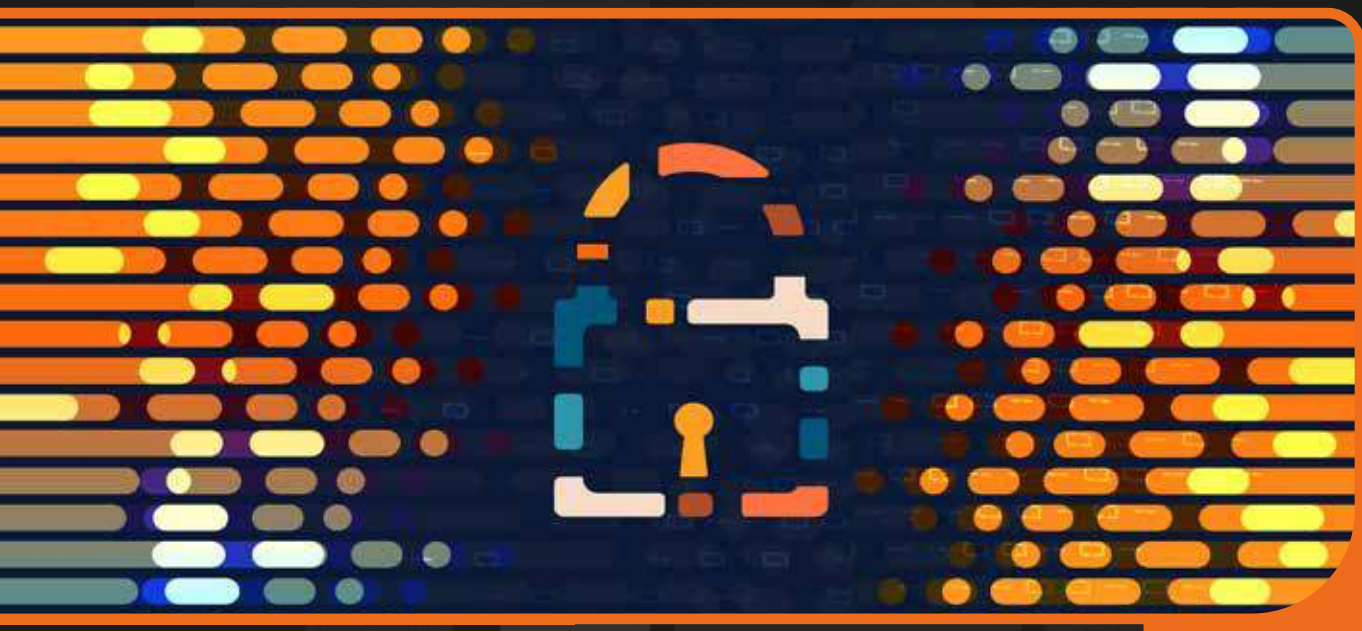
International
Comparative
Legal Guides



Practical cross-border insights into cybersecurity

Cybersecurity 2023

Sixth Edition

Contributing Editor:
Edward R. McNicholas
Ropes & Gray LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Ireland

Claire Morrissey

Brian Clarke

Maples Group

1 Cybercrime

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

Hacking (i.e. unauthorised access)
Yes, hacking is an offence under section 2 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 (the "**2017 Act**"). A person who, without lawful authority or reasonable excuse, intentionally accesses an information system by infringing a security measure, commits an offence.

Denial-of-service attacks
Yes, denial-of-service attacks are an offence under section 3 of the 2017 Act. 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, commits an offence.

Phishing
Phishing does not in itself 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 under Irish law. Pursuant to section 4 of the 2017 Act, any 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.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
Distribution, sale or offering for sale hardware, software or other tools used to commit cybercrime are also offences under Irish law (section 6 of the 2017 Act). It 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.

Possession or use of hardware, software or other tools used to commit cybercrime
As above, possession or use of hardware, software or other tools used to commit cybercrime constitutes an offence under the 2017 Act (section 6).

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, herself or another; or 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.

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, herself or another, or of causing loss to another.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Unsolicited penetration testing is an offence under the 2017 Act (section 2) where it involves intentionally accessing an IT system by infringing a security measure without lawful authority (i.e. permission of the system owner/right holder or where otherwise permitted by law) or "reasonable excuse". This term is not defined under the 2017 Act, and its application will depend on future judicial interpretation.

