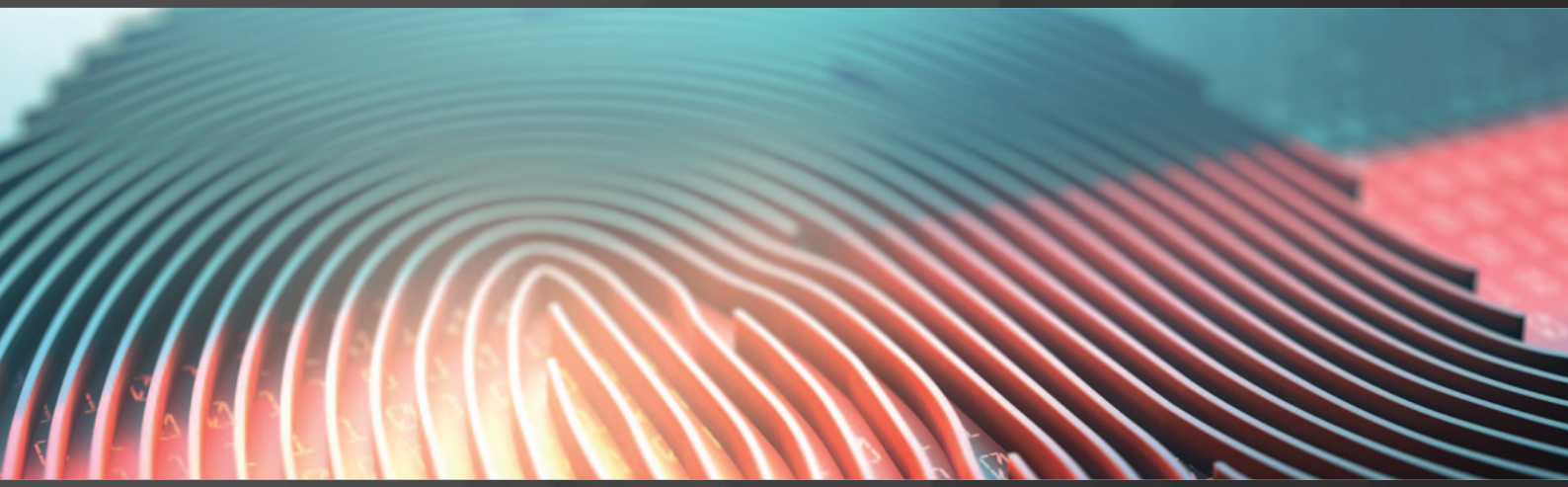
International Comparative Legal Guides



Cybersecurity 2020

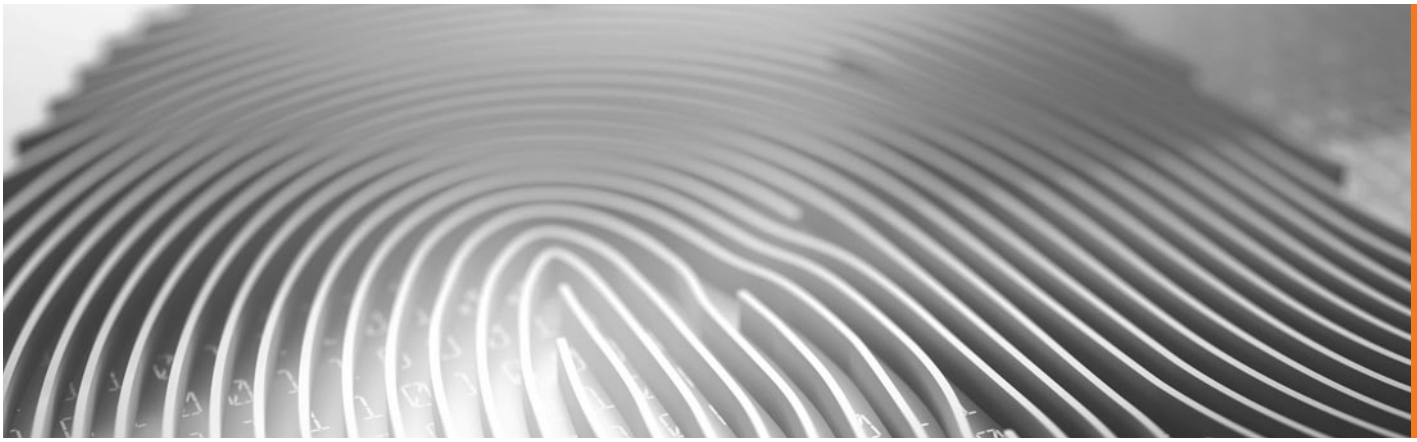
A practical cross-border insight into cybersecurity law

