The Guide to Managing a Corporate Crisis

Third Edition

Editors
Sergio J Galvis, Robert J Giuffra Jr and Werner F Ahlers

The Guide to Managing a Corporate Crisis

Third Edition

Editors
Sergio J Galvis, Robert J Giuffra Jr and Werner F Ahlers

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2020
For further information please contact Natalie.Clarke@lbresearch.com

LATIN LAWYER

Publisher
Clare Bolton

Business Development Manager
Jack Levy

Associate Publisher
Rosie Cresswell

Editorial Assistant
Tommy Lawson

Production Operations Director
Adam Myers

Production Editor
Helen Smith

Subeditor
Robbie Kelly

Chief Executive Officer
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 3435 Farringdon Street, London, EC4A 4HL, UK

www.latinlawyer.com

ISBN 978-1-83862-429-3

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following law firms, advisory firms and corporations for their learned assistance throughout the preparation of this book:

Anheuser-Busch InBev

The Arkin Group LLC

Chevez Ruiz Zamarripa

Cleary Gottlieb Steen & Hamilton LLP

Creel, García-Cuéllar, Aiza y Enriquez

Debevoise & Plimpton LLP

Dechert LLP

D'Empaire

Galicia Abogados

Finsbury

McLarty Associates

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

Mitrani, Caballero & Ruiz Moreno

Morrison & Foerster LLP

Payet, Rey, Cauvi, Pérez Abogados

Pinheiro Neto Advogados

Posse Herrera Ruiz

Rodrigo, Elías & Medrano Abogados

Sullivan & Cromwell LLP

Publisher's Note

Latin Lawyer is delighted to publish *The Guide to Managing a Corporate Crisis*.

Edited by Sergio J Galvis, Robert J Giuffra Jr and Werner F Ahlers of Sullivan & Cromwell LLP, and containing the knowledge and experience of 50 leading practitioners from a variety of disciplines, it provides guidance that will benefit all practitioners when an unexpected crisis hits.

Corruption investigations, expropriation, industrial accidents, pandemics: corporate crises take many forms, but each can be equally dangerous for companies in Latin America. Covering the impact of political instability, the role of communications in crisis response, approaches to bribery investigations and game plans in response to financial stress, this book is designed to assist key corporate decision-makers and their advisers in effectively planning for and managing corporate crises in the region.

We are delighted to have worked with so many leading firms and individuals to produce *The Guide to Managing a Corporate Crisis*. If you find it useful, you may also like the other books in the Latin Lawyer series, including our *Guide to Corporate Compliance, and Regulators*, our online tool that provides an overview of the major regulators in Latin America.

My thanks to the editors for their vision and energy in pursuing this project and to my colleagues in production for achieving such a polished work.

Contents

Part III

Stakeholder Relations

11

Data Privacy and Cybersecurity: Crisis Avoidance and Management Strategies

Jeremy Feigelson, Andrew M Levine, Christopher Ford, Anna R Gressel, Stephanie Cipolla and Hilary Davidson[1]

While much of the world has changed in 2020, lawmakers' and regulators' focus on data privacy and cybersecurity has not. Tough new laws and regulations have been enacted, or taken effect, across the globe. In Latin America, the Brazilian General Data Protection Law (LGPD)[2] recently became operative after a number of delays, though penalties and sanctions for noncompliance will not be enforced until August 2021. The new Panamanian Law No. 81, which will take effect in 2021, and draft legislation in Argentina, Bolivia and Chile also are powerful examples of this trend.

Even as they contend with new challenges from remote workforces and the pressures of maintaining business as usual during the challenging conditions of the covid-19 pandemic, companies face increasingly stringent legal obligations to carefully handle corporate data. With regard to personal data, companies must comply with privacy protections in a broad range of areas such as initial data collection; daily data usage in the ordinary course; the transfer of personal data to vendors, acquirers or other third parties; and the sending of personal data to other countries.

These data privacy requirements go hand in hand with escalating requirements on data security. Under the laws of many jurisdictions, corporate cybersecurity programmes must now be at a certain level of substantive adequacy – often defined as 'reasonable' or 'appropriate' security. These mandates generally apply both to personal data and to other important corporate data, such as intellectual property and financial information. Companies are also increasingly required to disclose breaches of data security to regulators, affected individuals, counterparties and others.

---

1 Jeremy Feigelson and Andrew M Levine are partners, and Christopher Ford, Anna R Gressel, Stephanie Cipolla and Hilary Davidson are associates at Debevoise & Plimpton LLP.

