Cybersecurity 2021

Contributing editors
Benjamin A Powell and Jason C Chipman



LEXOLOGY®
Getting The Deal Through

GDR

© Law Business Research 2021

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between January and February 2021. Be advised that this is a developing area.

© Law Business Research Ltd 2021
No photocopying without a CLA licence.
First published 2015
Seventh edition
ISBN 978-1-83862-643-3

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Cybersecurity
2021

Contributing editors
Benjamin A Powell and Jason C Chipman
Wilmer Cutler Pickering Hale and Dorr LLP

Lexology Getting The Deal Through is delighted to publish the seventh edition of *Cybersecurity*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes a new chapter on Belgium and the European Union.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors Benjamin A Powell and Jason C Chipman of Wilmer Cutler Pickering Hale and Dorr LLP, for their continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
February 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in March 2021
For further information please contact editorial@gettingthedealthrough.com

© Law Business Research 2021

Contents

Global overview 3
Benjamin A Powell and Jason C Chipman
Wilmer Cutler Pickering Hale and Dorr LLP

Austria 4
Árpád Geréd
MGLP Rechtsanwälte | Attorneys-at-Law

Belgium 13
Peter Craddock and Camille De Munter
NautaDutilh

China 21
Yunxia (Kate) Yin, Jeffrey Ding and Gil Zhang
Fangda Partners

European Union 29
Thomas Kahl, Detlef Klett and Paul Voigt
Taylor Wessing

France 36
Claire Bernier and Elise Neau
ADSTO

Germany 43
Axel von Walter
Beiten Burkhardt

India 51
Rohan Bagai and Aprajita Rana
AZB & Partners

Japan 60
Masaya Hirano and Kazuyasu Shiraishi
TMI Associates

Mexico 69
Begoña Cancino
Creel García-Cuéllar Aiza y Enriquez SC

Poland 76
Michał Korszla and Kamila Spalińska
Adwokaci i Radcowie Prawni spółka komandytowa Izabella Żyglicka i Wspólnicy

Singapore 85
Lim Chong Kin
Drew & Napier LLC

Switzerland 96
Michael Isler, Jürg Schneider and Hugh Reeves
Walder Wyss

Turkey 104
Stéphanie Beghe Sönmez
Paksoy

United States 112
Benjamin A Powell, Jason C Chipman and Matthew F Ferraro
Wilmer Cutler Pickering Hale and Dorr LLP

© Law Business Research 2021

Mexico

Begoña Cancino

Creel García-Cuéllar Aiza y Enriquez SC

LEGAL FRAMEWORK

Legislation

1 | Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Below is a list of the main statutes and regulations that promote cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of incidents:

- the Mexican Constitution;
- the Federal Telecommunications and Broadcasting Law (FTBL);
- the Federal Law on the Protection of Personal Data held by Private Parties (the Data Protection Law), its regulations, recommendations, guidelines and similar regulations on data protection;
- the Federal Law on the Protection of Personal Data held by Obliged Subjects;
- the Federal Law on Transparency and Access to Public Information;
- the General Law on Transparency and Access to Public Information;
- the General Law of the National Security System;
- NOM-151 – General 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 Federal Law for Industrial Property Protection;
- 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 2019–2024;
- the National Strategy of Cybersecurity 2017;
- the Sector Program for Security and Citizens' Protection 2020–2024; and
- the National Plan of Peace and Security 2018–2024.

2 | Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

There is an industry-specific risk in certain sectors: financial, telecommunications and health not only in the private sector, but also at the governmental level. The National Security Guard Act of 8 November 2019, which allows Mexican authorities to rule judicial decisions to intervene in private communications for national security purposes, anticipated the replacement of the Center of Investigation and National Security by the newly created National Intelligence Center, a Mexican intelligence agency controlled by the Ministry of Security and Civilian Protection, the main purpose of which is to preserve the state's integrity, stability and endurance. This was a radical structural change in the Mexican government, as the former intelligence agency was under the control of the Ministry of Interior – the purpose is to reinvent the image of the agency as an authority focused on security instead of conducting 'authorised' espionage. During 2019, the National Intelligence Center hosted an official meeting where representatives of the National Bureau of Investigation and the Department of Justice agreed with the Mexican government on a programme to coordinate efforts to reinforce the exchange of information concerning cybersecurity, including best practices to cope with activities that pose a risk for Mexico and the United States of America (ie, regarding financial, telecommunications and health information, not only in the private sector but also at the governmental level).

