level of security appropriate to the harm that might result from a breach and the nature of the data concerned. The DPC has issued guidance which suggests the introduction of measures such as access controls, automatic screen-savers, encryption, anti-virus software, firewalls, software patching, secure remote access, back-up systems and Incident response plans.

Under the e-Privacy Regulations, providers of publicly available telecommunications networks or services are required to take appropriate technical and organisational measures and ensure the level of security appropriate to the risk presented, having regard to the state of the art and cost of implementation. Such measures shall at least ensure that personal data can only be accessed by authorised personnel for legally authorised purposes, protect personal data against accidental or unlawful destruction, loss, alteration, processing, etc., and ensure the implementation of a security policy.

The NISD Regulations require that operators of essential services take appropriate measures to prevent and minimise the impact of Incidents affecting the security of the network and information systems used for the provision of essential services with a view to ensuring continuity. Similarly, digital service providers are required to identify and take appropriate and proportionate technical and organisational measures to manage risks posed having regard to the state of the art and take account of, *inter alia*, the security of the systems and facilities, Incident handling, business continuity management and compliance with international standards.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Applicable Laws are largely harmonised at an EU level, and as such the risk of conflicts of laws is minimised. However, the existence of differing requirements for organisations with operations both within the EU and externally may present compliance challenges for such companies.

With regard to the confidentiality of electronic communications, it is understood that updated interception legislation is in the process of being prepared, namely the Interception of Postal Packets and Telecommunications Messages (Regulation) (Amendment) Bill. This was included in the Government's autumn 2019 legislative programme, but has not been prioritised for the current legislative session. The purpose of the bill is to update the Postal and Telecommunications Acts 1983 and 1993, which are limited in scope to postal services and traditional telecommunications providers, to regulate the lawful interception of all communications delivered over the internet.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Section 86 of the DPA contains a general personal data breach notification obligation to the DPC. Where a personal data breach occurs, the controller shall without undue delay and, where feasible, within 72 hours of becoming aware of the breach, notify the DPC of the breach. This notification shall include a description of the breach, the number or approximate number of data subjects concerned and personal data records concerned. It must also contain a list of likely consequences of the breach and measures taken or proposed to be taken to address the breach.

Where a data breach occurs that is likely to result in a high risk to the rights and freedoms of a data subject, Section 87 of the DPA requires the controller to notify the data subject to whom the breach relates. The requirement is waived where the controller has implemented appropriate measures to protect the data; in particular where the measures render the data unintelligible through encryption or otherwise to any person not authorised to access it. This notification must contain at least the same information provided to the DPC as described above.

Providers of publicly available telecommunications networks or services are required to report information relating to Incidents or potential Incidents to the DPC (to the extent that such Incidents relate to personal data breaches). In the case of a particular risk of a breach to the security of a network, providers of publicly available telecommunications networks or services are required to inform their subscribers concerning such risk without delay and, where the risk lies outside the scope of the measures to be taken by the relevant service provider, any possible remedies including an indication of the likely costs involved. In case of a personal data breach, such providers must notify the DPC without delay and where the said breach is likely to affect the personal data of a subscriber or individual, notify them also. If the provider can satisfy the DPC that the data would have been unintelligible to unauthorised persons, there may be no requirement to notify the individual or subscriber of the breach.

Under Article 17of the NISD Regulations, operators of essential services must notify the National Cyber Security Centre without delay of any Incident having a substantial impact on the provision of a service. The notification must provide sufficient information so that the National Security Cyber Centre can assess the significance of same and any cross-border impact. The NISD Regulations stipulate that notification shall not make the notifying party subject to increased liability.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

See above at question 2.5 regarding the requirement to notify the DPC.

The National Cyber Security Strategy published in 2015 outlines the intention of the DCCAE to deepen its partnerships with third-level institutions to aid the sharing of knowledge, experience and best practice. Moreover, the Strategy outlines the active information-sharing role between the DCCAE and other public sector bodies and industry at the time (including IRISS-CERT). Under the NISD Regulations, the CSIRTs Network is tasked with exchanging and making available, on a voluntary basis, non-confidential information concerning individual Incidents.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

See question 2.5 above.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

Parties must ensure that personal data is processed (e.g., shared) in accordance with the DPA and take appropriate security measures with regard to any onward transmission of data including in the context of notifications of Incidents. Personal data includes data relating to a living individual who is or can be identified from either the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the controller. There are exemptions under the DPA such as for the processing of data which is necessary for the administration of justice or to enable the

controller to comply with a legal obligation. Therefore, different considerations apply in the context of voluntary sharing of personal data relating to a breach, and mandatory reporting. For that reason, controllers should take particular care when a notification includes any personal data and take steps to anonymise data where appropriate. Additional considerations also apply in the case of 'special categories of personal data' as set out in Part 3, Chapter 2 of the DPA.