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 created the offence of "intercepting the transmission of data without lawful authority". This 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).

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 relevant 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.

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. 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.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

The offences under the 2017 Act all provide that they are committed without "lawful authority" (i.e. permission of the system owner/right holder or where otherwise 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 not defined under the 2017 Act, and so its application will depend on future judicial interpretation.

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.

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 cyber-related crime (e.g. remorse, amends, co-operation with investigators, criminal history, and extent of damage).

2 Cybersecurity Laws

2.1 *Applicable Laws*: 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, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, 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 General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**") and the Data Protection Acts 1988 to 2018 (the "**DPA**") govern the manner in which personal data is collected and processed in Ireland. Data controllers are required to 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, and comply with strict reporting obligations in relation to Incidents. The DPA also provides for offences related to disclosure and/or sale of personal data obtained without prior authority.
- **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 implement appropriate technical and organisational measures to safeguard the security of its services and report Incidents. It also prohibits interception or surveillance of communications and the related traffic data over a publicly available electronic communications service without users' consent. The draft EU e-Privacy Regulation is intended to replace the existing e-Privacy Directive and e-Privacy Regulations and expand the current regime to cover all businesses that provide online communication services.
- **Network and Information Systems**: The Security of Network and Information Systems Directive 2016/1148/EU (the "**NISD**") was transposed into Irish law under S.I. 360/2018 European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 (the "**NISD Regulations**"). The European Parliament and the Council reached a provisional agreement on the text of a revised Directive on the Security of Network and Information Systems on 13 May 2022 ("**NIS2**"), which will replace the NISD. NIS2 will introduce a number of key changes to the NISD framework, including having broader applicability than the NISD. NIS2 will cover additional sectors and include medium and large entities operating within the sectors covered by NIS2 in its scope, rather than only operators of essential services and digital services providers. Higher administrative fines up to €10 million or 2% of global annual turnover will also be introduced.
- **Payments Services**: The Payments Services Directive II (Directive 2015/2366/EU or "**PSD2**"), was transposed by the European Union (Payment Services) Regulations 2018 (S.I. 6 of 2018) (the "**Payment Services Regulations**"), 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.
- **Other**: If there is a security breach that results in the dissemination of inaccurate information, persons about whom the inaccurate data relates may seek a remedy under the Defamation Act 2009 or at common law for breach of confidence or negligence.

See also sections 1 and 5.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The NISD Regulations and 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, will apply. The National Cyber Security Strategy 2019–2024 provides a mandate for the National Cyber Security Centre (the "**NCSC**") to engage in activities to protect critical information infrastructure. Enforcement powers under the NISD Regulations allow NCSC-authorised officers to conduct security assessments and audits, require the provision of information and issue binding instructions to remedy any deficiencies.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the GDPR and DPA, controllers are required to take appropriate measures, as outlined in questions 1.1 and 2.1 above. The GDPR and DPA do 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 Data Protection Commission (the "**DPC**") has issued guidance for controllers on data security, including recommending encryption, anti-virus software, firewalls, software patching, secure remote access, logs and audit trails, back-up systems and Incident response plans. At the outset of COVID-19, the DPC published guidance on protecting personal data when working remotely. It supplements existing DPC security guidance and focuses on keeping devices, emails, cloud and network access and paper records secure.

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 must 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 ("**OES**") and digital 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 and digital services with a view to ensuring continuity.

2.4 *Reporting to authorities*: 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.

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 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, the controller must 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. The DPC and European Data Protection Board have also published guidelines on data breach notification.

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.

The NISD Regulations require OES and digital providers to notify the NCSC without delay of any Incident having a substantial impact on the provision of a service. The notification must provide sufficient information so that the NCSC can assess the significance of the same and any cross-border impact. The NISD Regulations stipulate that notification shall not make the notifying party subject to increased liability.

Section 19 of the Criminal Justice Act 2011 mandates reporting certain cybercrimes to the Irish police force, An Garda Síochána. Failure to make such a report, without reasonable excuse, is an offence.

The Central Bank of Ireland's (the "**CBI**") *Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks* ("**Cross Industry Guidance**") requires firms to notify the Bank when they become aware of a cybersecurity Incident that could have a significant and adverse effect on the firm's ability to provide adequate services to its customers, its reputation or financial condition.

2.5 *Reporting to affected individuals or third parties*: 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.