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

On 14 April 2015, the Ministry of Economy published in the Mexican Official Gazette the implementation of three Mexican official standards, including:

- NMX-I-27001-NYCE-2015 Tecnologías de la Información-Técnicas de Seguridad-Sistemas de Gestión de Seguridad de la Información-Requisitos, which reproduces the provisions set forth in the ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements; and
- NMX-I-27002-NYCE-2015 Tecnologías de la Información-Técnicas de Seguridad-Código de Buenas Prácticas para el Control de la Seguridad de la información, which reproduces the provisions set forth in the ISO/IEC 27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Controls.

These Mexican official standards are mandatory in Mexico for all types of organisations, regardless of their nature.

4 | What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Several activities include specific obligations and sanctions for those who, within the scope of their employment, take part in any of them. For a better reference on who is liable and how they may be held responsible for inadequate cybersecurity, see 'Scope and jurisdiction'.

© Law Business Research 2021

5 How does your jurisdiction define cybersecurity and cybercrime?

The terms cybercrime and cybersecurity are not defined in Mexican laws; however, the National Strategy of Cybersecurity 2017 defines both terms as follows:

> *Cybercrimes: Criminal actions carried out by individuals that use information and communication technologies as a means or as an end and that are typified in a criminal code or other national code. Accordingly, the Federal Criminal Code regulates illegal behaviors committed through electronic means that could be identified as cybercrimes by the use of electronic means for their commission.*

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

According to Mexican laws (specifically, the Mexican Privacy Law), organisations are compelled to implement corrective, preventive and improvement measures to make security measures adequate to avoid a breach. Organisations should be able to differentiate between material and non-material harm under Mexican laws by conducting a risk analysis. Material harm should be prioritised over non-material harm and will always depend on the business, scope, context and processing of the data compromised in the incident. Industry-specific risk identification of material and non-material harm is thus crucial for all companies facing a cybersecurity incident. Certain sectors, such as healthcare and banking, should provide companies with the required latitude to adapt their own internal policies. Compromising the security of databases, sites, programmes or equipment (and this may include failure to implement security measures required) constitutes an administrative infringement of the Mexican Privacy Law, which could be sanctioned with fines of up to 25.6 million Mexican pesos, a fine that may be doubled if sensitive data is compromised.

Scope and jurisdiction

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

See below.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

See below.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

The Mexican Constitution includes the constitutional right to the inviolability of private communications; accordingly, the federal criminal code includes specific provisions to sanction these practices. There are exceptions in the following cases:

- The Federal Law against Organised Crime provides:
  - 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
  - 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.
- The General Law to Prevent and Sanction Kidnapping Crimes provides the possibility to intercept private communications.
- The National Security Law, in the 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.
- The FTBL, according to articles 189 and 190, provides that concessionaires, authorised entities and service providers of applications or contents are required to:
  - allow the corresponding competent authorities to control and tap private communications; and
  - 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 alleged perpetrator of a crime and his or her counsel.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

- Hacking (ie, 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 given a prison sentence of six months to two years, by the relevant authority, as well as a fine of approximately 8,004 to 24,012 pesos. The aforementioned penalty could be doubled 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 or she handles information through deceit, takes advantage of errors or misleads a person with the intent of obtaining a financial gain. In such case, the relevant authority shall impose a prison sentence of three days to 12 years, as well as a fine of approximately 2,400 to 24,012 pesos, 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. If the criminal offence is committed against the state, the relevant authority shall impose a prison sentence of one year to four years, as well as a fine of approximately 16,000 to 48,024 pesos.
- Possession or use of hardware, software or other tools used to commit cybercrime (eg, hacking tools): the Federal Criminal Code provides this criminal offence as hacking, which is described above.
- Identity theft or identity fraud (eg, 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 or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be given a prison sentence of three to nine years, by the relevant authority, as well as a fine of approximately 2,401,200 to 24,012,000 pesos.