2 Lei Geral de Proteção de Dados (Law No. 13,709/2018). English translation available at https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf.

As the way business is conducted changes in response to the covid-19 pandemic, the cyber risks companies face – and what would be considered reasonable security to protect against those risks – are also evolving. For example, what was reasonable when many sensitive meetings were face-to-face may not be reasonable now that almost all communication is remote. Companies' increasing reliance on work-from-home technology also creates new opportunities for hackers, who have found remote workers often make easier targets for phishing.

Importantly, data privacy and cybersecurity are not just legal issues. They are crucial to the trust between a company and its customers and other stakeholders. People want to know that the companies they do business with, work for or invest in will handle data with care. Missteps in privacy and cybersecurity, therefore, can create a crisis with the potential to cut deeply into a company's reputation and balance sheet.

A prominent example of the long-lasting impacts of a breach is Equifax, one of the leading credit reporting agencies. In 2017, when Equifax disclosed a data breach affecting the personal data of nearly 150 million Americans, *USA Today* reported on the incident under the headline, 'Equifax image is battered by data breach as consumers feel violated'. Years later, the financial cost of the breach has continued to climb, and Equifax has spent nearly US$2 billion to resolve dozens of government investigations and private lawsuits.

We discuss below some of the key legal requirements that apply around the globe, starting with a focus on Latin America, and strategies for reducing legal and reputational risks related to data management. Because the applicability of many data protection laws depends on where the data subject lives and not necessarily where the company collecting or using the data is located, a broad understanding of global laws is valuable. Many best practices can help mitigate the risks that may materialise into a crisis, but the bottom line is simple: prepare, prepare, prepare. Bad data events do happen to good companies. It is best to assume that such bad events, in time, will happen to yours. Companies are thus well advised to be ready to respond vigorously and transparently, with a focus on maintaining that all-important trust.

Latin America

Argentina

Key privacy and cybersecurity laws

Argentina enacted the Personal Data Protection Law Number 25,326 (PDPL) in October 2000.[3] Since 2003, Argentina has been recognised by the European Commission as a jurisdiction providing an adequate level of data protection.[4]

In May 2019, the Agency of Access to Public Information issued Resolution 4/2019 setting out guidelines for the interpretation and application of data protection law in Argentina. The resolution provides guidance on consent (including consent of minors), automated data processing, data dissociation, right of access to personal data collected through surveillance

3 English translation available at www.ics.uci.edu/~kobsa/privacy/argentine-privacy.htm.

4 European Commission Decision C (2003) 1731 of 30 June 2003.

and biometric data.[5] Prior to the 2019 presidential election, the Agency of Access to Public Information also issued guidance, by way of Resolution 86/2019, to confirm that political opinions are considered sensitive personal information.[6]

Key obligations of companies

Companies processing personal data must register their database or other data storage system with the Argentine Personal Data Protection Agency.[7] Personal data cannot be processed beyond the purpose for which it was collected.[8] Companies are obligated to ensure the accuracy of the personal data they process.[9] Prior to processing personal data, companies must provide notice to and obtain consent from data subjects.[10] The PDPL also requires companies to enact measures to guarantee the security and confidentiality of personal data that they hold and process.[11]

Key rights of data subjects

Data subjects in Argentina have the right to request information from data controllers and receive access to certain of their personal information.[12] Data subjects can also request the correction, modification or suppression of personal information stored by data controllers.[13]

Breach notification

There is not currently a breach notification obligation in Argentina.

Cross-border transfers

Transfer of personal data requires the consent of the data subject and is prohibited unless the receiving country provides an adequate level of protection.[14] In 2018, the Agency of Access to Public Information promulgated Provision 159/2018, the Guidelines and Basic Contents of Binding Corporate Rules for International Data Transfers. Similar to the use of such rules for data transfers out of the European Union, a company's adoption of these model rules allows for the transfer of personal data from Argentina to a country that Argentina deems not to have an adequate level of protection.

5 Agencia de accesso a la informacion publica (Resolución 4/2019) http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318874/norma.htm.

6 Agencia de accesso a la informacion publica (Resolución 86/2019) http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/323901/norma.htm.