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

Cybersecurity 2020

Third Edition

Contributing Editors:
Nigel Parker and Alexandra Rendell
Allen & Overy LLP

Strategic Partners

©2019 Global Legal Group Limited.
All rights reserved. Unauthorised reproduction by any means, digital or analogue, in whole or in part, is strictly forbidden.

Disclaimer
This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.
This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

Expert Chapters

1 **Effective Cyber Diligence – The Importance of Getting it Right**
Nigel Parker & Alexandra Rendell, Allen & Overy LLP

4 **Franchising in a Sea of Data and a Tempest of Legal Change**
Paul Luehr, Huw Beverley-Smith, Nick Rotchadl & Brian Schnell, Faegre Baker Daniels

11 **Why AI is the Future of Cybersecurity**
Akira Matsuda & Hiroki Fujita, Iwata Godo

Country Q&A Chapters

15 **Albania**
Boga & Associates: Genc Boga & Armando Bode

21 **Australia**
Nyman Gibson Miralis: Dennis Miralis, Phillip Gibson & Jasmina Ceic

29 **Belgium**
Sirius Legal: Roeland Lembrechts & Bart Van den Brande

37 **Brazil**
Siqueira Castro – Advogados:
Daniel Pitanga Bastos De Souza & João Daniel Rassi

43 **Canada**
McMillan: Lyndsay A. Wasser & Kristen Pennington

51 **China**
King & Wood Mallesons: Susan Ning & Han Wu

59 **Denmark**
Synch Advokatpartnerselskab: Niels Dahl-Nielsen & Daniel Kiil

66 **England & Wales**
Allen & Overy LLP: Nigel Parker & Alexandra Rendell

75 **France**
Stehlin & Associés: Frédéric Lecomte & Mélina Charlot

82 **Germany**
Eversheds Sutherland: Dr. Alexander Niethammer & Constantin Herfurth

89 **Greece**
G+P Law Firm: Ioannis Giannakakis & Stefanos Vitoratos

97 **India**
Shardul Amarchand Mangaldas & Co.:
GV Anand Bhushan, Tejas Karia & Shahana Chatterji

106 **Ireland**
Maples Group: Kevin Harnett

115 **Israel**
Pearl Cohen Zedek Latzer Baratz: Haim Ravia & Dotan Hammer

122 **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi

130 **Kenya**
Gikera & Vadgama Advocates: Hazel Okoth & Stella Ojango

137 **Korea**
Lee & Ko: Hwan Kyoung Ko & Kyung Min Son

144 **Kosovo**
Boga & Associates: Renata Leka & Delvina Nallbani

150 **Malaysia**
Christopher & Lee Ong: Deepak Pillai & Yong Shih Han

159 **Mexico**
Creel, García-Cuéllar, Aiza y Enríquez, S.C.:
Begoña Cancino

165 **Norway**
Advokatfirmaet Thommessen AS:
Christopher Sparre-Enger Clausen & Uros Tosinovic

172 **Poland**
Lesniewski Borkiewicz & Partners (LB&P):
Mateusz Borkiewicz, Grzegorz Lesniewski & Joanna Szumilo

180 **Portugal**
Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.: Catarina Costa Ramos

186 **Singapore**
Rajah & Tann Singapore LLP: Rajesh Sreenivasan, Justin Lee & Yu Peiyi