Please see the response to question 2.4 above.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Please see the response to question 2.4 above.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Failure to have appropriate security measures in place and/or report a data security breach in accordance with the GDPR can result in one of a number of administrative sanctions, including a ban on processing, and the potential exposure to fines up to €10 million or 2% of the global turnover (whichever is higher).

Failure by providers of publicly available telecommunications networks or services to comply with the above-mentioned requirements under the e-Privacy Regulations is an offence, liable to a fine of up to €250,000. 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.

Failure by an OES or a digital service provider to notify an Incident is an offence under the NISD Regulations liable to a fine of up to €500,000.

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

The years 2021 and 2022 saw some high-profile enforcement activity in respect of these requirements. In December 2021, the CBI fined Bank of Ireland ("**BOI**") €24.5 million in connection with breaches pertaining to its IT service continuity framework and related internal controls failings.

In 2022, the DPC announced large fines on Meta Platforms ("**Meta**") and BOI for various breaches of the GDPR. A €17 million fine was imposed on Meta for the failure to have in place appropriate technical and organisational measures that would enable it to readily demonstrate the security measures that it implemented in practice to protect EU users' data, in the context of 12 personal data breaches. BOI was fined €463,000 for the failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of customer data in transferring information to the Central Credit Register, failure to report data breaches to the DPC without undue delay, and failure to notify those data subjects affected by the breach without undue delay.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

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)
There is no specific prohibition on the use of beacons for such purposes, but careful consideration would need to be given as to whether such use might itself constitute "hacking" under the 2017 Act.

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.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber attacks?

Monitoring or interception of electronic communications on private networks to prevent or mitigate the impact of cyber-attacks must comply with the GDPR's requirements, including in relation to transparency, necessity and proportionality. The e-Privacy Regulations prohibit interception or surveillance of communications and the related traffic data over a publicly-available electronic communications service without users' consent.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber attacks?

The export of dual-use technology (i.e. technology that can be used for both civil and military purposes) is restricted. Most dual-use items can move freely within the EU; however, a licence is required to export them to a third country (i.e. outside the EU). Very sensitive items, such as equipment or software designed or modified to perform "cryptanalytic functions", require a transfer licence for movement within the EU.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practices regarding information security varied considerably in Ireland depending on the industry sector concerned. Businesses in industries recognised as being particularly vulnerable to Incidents, such as the financial services sector, were more likely to have adequate processes in place to effectively address cyber risk. However, the GDPR and factors such as COVID-19, with the increased reliance on remote working and technology, have accelerated investment in information security across all sectors. COVID-19 also provided more opportunities for scams and cyber-attacks with the 2021 Conti cyber-attack on the Irish Health Service Executive (the "**HSE**") being the most high profile. In response to the attack, the Garda Cybercrime Bureau, Ireland's cybercrime unit, seized domains used in the attack and is engaging with Europol and Interpol. The full independent post-incident review of the attack was published in December 2021. Overall, the trends are towards increased security and systems.

4.2 Excluding the requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

(a) Not *per se*; however, the requirement for appropriate systems and procedures is the subject of regulatory focus, and the CBI is focused on ensuring that firms in the financial services sector have appropriate systems, policies and procedures in place, as part of its regulatory supervision mandate. So, for example, the CBI has published Cross Industry Guidance to financial institutions, which 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. Further, the NISD Regulations introduce security measures and Incident reporting obligations for credit institutions. See also the reference to the Payment Services Regulations at question 2.1 above. The European Commission's draft Digital Operational Resilience Act (the "**DORA**") published in September 2020 sees EU financial regulators expanding their focus beyond financial resilience to operational resilience including effective and prudent management of ICT risks and cybersecurity incidents. A Consultation Paper on the CBI's Cross Industry Guidance on Operational Resilience is currently active. The guidance will apply to all regulated financial service providers and includes recommendations regarding identifying, preparing for, responding to, adapting to and learning from operational disruptions, including cybersecurity incidents.

(b) As noted above, electronic communications companies (such as telecoms companies and ISPs) are governed by the GDPR, the DPA, and also the e-Privacy Regulations. Certain operators (IXPs, DNS service providers and TLD name registries) also now fall within the ambit of the NISD Regulations together with essential operators in the energy, transport, health, drinking water and digital infrastructure sectors.

