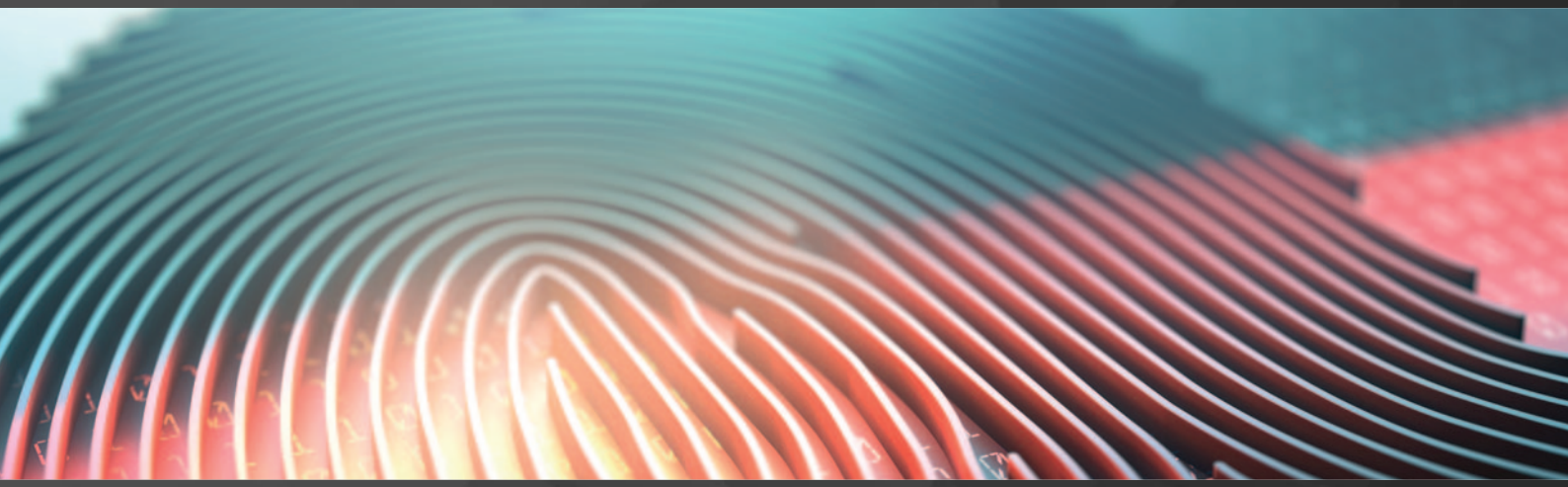
International Comparative Legal Guides



Cybersecurity 2020

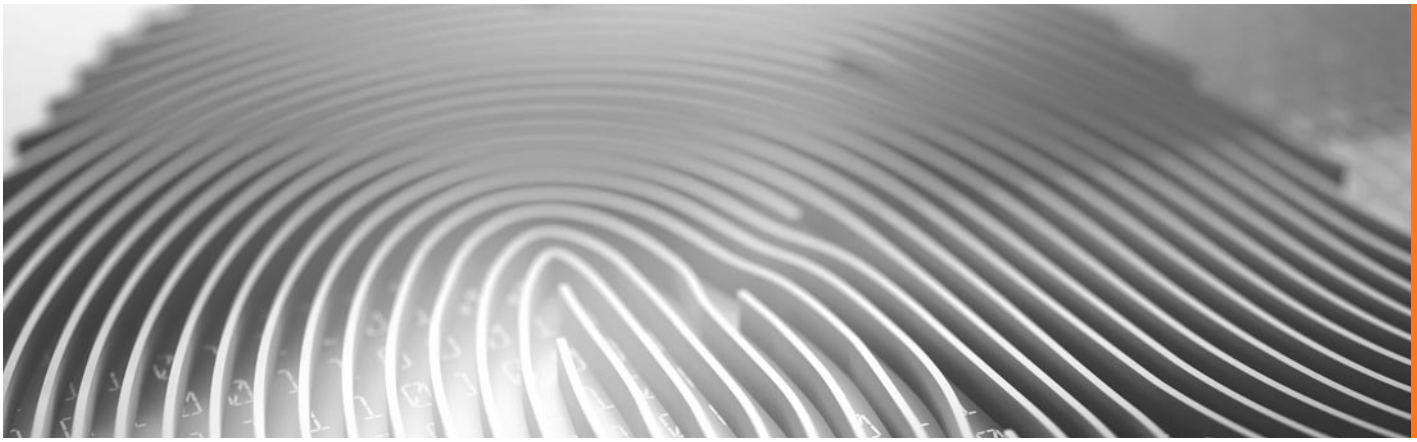
A practical cross-border insight into cybersecurity law