194 **South Africa**
Cliffe Dekker Hofmeyr: Fatima Ameer-Mia, Christoff Pienaar & Nikita Kekana

202 **Spain**
SAMANIEGO LAW: Javier Fernández-Samaniego & Gonzalo Hierro Viéitez

208 **Sweden**
Synch Advokat: Anders Hellström & Erik Myrberg

216 **Switzerland**
Niederer Kraft Frey Ltd.: Clara-Ann Gordon & Dr. András Gurovits

223 **Taiwan**
Lee and Li, Attorneys-at-Law: Ken-Ying Tseng

230 **Thailand**
R&T Asia (Thailand) Limited: Supawat Srirungruang & Visitsak Arunsuratpakdee

238 **USA**
Ropes & Gray: Edward R. McNicholas & Kevin J. Angle

246 **Venezuela**
LEĜA: Carlos Dominguez & Hildamar Fernandez

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

Mexico

Creel, García-Cuéllar, Aiza y Enríquez, S.C.



Begoña Cancino

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:

There is no definition in Mexican law of the terms "cybercrime" and "cybersecurity"; however, the Federal Criminal Code regulates illegal behaviours committed through electronic means that could be identified as cybercrimes by the use of electronic means for their commission.

Regarding examples of jurisdiction in Mexico, according to Article 16 of the Political Constitution of the United Mexican States ("Mexican Constitution"), no one shall be disturbed in his/her private affairs, family, home, papers or possessions (including private information), except by written order of a competent authority, duly grounded in law and fact, which sets forth the legal cause of the proceeding. In this regard, any non-consented access to private information may be sanctioned by law; thus, only a federal judicial authority may authorise any investigation regarding criminal offences.

Hacking (i.e. unauthorised access)
Article 211*bis* of the Federal Criminal Code provides that whoever, without authorisation, modifies, destroys or causes loss of information contained in systems or computer equipment protected by a security mechanism shall be imposed with a prison sentence of six months to two years, by the relevant authority, as well as a fine of approximately MN$8,004.00 to MN$24,012.00. The aforementioned penalty could be duplicated in case the information is used for one's own benefit or to benefit a third party.

Denial-of-service attacks
The Federal Criminal Code does not provide any definition, or similar definition, for this criminal offence.

Phishing
The Federal Criminal Code does not provide any definition for phishing; however, such criminal offence could be considered as fraud. According to Article 386 of the Federal Criminal Code, a person commits fraud when he/she, with the intent of obtaining a financial gain, handles information through deceit, takes advantage of errors, or misleads a person.

In such case, the relevant authority shall impose a prison sentence of three days to 12 years, as well as a fine of approximately MN$2,400.00 to MN$24,012.00, depending on the value in each case.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
The Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour is similar to hacking. The aforementioned penalties are applicable in this case.

In case the criminal offence is committed against the state, the relevant authority shall impose a prison sentence of one to four years, as well as a fine of approximately MN$16,000.00 to MN$48,024.00.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
The Federal Criminal Code provides this criminal offence as "hacking", which is described above.

Identity theft or identity fraud (e.g. in connection with access devices)
The Credit Institutions Law provides that a person who produces, manufactures, reproduces, copies, prints, sells, trades or alters any credit card, debit card, cheques or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be imposed a prison sentence of three to nine years, by the relevant authority, as well as a fine of approximately MN$2,401,200.00 to MN$24,012,000.00.

In addition, the Federal Criminal Code provides that a person who, with or without authorisation, modifies, destroys or causes loss of information contained in credit institutions' systems or computer equipment protected by a security mechanism shall be imposed with a prison sentence of six months to four years, by the relevant authority, as well as a fine of approximately MN$8,004.00 to MN$24,012.00.

Moreover, a person who without authorisation knows or copies information in credit institutions' computer systems or equipment protected by a security mechanism shall be imposed a prison sentence of three months to two years, as well as a fine of approximately MN$4,002.00 to MN$24,012.00.