Parties must also be conscious of their contractual obligations and whether issues may arise regarding the sharing of price-sensitive or confidential information, particularly if there is no mandatory requirement to do so.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The DPC is the primary regulator responsible for enforcing the requirements outlined above. The DPC is an independent body established under the DPA.

Under the NISD, the national competent authority is the National Cyber Security Centre.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

There is no automatic penalty for controllers under the DPA in the event of a data breach. However, if the DPC issues an information notice (requiring certain information) or enforcement notice (requiring certain action), a controller or processor must comply with same. If they do not comply, it will constitute an offence. The DPC (unlike under the previous regime) can now impose administrative fines directly as follows:

- a maximum of €5,000 or imprisonment for a term not exceeding 12 months or both on summary conviction; and
- a maximum of €250,000 or imprisonment for a term not exceeding five years or both for conviction on indictment.

The original draft of the DPA exempted public bodies from administrative fines, but following intense lobbying, the DPA now provides for fines of up to €1 million in respect of those bodies.

Further, the DPA also incorporates in Section 141 the right of the DPC, as the supervising authority, to impose fines of up to €20 million or 4% of global turnover as set out in Article 83 of the GDPR.

Under the e-Privacy Regulations, a person who commits an offence is liable on summary conviction to a fine. Furthermore, if a person is convicted of an offence, the court may order any material or data that appears to it to be connected with the commission of the offence to be forfeited or destroyed and any relevant data to be erased.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In the first half of 2018 the DPC completed its investigation into Yahoo! EMEA Limited ("**Yahoo!**") following a data breach at that company which was first reported in 2016, where material was taken from approximately 500 million user accounts.

The investigation concluded amongst other things that Yahoo!'s security policies did not take adequate account of its obligations under data protection laws. It was instructed by the DPC to review and update its policies to so take account of data protection laws.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Subject to compliance with the various legislation identified above, there is no specific prohibition on the use of beacons for such purposes.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Subject to compliance with the various legislation identified above, there is no specific prohibition on the use of honeypots for such purposes.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Subject to compliance with the various legislation identified above, there is no specific prohibition on the use of sinkholes for such purposes.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, market practice with respect to information security varies considerably in Ireland dependent on the industry sector concerned. Businesses in industries that are recognised as being particularly vulnerable to Incidents, such as the financial services sector, are more likely to have adequate processes in place to effectively address cyber risk. With current and long-term trends, such as the continued expansion of cloud computing, mobile data and the internet of things further increasing exposure to cyber risk, financial services firms are expected to update and implement their processes accordingly. The publication of the Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks by the regulator for financial institutions, the Central Bank of Ireland, provides valuable information on the practices that financial services firms are expected to apply in order to protect their organisations from cyber threats.

Other industries have previously been less cognisant of the need for adequate cybersecurity protections. For example, the manufacturing industry in Ireland has been largely unaffected by Incidents. However, advances in robotics, technology and the digital marketplace have increased the awareness of manufacturers to the need for maintenance and protection of cyber infrastructure. In response to this, IBEC, the largest business and employer association for organ-

isations based in Ireland, has highlighted the prioritisation of cybersecurity as a key component in the development of the manufacturing industry in Ireland and has set out a number of recommendations in a recent report setting out their short- to medium-term strategy for Ireland's manufacturing industry.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) There is currently no specific legislation focused on cybersecurity applicable to organisations in the financial services sector. In the absence of any codified law, the Central Bank of Ireland has published Cross Industry Guidance, which relates to IT governance and risk management by regulated financial institutions in Ireland. The publication makes a number of recommendations including (but not limited to): the preparation of a well-considered and documented strategy to address cyber risk; the implementation of security awareness training programmes; the performance of cyber risk assessments on a regular basis; and the implementation of strong controls by firms over access to their IT systems. The NISD Regulations introduce security measures and Incident reporting obligations for credit institutions. See also reference to Payment Sources Regulations in question 2.1 above.