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



ISBN 978-1-83918-005-7
ISSN 2515-4206

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
www.iclg.com

Group Publisher
Rory Smith

Associate Publisher
James Strode

Senior Editors
Caroline Oakley
Rachel Williams

Deputy Editor
Hollie Parker

Creative Director
Fraser Allan

Printed by
Stephens & George
Print Group

Cover Image
www.istockphoto.com

Strategic Partners

Cybersecurity 2020

Third Edition

Contributing Editors:

Nigel Parker and Alexandra Rendell
Allen & Overy LLP

Expert Chapters

Country Q&A Chapters

ICLG.com

From the Publisher

Dear Reader,

Welcome to the third edition of *The International Comparative Legal Guide to Cybersecurity*, published by Global Legal Group.

This publication, which is also available at www.iclg.com, provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to cybersecurity laws and regulations around the world.

This year, there are three general chapters which provide an overview of key issues affecting cybersecurity, particularly from the perspective of a multi-jurisdictional transaction.

The question and answer chapters, which cover 32 jurisdictions in this edition, provide detailed answers to common questions raised by professionals dealing with cybersecurity laws and regulations.

As always, this publication has been written by leading cybersecurity lawyers and industry specialists, to whom the editors and publishers are extremely grateful for their invaluable contributions.

Global Legal Group would also like to extend special thanks to contributing editors Nigel Parker and Alexandra Rendell of Allen & Overy LLP for their leadership, support and expertise in bringing this project to fruition.

Rory Smith
Group Publisher
Global Legal Group

Spain

SAMANIEGO LAW

Javier Fernández-Samaniego

Gonzalo Hierro Viéitez

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:

Hacking (i.e. unauthorised access)
Article 197 *bis* of the Spanish Criminal Code (hereinafter, "**SCrC**") establishes that those, who by any means, without being authorised, breach the security measures and access or facilitate access to an information system, or part of it, or stays in it against the will of whoever has the legitimate right to exclude access, may be punished with up to two years in prison.

Denial-of-service attacks
Denial-of-service attacks ("**DOS**" attacks) are foreseen in Article 264 *bis* SCrC, which holds that causing unauthorised hinderance or interruptions to an informatic system is punishable by up to three years in prison. Article 264.2 SCrC enumerates a series of aggravated cases where the prison term may be as high as five years' imprisonment and a fine.

Phishing
Phishing is foreseen in Article 248.2 SCrC, which identifies phishing as "those who, for profit and using any kind of informatic manipulation –or similar– obtain a non-consensual transfer of assets to the detriment of another". The maximum penalty is three years in prison.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Article 264.1 SCrC holds that any unauthorised erasure, damage, deterioration, alteration or deletion of computer data, software or electronic documents of others, or making it inaccessible, where the result produced is serious, shall be punished with imprisonment of up to a maximum of three years. Article 264.2 SCrC enumerates a series of aggravated cases where the prison term may be as high as five years and a fine.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
The possession or use of hardware, software or other tools used to commit cybercrime, as well as their import, production or, by any means, supply to third parties is foreseen in Article 197 *ter* SCrC. The penalty may be a maximum of two years in prison or a fine.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft is not expressly foreseen in the Spanish Criminal Code. However, some of the most common crimes associated with identity theft or identity fraud, such as those in connection with access devices, e.g. swindling and fraud, are found in Articles 248 *et seq.* and 436 *et seq.*, respectively.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Article 199 SCrC holds that whoever reveals other people's secrets, which he is aware of by reason of his trade or his employment relationships, shall be punished by imprisonment of up to three years and receive a fine.