All the penalties aforementioned could be duplicated if the criminal offence is committed by any counsellor, official, employee or service provider of any credit institution.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
As mentioned, the Credit Institutions Law provides that any person who produces, manufactures, reproduces, copies, prints, sells, trades or alters, any credit card, debit card, cheque or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be imposed with a prison sentence of three to nine years, as well as a fine of approximately MN$2,401,200.00 to MN$24,012,000.00. The aforementioned penalties may be duplicated if the criminal offence is committed by any counsellor, official, employee or service provider of any credit institution.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Yes: espionage; conspiracy; crimes against means of communication; tapping of communications; acts of corruption; extortion; and money laundering could be considered as threats to the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

Failure by an organisation to implement cybersecurity measures
Considering the absence of a specific law which regulates cybersecurity in Mexico, there are no minimum protective measures that organisations must implement to protect data and information technology systems from cyber threats; however, the Federal Law on Protection of Personal Data held by Private Parties ("Data Protection Law") provides that data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

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

Yes; however, Mexico has not yet adopted international standards related to cybersecurity.

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?

Yes, in the following cases:

1) The Federal Law Against Organized Crime provides: (a) that in the investigation of a crime in which it is assumed on good grounds that a member of organised crime is involved, it is possible to tap private communications; and (b) the obligation of concessionaires, authorised entities and any person holding a means or system that could be intercepted, to cooperate with the authorities, prior to a judicial order.
2) The General Law to Prevent and Sanction Kidnapping Crimes provides the possibility to intercept private communications.
3) The National Security Law, in case of an immediate threat to national security, provides that the Mexican government must request a judicial warrant to intercept private communications for national security purposes.
4) The Federal Telecommunications and Broadcasting Law ("FTBL"), according to Articles 189 and 190, provides that: (i) concessionaires; (ii) authorised entities; and (iii) service providers of applications or contents, are required to: a) allow the corresponding competent authorities to control and tap private communications; and b) provide the support that such authorities request, in terms of the applicable law.

In addition to the federal legislation provided above, there are state laws that allow the interception of individual communications prior to any request from the relevant state authorities (Public Prosecutor of the corresponding state) to a federal judge.

Intervention of private communications is not allowed in: electoral tax; commercial; civil; labour; or administrative matters, or in the case of communications between the arrested and his/her counsel.

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.

As mentioned, the Federal Criminal Code also regulates as a criminal offence the act of sabotage or unlawful interference with: roads, public services, or state services; steel, electric or basic industries; and centres of production or distribution of weapons, ammunition or military equipment, with the aim of disrupting the economic life of the country or to affect its ability to defend itself.

Also, the relevant Code protects means of communication such as telegrams, telephone lines, radio communications, telecommunication networks, and any component of an installation of production of magnetic or electromagnetic energy or its means of transmission.

In addition, the Federal Criminal Code provides that persons who manufacture, import, sell or lease any device or system, or commit any act with the purpose of decoding any encrypted/protected satellite signal without the legitimate authorisation of the licensed distributor, shall be imposed with a prison sentence of six months to four years.

On the other hand, the Law on Negotiable Instruments and Credit Operations sanctions diverse actions that affect any kind of financial payment instrument (e.g., credit or service cards) or the information contained on them.

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 Mexican Constitution.
- The FTBL.
- The Data Protection Law, its Regulations, Recommendations, Guidelines and similar regulations on data protection.
- The Federal Law on Transparency and Access to Public Information.
- The General Law on Transparency and Access to Public Information.
- General Standards as the Mexican Official Standard Regarding the Requirements that shall be Observed when Keeping Data Messages.
- The Law on Negotiable Instruments and Credit Operations.
- The Mexican Federal Tax Code.
- The Credit Institutions Law.
- The Sole Circular for Banks.
- The Industrial Property Law.
- The Mexican Copyright Law.
- The Federal Criminal Code.
- The National Security Law.
- The Federal Labour Law.
- The Federal Law for the Federal Police.
- The National Development Plan 2013–2018.
- The National Programme of Public Security 2014–2018.
- The National Programme of Security 2014–2018.

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.