(b) While there are no specific laws on cybersecurity, electronic communications companies (such as telecoms companies and ISPs) are governed by the DPA, and also the e-Privacy Regulations. Under the e-Privacy Regulations, there are more explicit rules governing the security of personal data. The electronic communications sector has been further affected by the introduction of the DPA in May 2018. Businesses in the sector have had to familiarise themselves with the new requirements introduced, notably in the areas of transparency, security and accountability for controllers and processors. Certain operators (IXPs, DNS service providers and TLD name registries) also now fall within the ambit of the NISD Regulations.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

While there are no express directors' duties specific to cybersecurity, directors owe fiduciary duties to their company under common law and under the Companies Act 2014 (the "**CA 2014**").

There are a number of key fiduciary duties of directors set out in the CA 2014. This list, however, is not exhaustive. Some examples of directors' duties which could be considered to extend to cybersecurity are:

- exercise their powers in good faith in what the director considers to be the interests of the company;
- act honestly and responsibly in relation to the conduct of the affairs of the company;
- act in accordance with the company's constitution and exercise his or her powers only for the purposes allowed by law;
- exercise the care, skill and diligence which would be exercised in the same circumstances by a reasonable person having both the knowledge and experience that may reasonably be expected of a person in the same position as the director with the knowledge and experience which the director has; and
- have regard to the interests of its employees in general.

Directors have a general duty to identify, manage and mitigate risk, as well as fiduciary duties, such as those outlined above, which would extend to cybersecurity. Such duties could be interpreted to mean that directors should have appropriate policies and strategies in place with respect to cyber risk and security and that directors should review and monitor these on a regular basis. Regard may also be had to compliance by a company with all relevant legislative obligations imposed on that company in assessing compliance by directors with their duties. Appropriate insurance coverage should also be considered.

Directors should be fully briefed and aware of all of the key issues relating to cyber risk. Larger organisations may choose to delegate more specific cyber risk issues to a specific risk sub-committee.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

While there are no such express obligations from a company law perspective, general director fiduciary duties, best corporate governance practices, as well as the "appropriate security" requirements under the DPA, may dictate that such actions are performed. See question 4.1 above for more detail on directors' duties. For industry-specific requirements, see question 3.1 above.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

While there are no such express obligations from a company law perspective, general director fiduciary duties, as well as best corporate governance practices, may dictate that such actions are performed. See question 4.1 above for more detail on directors' duties.

The e-Privacy Regulations oblige electronic communications service providers to report all data breaches to the DPC. The DPA has introduced a more general personal data breach notification obligation to the DPC, which may be of relevance to an Incident. The NISD Regulations introduced Incident reporting obligations for certain operators of essential services. Where an Incident is relevant to the carrying out of a function regulated by the Central Bank of Ireland, this may give rise to a disclosure requirement to the Bank.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

This chapter sets out the principal laws and requirements relating to cybersecurity in Ireland. However, there may be other requirements and/or recommendations established by industry-specific codes of conduct. In addition, there may be other laws that do not directly relate to cybersecurity but which establish requirements that bear on cybersecurity. See, in addition, section 2 above.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

As discussed in response to question 5.3 below, an Incident may give rise to various claims under the law of tort. It is also conceivable that an Incident would, depending on the circumstances, give rise to a claim for breach of contract.

In order to be entitled to compensation in damages, whether under a tortious or contractual analysis, a plaintiff will be required to establish: that a duty or obligation was owed to him/her by the defendant; that an Incident has occurred as a result of the defendant acting in breach of that duty or obligation; and loss or damage has been sustained to the plaintiff which would not have been sustained, but for the defendant's conduct.

It should be noted that many classes of Incident will also give rise to claims for damages for breach of the constitutional right to privacy. Moreover, where an Incident is committed by a State actor, for example, during the course of an investigation, it may give rise to an action in judicial review to prevent misuse of any inappropriately obtained data and/or to quash any decision taken in relation to, and/or on foot of, the Incident or any improperly obtained data.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Duggan v Commissioner of an Garda Síochána, Ireland and the Attorney General [2017] IEHC 565 – This case affirmed the previously stated position from *Collins v FBD Insurance Plc* [2013] IEHC 137 that a breach of the Data Protection Acts 1988 and 2003 would not automatically entitle a data subject to compensation irrespective of whether or not they could prove actual loss or damage. The High Court concluded that a data subject has no entitlement to automatic compensation for a technical breach of his/her rights under the Data Protection Acts 1988 and 2003 where he/she cannot prove that he/she has suffered loss or damage as a result of the breach. Under the new regime, Article 82 of the GDPR provides that a person who has suffered material or *non-material* damage as a result of an infringement of the GDPR has a right to compensation. The introduction of a right of action for "non-material" damage will likely result in a lower threshold for recoverability as a result of Incidents with a personal data dimension.