© Law Business Research 2021

- Electronic theft (eg, 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 or, in general, any other payment instrument, including electronic devices, issued by credit institutions without authorisation of the holder, shall be given a prison sentence of three to nine years, as well as a fine of approximately 2,401,200 to 24,012,000 pesos. The aforementioned penalties could be doubled if any counsellor, official, employee or service provider of any credit institution commits the criminal offence.
- In addition, under the Federal Law for the Protection of Industrial Property, the theft of trade secrets – either by electronic means or not – by current or former employees constitutes a crime and triggers imprisonment and fines to the responsible parties.
- Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime: the Federal Criminal Code contains a specific criminal offence in this regard, providing that those who manufacture, import, distribute, rent or in any way market devices, products or components intended to circumvent an effective technological measure would be subject to imprisonment from six months to six years and a fine.
- Possession or use of hardware, software or other tools used to commit cybercrime: the Federal Criminal Code provides that those who, knowingly, without authorisation and for profit, suppress or alter, by themselves or through another, any information on rights management, will be imprisoned from six months to six years and liable to pay a fine. The same penalty will be imposed on whoever, for profit:
    - distributes or imports for distribution information on rights management, knowing that it has been suppressed or altered without authorisation; or
    - distributes, imports for distribution, transmits, communicates or makes available to the public copies of works, performances or phonograms, knowing that the information on rights management has been suppressed or altered without authorisation.
- Unsolicited penetration testing (ie, the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points): the Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour may fall into the scope of hacking. The aforementioned penalties are applicable in this case. If the criminal offence is committed against the state, the relevant authority shall impose a prison sentence of one year to four years, as well as a fine .

In addition, activities such as 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.

Also, 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 given a prison sentence of six months to four years, by the relevant authority, as well as a fine of approximately 8,004 to 24,012 pesos. Moreover, an unauthorised person who knows or copies information from credit institutions' computer systems or equipment protected by a security mechanism shall be subject to a prison sentence of three months to two years, as well as a fine of approximately 4,002 to 24,012 pesos. All the aforementioned penalties could be doubled if any counsellor, official, employee or service provider of any credit institution commits the criminal offence.

On the other hand, it should be considered that under the Mexican Privacy Law (Federal Law on the Protection of Personal Data held by Private Parties), authorising to process personal data for profit, causing a security breach and affecting databases constitutes a criminal offence and the data controller would be liable if these actions occur with databases under his or her custody. The individual responsible will be subject to imprisonment for between three months and three years, which may be doubled if the personal data compromised includes sensitive information.

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

Security challenges associated with cloud computing typically arise because of differences or lack of legal provisions or inefficient contractual structures regulating the relationship between the organisation and the cloud services provider. The Mexican Privacy Law sets forth the importance of entering into service agreements with at least the following contractual conditions for the cloud computing services provider:

- it shall use similar policies to protect personal data to those reflected in Mexican law;
- if the service provided involves subcontracting, such provisions should be transparent;
- it should not assume any ownership of the information regarding the service provided; and
- it should maintain confidentiality with respect to the personal data it holds.

In addition, the cloud computing services provider should, as a minimum, have mechanisms in place for:

- disclosing changes in its privacy policies and the services provided;
- permitting the data controller to limit the type of processing of personal data included in the service provided;
- establishing and maintaining adequate security measures to protect data included in the service provided;
- ensuring the suppression of data after the service has been provided;
- impeding access to non-authorised parties and informing the data controller if there is an official request of data from a competent authority; and
- informing the data controller of the events of the breach immediately after its occurrence, and providing the data controller with all the necessary information for assessing the extent of the damage caused by the breach in accordance with Mexican legal provisions.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Yes, Mexican provisions are applicable to foreign organisations doing business in the country.

BEST PRACTICE

Increased protection

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Yes, there are non-mandatory guidelines drafted by certain federal regulators (such as the Network for Integrity (INAI)) to complement existing provisions and to allow organisations to implement self-regulations.

© Law Business Research 2021

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

Not applicable.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

There are several standards of computer security, starting with the group of standards ISO/IEC 27000 [7], which integrate an information security management system that is focused on the security of information under an explicit administrative control of it.