Article 270 SCrC, which foresees criminal copyright infringement, dictates that those who, in order to obtain a direct or indirect economic benefit to the detriment of a third party, reproduce, plagiarise, distribute, publicly communicate or exploit, in whole or in part, a literary, artistic or scientific work without the authorisation of the holders of the corresponding intellectual property rights, or their assignees, may be punished with up to four years in prison and a fine.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Article 197 SCrC foresees that the interception of telecommunications via listening, transmitting, recording and/or reproduction devices shall be punishable by imprisonment of up to four years and receive a fine.

Failure by an organisation to implement cybersecurity measures
No, failure to implement appropriate cybersecurity measures is not foreseen by the SCrC. However, under the GDPR, organisations may be fined if they do not have in place the appropriate measures to prevent data breaches, taking into account the most recent technical developments, risks, the nature of personal data being processed and the damages to the rights and freedom of the data subject.

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

The extraterritorial application of the SCrC is foreseen in Article 23.2 of the Organic Law 6/1985, of 1 July, on Judicial Power. Article 23.2 holds that Spanish courts will know of crimes committed outside of the Spanish territory as long as the authors are Spanish or they obtain the Spanish nationality, and the following three requisites are met:

i. that the crime is punishable at the place of execution (unless, under an international treaty or a normative act of an international Organisation to which Spain is a party, such a requirement is not necessary);

ii. that the aggrieved person or the Public Prosecutor's Office files before the Spanish courts; and
iii. that the offender has not been acquitted, pardoned or sentenced abroad, or, in the latter case, has not served his sentence.

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?

Besides the mitigating circumstances (Article 21) and the exceptions (Articles 19 and 20) under the general rules of the SCrC, we must highlight, in relation to companies, that an effectively implemented compliance programme may exempt a company from liability.

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.

Article 573.2 SCrC holds that the crimes established under Articles 197 *bis*, 197 *ter* and 264 through 264 *quater* are considered terrorism offences when done with any of the following ends:
i. subvert the constitutional order, supress or destabilise political institutions or economic or social structures of the State or compel the public authorities to perform an act, or to refrain from doing so;
ii. alter public peace;
iii. destabilise the functioning of an international organisation; or
iv. provoke a state of terror in the population or a part of it.

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.

The following European Union ("**EU**") Regulations have a direct effect in Spain:
i. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**"); and
ii. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification ("**Cybersecurity Act**").

Please find the link to the Cybersecurity Code, published by the Spanish Official Gazette editorial, listing all the Applicable Laws related to cybersecurity. Due to the complexity and length of the Spanish regulation on cybersecurity, encompassing over 50 different Applicable Laws, we list below the most relevant ones:
i. Law 36/2015, of 28 September 2015, on National Security;
ii. Law 8/2011, of 28 April 2011, on Measures for the Protection of Critical Infrastructure incorporating Directive 2008/114/EC;
iii. Royal Decree-Law 12/2018, of 7 September 2018 ("**Royal Decree-Law 12/2018**"), incorporating Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union ("**NIS Directive**");
iv. Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce, incorporating E-Commerce Directive 2000/31/EC;
v. Law 59/2003, of 19 December, on the Electronic Signature, incorporating Directive 1999/93/EC;
vi. the General Telecommunications Law 9/2014, of 9 May;
vii. Organic Law 10/1995, of 23 November, on the Criminal Code; and
viii. Organic Law 3/2018, of 5 December on Data Protection and the Guarantee of Digital Rights ("**LOPDGDD**" as per its Spanish initials), which develops the GDPR in Spain.

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.

Article 13 of Law 8/2011 of 28 April on Measures for the Protection of Critical Infrastructures mentions that those who operate Critical Infrastructures must elaborate security plans while Article 16 requires them to appoint a Security and Liaison Officer.

The Regulation on the Protection of Critical Infrastructures, approved by the Royal Decree-Law 704/2001 of 20 May, has developed, concreted and expanded the aspects referred to in Law 8/2011. Articles 22.4 and 25.5 of the Regulation established that the State Secretary of Security would indicate the minimum contents of the Security Plans of the Operator and of the Specific Security Plans mentioned in Article 14 of Law 8/2011. Said minimum contents are described in the Resolution of 8 September 2015 of the State Secretary of Security ("**Resolution**").

The Resolution does not impose any specific cybersecurity requirements. Its main purpose is to establish a methodology to elaborate and design the Security Plans of the Operator (Annex I) and the Specific Security Plans (Annex II).