CRH plc and Others v Competition and Consumer Protection Commission [2017] IECS 34 – The Supreme Court upheld the finding of the High Court that, in seizing material unrelated to an investigation, the Competition and Consumer Protection Commission had acted outside the scope of its statutory powers and would be acting in breach of the applicants' rights to privacy were it to examine such material. In the exercise by the State of its powers of search, the Supreme Court held that interference with the right to privacy was inevitable but that such interference must be proportionate.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Depending on the specific type of Incident concerned, liability in tort may arise. Examples of such tortious liabilities are as follows:

- The DPA permits a data subject to take a data protection action against a controller or processor where they believe their rights have been infringed. This is deemed to be an action founded in tort. Importantly, the DPA confirms that the damage for which the data subject is seeking compensation need not be just financial. A data subject can sue for other types of damage including pain and suffering.
- A breach of a person's privacy rights may give rise to a claim in tort for breach of confidence or negligence, depending upon the circumstances.
- Incidents involving the theft of information or property may give rise to claims in the tort of conversion.
- Incidents involving the publication of intrusive personal information may in some circumstances constitute the tort of injurious or malicious falsehood.
- Incidents involving the misuse of private commercial information may give rise to claims for damages for tortious interference with economic relations.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

"Cyber insurance" products are being taken up by businesses with increasing frequency and are now seen as routine. Such products afford cover for various data- and privacy-related issues including: the financial consequences of losing or mis-appropriating customer or employee data; the management of a data breach and attendant consequences, including the costs associated with involvement in an investigation by the DPC and fines levied for breaches; and the costs associated with restoring, recollecting or recreating data after an Incident.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no legal limits placed on what the insurance policy can cover. In the ordinary way, however, the consequences of intentional wrongdoing tend to be contractually excluded, as are the consequences of failure to remedy ascertained weaknesses or shortcomings in systems.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

An employer should avoid covert and excessive monitoring of employees. Under the DPA and the ECHR, employees are entitled to privacy, which generally means that employers must balance their need to monitor employees for the purposes of protecting their business against the individual employee's right to privacy. Each case would be decided on its particular circumstances.

The Irish whistleblowing legislation, the Protected Disclosures Act 2014, protects employees from penalisation arising out of reporting actual or possible wrongdoing. In addition, the employer should keep in mind its obligations under data protection legislation when processing personal data, including that such data is kept secure and, where applicable, obligations arising under the e-Privacy Regulations and under the NISD. Employees should be made aware, typically by means of a written company policy or relevant provision in the employment contract, of such obligations and their duty to adhere to such obligations on behalf of the company.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No. Whistleblowing laws do not limit or prohibit such reporting by an employee; instead, they are intended to protect the employee from penalisation following his/her making such a report to the employer.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Under the 2017 Act, the Irish police force (generally operating out of the Garda National Economic Crime Bureau) is given a relatively broad authority to investigate cybersecurity Incidents or suspected activity. Specifically, a warrant is obtainable so as to enter and search a premises, and examine and seize (demanding passwords, if necessary) anything believed to be evidence relating to an offence, or potential offence, under the 2017 Act, from a District Court Judge on foot of a suitable Garda statement, on oath.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no requirements under Irish law for organisations to implement backdoors to their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys.

Kevin Harnett joined Maples Group in 2009 and was elected as a partner in 2016. He previously worked for a multinational software company as corporate counsel and prior to that, he trained and practised with a large Irish corporate law firm. Kevin has extensive experience advising both domestic and multinational clients on large and complex commercial disputes, including proceedings before the Commercial Court, as well as all forms of alternative dispute resolution and related advisory work. He has a particular focus on the financial services, technology and construction sectors.

Maples Group
75 St. Stephen's Green
Dublin 2, D02 PR50
Ireland

Tel: +353 1 619 2036
Email: kevin.harnett@maples.com
URL: www.maples.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Law
Business Crime
Cartels & Leniency
Class and Group Actions
Competition Litigation
Construction & Engineering Law
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investments
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Sanctions
Securitisation
Shipping Law
Telecoms, Media and Internet Laws
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by global legal group