This is not applicable in Mexico.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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.

As mentioned, there are no minimum protective measures that organisations must implement to protect data and information technology systems from cyber threats; however, the Data Privacy Law provides that data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

In addition to the foregoing, there are certain specific mandatory security measures that certain industries must adopt to protect their customers' data. Banking laws and regulations provide that banks must implement certain security measures in electronic banking transactions and require the use of several passwords depending on the amount and nature of the transaction.

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.

This is not applicable in Mexico.

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.

There is no obligation to report Incidents or potential Incidents to the authorities; however, the General Law on Transparency and Public Information Access provides, in Article 70 Section XLVII, that authorities must provide access and keep updated, for statistical purposes, the list of requests made to telecommunications concessionaires, service providers or internet applications related to the interception of private communications, access to the registry of communications, and the real-time geo-location of communication equipment, that contains the object, temporary scope and legal grounds of the request and, if applicable, a statement of judicial authorisation.

On the other hand, Data Privacy Laws do not provide a penalty for failure to comply with the rules on reporting threats or breaches; nevertheless, the National Institute for Access to Public Information and Data Protection ("INAI") is empowered to evaluate if the cause that originated a data breach was caused by a failure of compliance or negligence.

By the interpretation of the Mexican Constitution, organisations must cooperate with government agencies regarding Incidents; however, no law establishes specific requirements to report Incidents or potential Incidents.

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?

Please refer to our answer in question 2.5.

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.

There is no obligation to report any Incidents or potential Incidents; however, Data Protection Law provides that security breaches that materially affect the property or moral rights of data owners will be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights.

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?

No, the responses to questions 2.5 to 2.7 do not change.

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

The INAI is in charge of: (i) guaranteeing people's right of access to public government information; (ii) protecting personal data in possession of the federal government and individuals; and (iii) resolving denials of access to information that the dependencies or entities of the federal government have formulated.

The Federal Telecommunications Institute ("IFT") is in charge of regulating telecommunications and broadcasting services.

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

The Applicable Laws are silent in this regard.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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

This is not applicable in Mexico.

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

Answer not available at time of print.

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. According to the Data Protection Law, the data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

On the other hand, the Federal Criminal Code and the Law on Negotiable Instruments and Credit Operations provide several sanctions in order to avoid criminal offences regarding cybersecurity.

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?

Yes. Regarding financial services, the Law on Negotiable Instruments and Credit Operations and the Credit Institutions Law, including the Federal Criminal Code, are applicable in order to avoid cybercrimes.

The FTBL and the Federal Criminal Code are applicable in this matter.

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?

There are no specific laws in Mexico related to cybersecurity responsibilities or liabilities of personnel and directors. Nevertheless, and in accordance with the Data Protection Law, every private party, individual or organisation that processes personal information (data controller), has the obligation to appoint a data person or department (data protection officer) who will be a representative for the organisation in privacy and data protection matters and in charge, within the organisation, of the correct processing of personal data (including verification of security measures), as well as of processing requests from data owners for the exercise of their rights to access, rectification, suppression or rejection.

In relation to information security, data protection officers shall adopt measures to guarantee due processing of personal data, privileging the interests of the data owners and their reasonable expectation of privacy.

The measures that the data protection officer shall adopt, and that may be related to cybersecurity, include the following: (i) issuing policies and programmes, which shall be mandatory within the organisation; (ii) implementing training programmes; (iii) implementing a monitoring and surveillance system and internal or external audits to verify compliance with privacy policies; (iv) assigning resources for the implementation of programmes and policies related to privacy; (v) implementing a risk-detection programme to identify privacy risks when launching new products, services, technologies and business models as well as risk-mitigation strategies; (vi) periodically reviewing security policies and programmes to determine whether amendments are needed; (vii) performing compliance checks; and (viii) implementing personal data-tracking systems to trace which data are collected and where they are stored.

The Data Protection Law does not provide a specific sanction for data protection officers, responsible personnel and directors.

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?

Regarding personal data, all data controllers must designate a data protection officer or department; however, the Applicable Laws are silent on cybersecurity matters.