Royal Decree-Law 12/2018 does not impose harsher security requirements than the NIS Directive, however, it applies not only to Critical Infrastructures but also to Digital Service Providers.

There is a project of a regulation that will further develop the content of Royal Decree-Law 12/2018, which is in the stage of public consultation until 6 September, 2019.

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.

Pursuant to Articles 24 and 25 GDPR, the controller and the processor must implement appropriate technical and organisational measures, such as pseudonymisation, to ensure a level of security appropriate to the identified risk.

Article 28 LOPDGDD references Articles 24 and 25 GDPR in order to determine the appropriate technical and organisational measures to be implemented.

On a side note, the authors recommend to visit the webpage of the National Institute of Cybersecurity of Spain (*Instituto Nacional de Ciberseguridad de España*; "**INCIBE**" as per its Spanish initials) which has a help centre on cybersecurity, available for both companies and individuals, that may be reached by calling the Spanish free toll

number 900 116 117. Furthermore, they periodically publish a Bulletin on cybersecurity.

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.

The risk of conflicts of laws is minimised due to the harmonisation of Applicable Laws at EU level.

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.

Unlike Incidents in Critical Infrastructures or Digital Service Providers where Royal Decree-Law 12/2018 requires, in the event of an Incident that might have significant disturbing effects, that the competent authority be notified (a notification may also be made even if the Incident has not yet produced an adverse effect), organisations are not required to report information related to Incidents or potential Incidents unless the Incident relates to personal data. If such an Incident has an impact on the data subject's rights, the Spanish Data Protection Agency (*Agencia Española de Protección de Datos*; "**Spanish DPA**") should be notified. The notification shall at least:

i. describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
ii. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
iii. describe the likely consequences of the personal data breach; and
iv. describe the measures to be taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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?

Organisations are permitted to voluntarily share information related to Incidents and encouraged to do so with the Computer Security Response Team of INCIBE.

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.

When personally identifiable information of an individual is involved in an Incident, under the GDPR, the controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach, as well as recommendations to mitigate potential adverse effects.

For information purposes, the Spanish DPA has developed a Data Breach Notification form for controllers (Article 33 GDPR) through its online portal.

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?

None of these cases would change the responses to questions 2.5 to 2.7.

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

Regarding Critical Infrastructures, the relevant authority regarding Incidents is the National Centre for the Protection of Infrastructures and Cybersecurity (*Centro Nacional de Protección de Infraestructuras y Ciberseguridad*), whose email for information purposes is ses.cnpic-buzon@interior.es and for Incident-reporting purposes is incidencias.occ@interior.es.

Regarding Digital Service Providers, the relevant authority regarding Incidents depends on whether the Digital Service Provider is from the public or private sector. In the private sector, the relevant authority is the State Secretary for Digital Progress (*Secretaría de Estado para el Avance Digital*) under the Ministry of Economy, whose telephone number for information purposes is +34 912 582 852. In the public sector, the relevant authority is the National Cryptologic Centre (*Centro Criptológico Nacional*), whose email for information purposes is info@cnn-cert.cni.es and for Incident-reporting purposes is incidentes@cnn-cert.cni.es.

The relevant authority regarding Incidents with an impact on personal data is the Spanish DPA (*Agencia Española de Protección de Datos*), with headquarters in C/ Jorge Juan, 6, 28001 Madrid, telephone number +34 912 663 517.

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

Under the GDPR, depending on the nature of the infringement, the administrative fine may amount up to 10,000,000 EUR or 2% of the company's worldwide turnover, and 20,000,000 EUR or 4% of the company's worldwide turnover.

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

There have yet to be any enforcement actions related to the lack of reporting of Incidents imposing fines; however, there have been several warnings by the Spanish DPA.

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)
Yes, the use of beacons is allowed.

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)
Yes, the use of honeypots is allowed.

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)
Due to its direct consequences, sinkholing is usually done in special conditions by trusted third parties with the involvement of law enforcement authorities.

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.