ISO 15408 [8] is a standard developed in what is known as the Common Criteria and allows many different software applications to be integrated and tested in a secure manner.

RFC 2196 [9] is a memo published by the Internet Engineering Task Force for the development of security policies and procedures for information systems connected to the internet. It provides a broad and general vision of information security, including network security, incident response and security policies. The document is very practical and focused on day-to-day operations.

For the industrial field, in 2007, with the working group of the International Society for Automation (ISA), the ISA-99 standard, called Security for Industrial Automation and Control Systems, was started with the publication of ANSI/ISA-99.00.01-2007 Security for Industrial Automation and Control Systems: Concepts, Terminology and Models, in conjunction with the technical report ANSI/ISA-TR99.00.01-2007 Security Technologies for Manufacturing and Control Systems. At the beginning of 2009, with ANSI/ISA-99.02.01-2009 Security for Industrial Automation and Control Systems, the American National Standards Institute approved the establishment of an industrial automation and control systems security programme. Finally, in 2010, it was changed to the ISA/IEC 62443 standard to align the numbering of the standard documentation with the corresponding standards of the International Electrotechnical Commission (IEC).

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

There are specific guidelines issued by governmental authorities that are intended to address best practices on cybersecurity. The following are the most frequently used.

- Guidelines for the secure deletion of personal data.
- Guidelines to prevent identity theft.
- Guidelines of the Mexican Internet Association.
- Cybersecurity Strategy for Financial Institutions.
- ICC Cybersecurity Guide for Business.

Information sharing

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

Not applicable.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

On 12 June 2018, the Mexican Official Gazette published that Mexico has adopted the Council of Europe Convention 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and cross-border data flows. Both are binding international instruments that protect the individual against any abuse of the collection and processing of personal data, and at the same time they seek to regulate the cross-border flow of personal data.

Insurance

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

Yes, insurance for cybersecurity breaches is available and is becoming more common.

ENFORCEMENT

Regulation

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The applicable laws empower the following authorities to investigate an incident:

- the General Attorney Office;
- Public Prosecutors;
- the Network for Integrity (INAI); and
- the Federal Telecommunications Institute (IFT).

Public Prosecutors in Mexico are in charge of investigating cyber activities and of resolving them. A cyber police unit has been created to follow up on crimes or unlawful activities committed through the internet. Complaints directed to the cyber police unit can be submitted via its website, by phone or through a Twitter or email account. In addition, the Federal Police has created a scientific division called the National Centre For Cyber-Incidents Response, specialising in providing assistance to the victims or claimants of cyber threats and cyberattacks. In the case of data protection, the federal regulator on data privacy matters (INAI) may conduct investigations to follow up personal data matters. Regarding telecommunications, the federal regulator (IFT) is in charge of this sector.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

See above.

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

The most common enforcement actions brought by authorities relate to the breach of systems aimed at obtaining personal data (either sensitive or financial data) for profit. The private sector has been cooperative when the breach is caused by hackers; however, there are cases where the authorities have imposed fines on the private sector (which includes the financial, health and gaming sectors) because of breaches that have occurred as a result of not having the proper security measures in place.

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

There is no regulatory obligation to notify authorities after a cybersecurity breach; however, if the security breach compromised personal data of identifiable individuals, then the business (understood as data

© Law Business Research 2021

controller) must evaluate the breach through a risk assessment, implement the corrective, preventive and improvement actions to reinforce security measures, and determine if the event may result in prejudice to the property or non-pecuniary rights of the data subjects, if so, it should notify the affected parties. Under the Mexican Privacy Law (Federal Law on the Protection of Personal Data held by Private Parties), security breaches occurring at any stage of processing personal data must be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights. There is no official format to notify breaches; however, the Mexican Privacy Law and its regulations provide that the notification must include, at least, the nature of the breach, the personal data compromised, corrective actions implemented immediately by the data controller, recommendations concerning measures for the data owner to protect its interests after the breach and the means available for the data owner to obtain more information on the breach.