5 Corporate Governance

5.1 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' or officers' 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, which are relevant. This list, however, is not exhaustive. Relevant examples of directors' duties that could be considered to extend to cybersecurity are to:

- exercise the care, skill and diligence that 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, and the knowledge and experience that the director has;
- honestly and responsibly in relation to the conduct of the affairs of the company;
- act in accordance with the company's constitution and exercise their powers only for the purposes allowed by law;
- exercise their powers in good faith in what the director considers to be the interests of the company; and
- have regard to the interests of their 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 are likely to 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, but with the board retaining ultimate oversight and responsibility.

In relation to company secretaries, this will depend on what duties are delegated to the company secretary by the board of directors.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (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 directors' 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 5.1 above for more detail on directors' duties. For industry-specific requirements, see question 4.1 above.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) 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 5.1 above for more detail on directors' duties.

6 Litigation

6.1 Please provide details of any civil or other private 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 6.3 below, an Incident may give rise to various claims under the law of tort and under statute. 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 that would not have been sustained, but for the defendant's conduct.

Many classes of Incident may also give rise to claims for damages for breach of the constitutional right to privacy.

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 (see, e.g. *CRH plc and Others v Competition and Consumer Protection Commission* [2017] IECS 34).

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

In the recent case of *Shawl Property Investments Limited v A & B*, decided in February 2021, the Court of Appeal considered the question of strict liability for data breaches, and, in allowing a claim for breach of data protection rights to progress to a plenary hearing, commented that: "*Nothing stated in s.117 or indeed the Act itself [the Data Protection Act 2018] suggests that a data protection action is a tort of strict liability.*"

In *Lannon v Minister for Social Protection,* a damages action by a man whose address was given by a then employee of the Department of Social Protection to a private detective hired by solicitors for a bank, was settled in the High Court in 2019. This followed a statement of acknowledgment and regret on behalf of the Department that "*data relating to Mr Lannon was released in contravention of the 1988 Data Protection Act by a former employee*".

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Depending on the specific type of Incident concerned, liability for breach of statutory duty or in tort may arise. Examples of such 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.
- 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.

7 Insurance

7.1 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 misappropriating 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 the costs associated with restoring, recollecting or recreating data after an Incident.

7.2 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?

There are no specific regulatory limits placed on what an insurance policy can cover; however, the legal doctrine of the *ex turpi causa non oritur actio* principle (i.e. that a party should not be entitled to enforce a contract that is tainted with illegality in some form, or, a claimant has no remedy allowing it to profit from its own wrongdoing) is recognised under Irish law (see for example the Supreme Court decision in the 2015 case of *Quinn v IBRC*). There is presently no Irish equivalent to the decision of the English Court of Appeal in *Safeway Stores Limited v Twigger [2010] EWCA Civ 1472*, but Irish law recognises similar principles. Whether a policy would permit recovery is dependent on the circumstances, and the nature of the alleged wrongdoing.

As GDPR and DPA administrative fines are intended to be "effective, proportionate and dissuasive", it is certainly arguable that any such fines imposed should not be insurable. It may be said that to allow the same would undermine the dissuasive nature of the fines if they could simply be passed on to an insurer. Similarly, criminal fines prescribed by statute are not likely to be insurable in Ireland. However, there are also arguments to support a contention that where there has been a breach that amounts to an error, as opposed to a purposeful act or omission, that cover for such event and outcome should not offend the public principles.

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. anti-terrorism laws) that may be relied upon to investigate an Incident.

Under the 2017 Act, the Irish police force 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.

The DPC has broad powers to investigate breaches under the DPA, including the power to enter business premises unannounced and without a court-ordered search warrant.

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.

Claire Morrissey is Partner and Head of the Dublin Data, Commercial & Technology practice at Maples and Calder (Ireland) LLP, the Maples Group's law firm. Claire advises on a broad range of data protection issues and commercial contracts with a particular focus on compliance with the GDPR, technology and IP. In addition, Claire regularly advises on the technology, IP and data aspects of joint ventures and mergers & acquisitions.

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

Tel: +353 1 619 2113
Email: claire.morrissey@maples.com
URL: www.maples.com

Brian Clarke is a Partner in Maples and Calder (Ireland) LLP's Dispute Resolution & Insolvency team in the Maples Group's Dublin office. Brian 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 arbitration. Brian is also experienced in managing investigations and acting for clients across various sectors in relation to regulatory investigations and prosecutions.

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

Tel: +353 1 619 2042
Email: brian.clarke@maples.com
URL: www.maples.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group