The measures to be implemented are stronger in some business areas, particularly for Critical Infrastructures and Digital Service Providers, which must comply with Royal Decree-Law 12/2018. Companies who host personal health data must also implement stronger security measures as foreseen in the 17th additional provision of the LOPDGDD. With regards to the telecommunications sector, Article 44 of the General Telecommunications Law 9/2014, of 9 May, establishes that network operators and operators of electronic communications shall adequately manage security risks that may affect their network and services in order to ensure an adequate level of security, and avoid or minimise the impact that Incidents may have on users and interconnected networks.

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?

As mentioned above, the NIS Directive has been implemented in Spain by Royal Decree-Law 12/2018 which regulates, among others, the Critical Infrastructures and Digital Service Providers of these two sectors.

In relation to cybersecurity in the financial services sector, entities subject to the GDPR and the Directive (EU) 2015/2366 (the PSD2 Directive) will have to follow two notification processes in case they suffer a major Incident involving personal data. Furthermore, the National Securities Market Commission (*Comisión Nacional del Mercado de Valores*) is looking to regulate, in the short term, the cybersecurity measures which fund managers should implement to control the technological risks associated with their activities.

Regarding the requirements of the telecommunications sector, besides those established in Royal Decree-Law 12/2018, under Article 12 *bis* of Law 34/2002 of 11 July on Information Society Services and Electronic Commerce, Internet service providers have a series of obligations to inform its users, among others, of the different ways to implement and/or increase security measures. In addition, the ninth additional provision of Law 34/2002 holds that information society service providers, domain name registrations and registrars established in Spain are required to collaborate with the competent Computer Security Response Team in resolving Incidents affecting the Internet. Furthermore, they are required to follow specific recommendations on the management of cybersecurity Incidents, which will be developed via codes of conduct (which have yet to be developed). Also, see the answer to question 3.1.

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?

Such a failure may lead to a breach of the directors' duties, as Article 225 of the Spanish Companies Act, concerning duty of care, holds that directors shall perform the duties imposed by laws and statutes with the diligence of an ordained businessman, taking into account the nature of the position and duties assigned. In addition, directors shall have the appropriate dedication and take precise measures for the good direction and control of the company. The Spanish Companies Act, in case of a breach, allows for the director to be liable for damages caused by acts or omissions.

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?

Currently, there is no obligation to designate a CISO, establish a written Incident response plan or policy, conduct periodic risk assessments or perform penetration tests or vulnerability assessments. However, in order to comply with Article 32 GDPR, such measures may be required in order to ensure appropriate security measures. In this sense, security measures must be implemented with consideration given to the level of associated risk. Therefore,

the implementation of these security measures must be assessed on a case-by-case basis.

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)?

In connection with the directors' duty of care (see the answer to question 4.1), under the Spanish Companies Act, the shareholders of a company have the right to be informed when the topic is included in the agenda of the shareholders' meeting.

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

No, there are no other specific requirements.

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.

A civil liability action for damages may be brought under Article 1902 of the Spanish Civil Code, which holds that the person who, as a result of an action or omission, causes damage to another by his fault or negligence shall be obliged to repair the damage caused. Three elements are necessary to establish liability:

i. a fault;
ii. a damage; and
iii. a causal link between i. and ii.

Furthermore, under Article 79 GDPR, a civil action may be brought in the event of an Incident if the controller or processor has not complied with its provisions. In addition, the GDPR foresees the possibility to initiate "European-style" class actions related to data protection matters.

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

There have been many cases brought before the Spanish courts in relation to Incidents. As an example, a bank was sentenced to pay plaintiffs 139,257.04 EUR, amounting to the value stolen, by the Provincial Court of Barcelona in its decision of 22 January 2019 after suffering a phishing attack. However, due to the elusiveness of the authors of cybercrimes, many go unpunished, such as the case of the ransomware Wannacry which affected, among others, Telefónica.

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

In order to exclude liability under the accountability principle stated by the GDPR and the NIS Directive, companies should be in a position to provide sound evidence that they have implemented the appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

6 Insurance

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

Yes, under Law 50/1980, of 8 October, on Insurance Contracts ("**Law on Insurance Contracts**"), insurance against Incidents is permitted. With the number of cyberattacks on the rise, the Spanish cyber-insurance trend is growing rapidly with many major providers offering cyber-insurance in order to cope with these new risks.

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?

The Law on Insurance Contracts imposes two limitations:

i. the insurer does not cover loss or damage resulting from the insured's intentional or wilful misconduct; and
ii. the insurer does not cover the payment of any administrative or judicial sanction, neither any cost derived from it.