Penalties

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

- Hacking (ie, 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 given a prison sentence of six months to two years, by the relevant authority, as well as a fine of approximately 8,004 to 24,012 pesos. The aforementioned penalty could be doubled 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 or she handles information through deceit, takes advantage of errors or misleads a person with the intent of obtaining a financial gain. In such case, the relevant authority shall impose a prison sentence of three days to 12 years, as well as a fine of approximately 2,400 to 24,012 pesos, 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. If the criminal offence is committed against the state, the relevant authority shall impose a prison sentence of one year to four years, as well as a fine of approximately 16,000 to 48,024 pesos.
- Possession or use of hardware, software or other tools used to commit cybercrime (eg, hacking tools): the Federal Criminal Code provides this criminal offence as hacking, which is described above.
- Identity theft or identity fraud (eg, 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 or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be given a prison sentence of three to nine years, by the relevant authority, as well as a fine of approximately 2,401,200 to 24,012,000 pesos.
- Electronic theft (eg, 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 or, in general, any other payment instrument, including electronic devices, issued by credit institutions without authorisation of the holder, shall be given a prison sentence of three to nine years, as well as a fine of approximately 2,401,200 to 24,012,000 pesos. The aforementioned penalties could be doubled if any counsellor, official, employee or service provider of any credit institution commits the criminal offence.
- In addition, under the Federal Law for the Protection of Industrial Property, the theft of trade secrets – either by electronic means or not – by current or former employees constitutes a crime and triggers imprisonment and fines to the responsible parties.
- Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime: the Federal Criminal Code contains a specific criminal offence in this regard, providing that those who manufacture, import, distribute, rent or in any way market devices, products or components intended to circumvent an effective technological measure would be subject to imprisonment from six months to six years and a fine.
- Possession or use of hardware, software or other tools used to commit cybercrime: the Federal Criminal Code provides that those who, knowingly, without authorisation and for profit, suppress or alter, by themselves or through another, any information on rights management, will be imprisoned from six months to six years and liable to pay a fine. The same penalty will be imposed on whoever, for profit:
  - distributes or imports for distribution information on rights management, knowing that it has been suppressed or altered without authorisation; or
  - distributes, imports for distribution, transmits, communicates or makes available to the public copies of works, performances or phonograms, knowing that the information on rights management has been suppressed or altered without authorisation.
- Unsolicited penetration testing (ie, the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points): the Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour may fall into the scope of hacking. The aforementioned penalties are applicable in this case. If the criminal offence is committed against the state, the relevant authority shall impose a prison sentence of one year to four years, as well as a fine.

In addition, activities such as 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.

Also, 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 given a prison sentence of six months to four years, by the relevant authority, as well as a fine of approximately 8,004 to 24,012 pesos. Moreover, an unauthorised person who knows or copies information from credit institutions' computer systems or equipment protected by a security mechanism shall be subject to a prison sentence of three months to two years, as well as a fine of approximately 4,002 to 24,012 pesos. All the aforementioned penalties could be doubled if any counsellor, official, employee or service provider of any credit institution commits the criminal offence.

On the other hand, it should be considered that under the Mexican Privacy Law (Federal Law on the Protection of Personal Data held by Private Parties), authorising to process personal data for profit, causing a security breach and affecting databases constitutes a criminal offence

© Law Business Research 2021

and the data controller would be liable if these actions occur with databases under his or her custody. The individual responsible will be subject to imprisonment for between three months and three years, which may be doubled if the personal data compromised includes sensitive information.

25 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

See above.

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

According to article 32 V of the Federal Criminal Code, organisations and companies are civilly liable for the damage 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 who illegally causes harm to another person shall be obliged to repair the damage, unless he or she proves that the damage was produced because of the victim's guilt or negligence.

THREAT DETECTION AND REPORTING

Policies and procedures

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

To be prepared for a security incident and to improve security measures within a company, Mexican regulations provide for certain obligations of data controllers, such as:

- prepare an inventory of personal data and processing systems;
- determine the duties and obligations of those who process personal data;
- make a risk analysis of personal data identifying, by level, dangers and estimated risks;
- establish security measures and identify those effectively implemented so far;
- analyse the gap between existing security measures and those missing but necessary for the protection of personal data;
- prepare and update a work plan for the implementation of the missing security measures arising from the gap analysis;
- train personnel; and
- keep a record of personal data storage media.