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)?

The Applicable Laws are silent in this regard.

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

The Applicable Laws are silent in this regard.

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.

According to Article 32 of the Federal Criminal Code, organisations and companies are civilly liable for the damages caused to third parties by crimes committed by their partners, managers and directors. The state is similarly liable for the crimes committed by its public officials.

The Federal Civil Code provides a standard of civil liability established in Article 1910, which provides that a party that illegally causes harm to another person shall be obliged to repair the damage, unless he/she proves that the damage was produced as a consequence of the victim's guilt or negligence.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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

This is not applicable in Mexico.

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

This is not applicable in Mexico.

6 Insurance

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

Yes, organisations are permitted to take out insurance against Incidents in our jurisdiction.

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?

This is not applicable in Mexico.

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?

There are no specific requirements; however, the Data Protection Law provides that a person who is involved with personal data is obligated to establish and maintain physical and technical administrative security measures and in case of any breach, such employee must notify the data protection officer.

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?

This is not applicable in Mexico.

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.

The Applicable Laws empower the following authorities to investigate an Incident: (i) the General Attorney Office; (ii) Public Prosecutors; (iii) the INAI; and (iv) the IFT.

Public Prosecutors in Mexico are in charge of investigating and resolving cyber activities; a cyber police service has been created to follow up on crimes or unlawful activities committed through the Internet. Complaints directed to the cyber police can be submitted via its website, by phone, or through a Twitter or email account; in addition, the Federal Police have created a scientific division called the National Centre For Cyber-Incidents Response, specialised in providing assistance to the victims or claimants of cyber threats and cyber attacks.

In the case of data protection, the INAI may conduct investigations to follow up personal data matters. The IFT is in charge of the telecommunications sector.

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?

The Applicable Laws are silent in this regard.

© Published and reproduced with kind permission by Global Legal Group Ltd, London



Begoña Cancino is a partner in the Mexico City office. Her practice focuses on Intellectual Property, Data Privacy, Regulatory and Administrative Litigation. From the standard IP front, Ms. Cancino counsels clients from all kinds of industries with the protection and enforcement of their IP rights in Mexico, assisting also with the transfer of IP portfolios within the context of complex corporate transactions involving all sort of IP rights (such as trademarks, copyrights and appellations of origin). Ms. Cancino also provides assistance with her legal advice on regulatory and advertising, assessing our clients to comply with all applicable provisions with COFEPRIS and PROFECO. She has represented clients in all sort of administrative litigation proceedings, in general, concerning advertising, health, environmental and, of course, IP matters, before administrative authorities and federal judicial courts. Pursuant to the data privacy aspects of her practice, Ms. Cancino has counselled clients from multiple industries in the drafting and implementation of internal policies, privacy notices and specific legal concerns, not only regarding client daily operations, but also within the context of cross-border transactions and internal investigations for compliance.

Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Pedregal 24, 24th Floor
Molino del Rey
11040, Mexico City
Mexico

Tel: +52 55 4748 0679
Email: begona.cancino@creel.mx
URL: www.creel.mx

Creel, García-Cuéllar, Aiza y Enríquez is an award-winning, full-service corporate law firm. It has over 80 years of experience in providing international and domestic clients with technical excellence, knowledge of the market and unparalleled client service. The firm is a strategic service provider to clients with the most complex and demanding transactions and projects, affording them certainty and peace of mind. The firm provides innovative solutions to many of the largest, most intricate, first-ever market-leading deals in Mexico. We are a full-service corporate law firm, specialising in the following practice areas and industries: antitrust and competition; arbitration and dispute resolution; banking and finance; bankruptcy and restructuring; capital markets; corporate and commercial; employment and labour; energy and natural resources; environmental; infrastructure; insurance and reinsurance; intellectual property; mergers and acquisitions; private equity; *pro bono*; project development and finance; real estate; social security; tax; telecommunications; and transportation.

www.creel.mx

CREEL GARCÍA-CUÉLLAR AIZA Y ENRÍQUEZ

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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