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?

For the monitorisation of employees and the reporting of Incidents, three requirements should be met:

i. a previous communication where the employees are told that the company's computer is limited to professional use;
ii. that any breach of i. may be sanctioned; and
iii. that i. and ii. be proportional.

Regarding the reporting by employees to their employer, the designated data protection officer ("**DPO**") has the task of monitoring compliance with the GDPR, which includes the obligation of reporting certain Incidents. Besides the DPO, no other employee has a legal obligation to report a cyber risk, security flaw, Incident or potential Incident unless it is established by the employer through internal regulations.

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?

There are no Applicable Laws that may prohibit or limit reporting.

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.

Cybersecurity is classified as of special interest to national security by Article 10 of Law 36/2015, of 28 September, on National Security.

The laws that may be relied upon to investigate an Incident are, besides those already mentioned in question 2.1, the following:

i. Organic Law 4/2015, of 30 March, on the Protection of the Safety of Citizens;
ii. Law 5/2014, of 4 April, on Private Security; and
iii. Royal Decree-Law of 14 September 1882 approving the Criminal Procedure Law which foresees technology-related investigation measures such as searches on mass storage devices and remote searches on computer systems, among others.

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?

No, in Spain there is no Applicable Law that requires organisations to implement backdoors or to provide encryption keys, as one of the basic principles of Criminal Law is the privilege against self-incrimination and the presumption of innocence.

Javier Fernández-Samaniego is the Managing Director of SAMANIEGO LAW and his international practice focuses mainly on commercial/IT disputes (litigation, arbitration and ADR) and negotiations and major tech & privacy projects (new cloud and big data business models, outsourcing transactions, data protection review programmes, etc.). Javier has vast experience assisting European clients in their expansion into Latin America and US clients in their European expansion. Javier is Senior Fellow at Florida International University, developing its Latin Atlantic Tech Law Collaborative. Before launching Samaniego Law in 2017, Javier was founding and managing partner of the Spanish office of Bird & Bird and head of its Commercial, DR and IT teams for over a decade. Before that Javier worked at Linklaters, Cuatrecasas and CDTI (Spanish Centre for the Development of Industrial Technology).

SAMANIEGO LAW
c/ Serrano 16, 6 D
28001 Madrid
Spain

Tel: +34 910 66 41 06
Email: javier.samaniego@samaniegolaw.com
URL: www.samaniegolaw.com

Gonzalo Hierro Viéitez focuses his practice on transactional and contentious IT law. Before joining SAMANIEGO LAW, he was an associate in the Commercial & IT and Dispute Resolution Groups of Bird & Bird based in Madrid. Prior to that, he was an intern at Cuatrecasas NYC office in its M&A group and at Ashurst London office in its international arbitration group. Gonzalo holds a law degree from Rey Juan Carlos University, a double Master's degree from Carlos III University and ISDE in the Practice of Law and in International Law, Foreign Trade and International Relations, respectively, as well as a dual concentration LL.M. from Fordham University in Banking, Corporate and Finance (awarded *magna cum laude*) and in Information Technology Law. He is licensed to practise law in Spain, admitted to the Madrid Bar and has passed the July 2018 New York Bar Exam.

SAMANIEGO LAW
c/ Serrano 16, 6 D
28001 Madrid
Spain

Tel: +34 910 66 41 06
Email: gonzalo.hierro@samaniegolaw.com
URL: www.samaniegolaw.com

SAMANIEGO LAW is an Ibero-American alternative law firm specialising in IT law and dispute resolution with offices in Madrid and Miami. The firm is a hybrid that combines an international commercial law firm, a legal strategy consultancy firm and a sophisticated solutions platform. The team comprises lawyers and strategic and IT consultants, with support from a long-standing network of trusted professionals and legal interim managers. The firm boasts a simple and flexible organisational structure with smart use of technology, allowing it to offer clients a significant reduction in fees. The firm's clients are typically technology companies and providers of digital transformation solutions, as well as organisations that want to reinvent their business. The firm has a clear focus on the Latin Atlantic region and regularly advises American companies expanding into Europe and, *vice versa*, European companies expanding into the Americas.

www.samaniegolaw.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