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

When it comes to records containing personal data, organisations should keep records in accordance with the Federal Law on the Protection of Personal Data held by Private Parties (the Mexican Privacy Law) for as long as the investigation requires. Particular attention should be given to sensitive personal data as its storage and processing could pose a risk for organisations that do not adopt the applicable provisions of the Mexican Privacy Law.

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

Under the Mexican Constitution, organisations must cooperate with government agencies regarding incidents; however, no law establishes specific requirements to report incidents or potential incidents.

Time frames

30 What is the timeline for reporting to the authorities?

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 and, consequently, there is no timeline for reporting either.

Reporting

31 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Rules for reporting threats of breaches that may involve the unauthorised use of personal data are contained in the Mexican Privacy Regulations. These Regulations provide that the data controller must inform only the data subject, not the federal regulator or other authority. As per the timeline, the regulations only provide that this notification should be conducted without delay, and after assessing whether the breach significantly affects the property or non-pecuniary rights of the data subjects upon having conducted an exhaustive review of the magnitude of the breach, so that the prejudiced data subjects may take appropriate measures. Notices of breaches should contain at least the following information, as mentioned in the Mexican Privacy Regulations:

- the nature of the breach;
- the personal data compromised;
- recommendations to the data subject concerning measures that the latter can adopt to protect his or her interests;
- corrective actions implemented immediately; and
- the means by which he or she may obtain more information in this regard.

UPDATE AND TRENDS

Update and trends

32 What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Currently, the Federal Criminal Code provides for crimes related to IT systems protected by security measures. However, it has failures that range from the absence of a specific definition for the terms 'security systems' and 'cybercrime' (the latter only defined in the National Cybersecurity Strategy, of which the provisions are non-binding until they are elevated to law), to cyberbullying or malware not being treated as a crime. According to the Sector Plan of Security and Citizen's Protection 2020–2024, in the last six years there have been more than 260,000 download incidents, and 68,000 reports of citizens trying to download, from 26,000 websites used for illegal activities. This data collection has been achieved with the collaboration of international authorities in at least 4,500 cases.

Among the most common challenges in developing an effective set of cybersecurity regulations in Mexico are the following:

© Law Business Research 2021

- Insufficient storage, processing and transmission capacity of the information produced by security institutions, which requires the application of new technologies to expand these capacities. Likewise, the lack of inter-institutional agreements to expand coverage, diversify services and take advantage of new technologies.
- The information systems and databases of security institutions are not approved, so their interoperability is not feasible, especially when they require the sharing and exchange of information and intelligence products.
- The national broadcasting network is neither approved, nor aligned in terms of technology with the security institutions of the three levels of government, which is why it is not possible to establish efficient communication between them.
- Permanent training is required for the technical personnel of the security institutions, with the intention of providing the maintenance and attention that the services require for the efficient use of the technological infrastructure, which guarantees the availability and timeliness of the services.
- The need for constant technological updates requires more efficient information security management systems that incorporate cybersecurity strategies for the prevention and detection of, and response to, incidents such as cyberattacks in security institutions. In this sense, it is necessary to strengthen security in order to avoid logical and physical vulnerabilities in the technological platforms of security institutions, as well as to expand inter-institutional collaboration agreements to strengthen information security mechanisms.

Coronavirus

33 What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programmes, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

There is no emergency legislation, nor are there relief programmes or other initiatives, specific to cybersecurity that the Mexican state has implemented to address the pandemic. As regards best practices, below are our recommendations:

- evaluate the current portfolio and security measures to assess what would be the main risk in terms of data processing during the emergency, and reinforce internal policies accordingly (ie, revise internal policies for employees such as those allowing them to use their own devices for processing and storing data pertaining to their employment – 'bring your own device policies');
- prioritise compliance with data protection law when accelerating the move of business systems to the cloud; and
- implement technology to address and anticipate technological issues that may arise when adjusting security models to fit the company's needs.

CREEL GARCÍA-CUÉLLAR AIZA Y ENRÍQUEZ

Begoña Cancino
begona.cancino@creel.mx

Torre Virreyes, Pedregal 24, Piso 24
Col Molino del Rey
Mexico City, CP 11040
Mexico
Tel: +52 55 4748 0600
www.creel.mx

© Law Business Research 2021

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-643-3

© Law Business Research 2021