7 Chapter IV, Article 21.

8 Chapter II, Article 4.

9 Chapter II, Article 4.

10 Chapter II, Article 5.

11 Chapter II, Article 9.

12 Chapter III, Articles 13-14.

13 Chapter III, Article 16.

14 Chapter II, Article 12.

Brazil

Privacy and cybersecurity

In July 2019, Brazil amended its new data protection law, the LGPD, which was originally passed in August 2018. After several delays, the LGPD was expected to come into effect in August 2021. But in a surprise move on 27 August 2020, the Brazilian Senate officially declined to further postpone the law, meaning that the main provisions of the LGPD took effect on 18 September 2020, when the Brazilian President signed Conversion Bill 34/2020.

The LGPD was inspired by the European Union's General Data Protection Regulation (GDPR). The GDPR increasingly serves as a global model for data protection legislation. While the LGPD is not as extensive as the GDPR, it shares many similarities. The LGPD applies to all processing of personal data by private entities if the data is collected or processed in Brazil, or if the processing is for the purpose of offering or providing goods or services in Brazil. As amended, the law created the National Data Protection Authority (ANPD), which will be responsible for overseeing personal data protection compliance and implementing and enforcing sanctions.[15] On 26 August 2020, the President published Decree No. 10,464,[16] which will establish the ANPD once its executive director is appointed.

While the main provisions of the LGPD took effect on 18 September 2020, administrative sanctions under the LGPD are still subject to Law No. 14,010/20, which postpones sanctions until August 2021. Nevertheless, now that the main provisions are in force, there is a possibility of private lawsuits and public prosecutor actions. Companies operating in Brazil or that collect personal data from Brazilian data subjects therefore should review their compliance with the LGPD, including by reviewing privacy policies, implementing security measures, updating procedures, including breach notifications, and identifying agreements that involve cross-border transfers from Brazil. Brazilian regulators appear to be wasting no time in beginning to make use of this civil litigation authorisation, announcing the first civil action against a Brazilian company for alleged LGPD violations only four days after the law went into effect.[17]

Key obligations of companies

The LGPD establishes 10 principles applicable to all data processing in Brazil, key among them that all processing must be 'for legitimate, specific and explicit purposes of which the data subject is informed'.[18] Other key principles include limiting processing to the minimum necessary, free access and transparency to data subjects, and an obligation to ensure accuracy of data. Companies are also required to establish security measures to protect personal data and to appoint a data protection officer.

15 Law No 13.853/2019 (available at www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm).

16 Decree No. 10,464 (www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226).

17 MPDFT ajuíza 1ª ação civil pública com base na LGPD, 22 September 2020, www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/12384-mpdft-ajuiza-1-acao-civil-publica-com-base-na-lgpd.

18 LGPD Article 6.

Key rights of data subjects

The new law vests the data subject with the ownership rights to the subject's personal data,[19] and grants the subject the right to obtain access to and correction of personal data[20] and to revoke consent to process his or her personal data.[21]

Breach notification

The LGPD creates a data breach notification obligation.[22] Companies must notify both the Brazilian authorities and data subjects of any 'security incident that may create risk or relevant damage to the data subjects'. This notification must be completed within a reasonable period and contain a description of the incident, the information involved, the measures taken to protect the data, the risks related to the incident and measures taken to mitigate the effects.

Cross-border transfers

The LGPD prohibits the cross-border transfer of personal data unless such transfer falls within a limited number of enumerated exceptions.[23] Exceptions include where the receiving country or organisation provides a level of data protection comparable to the LGPD or the data subject has provided specific consent for the transfer 'distinct from other purposes'.

Chile

Key privacy and cybersecurity laws

Data privacy and cybersecurity in Chile is regulated through the Law for the Protection of Private Life (PDPL) 1999.[24]

Key obligations of companies

Companies are required to provide notice to and receive consent from data subjects prior to the processing of their personal information, unless otherwise permitted by law.[25] Personal data can only be used for the purpose for which it was collected.[26]

Key rights of data subjects

Data subjects have the right to object to a company's use of his or her personal data.[27] Data subjects also have the right to request modification and deletion.

19 LGPD Article 17.
20 LGPD Article 18.
21 LGPD Article 8.
22 LGPD Article 48.
23 LGPD Article 33.
24 Act No. 19-628, available in Spanish at www.leychile.cl/Navegar?idNorma=141599.
25 PDPL Article 4.
26 PDPL Article 9.
27 PDPL Article 3.

Breach notification

There is not currently a general breach notification obligation in Chile. Financial institutions regulated by the Superintendence of Banks and Financial Institutions (SBIF) do have regulatory obligations – updated as recently as August 2018 – that require reporting any incident that affects business continuity, the entity's funds or other resources, the quality of the entity's services, or the image of the entity. The SBIF has stated that it expects these reports to be made within 30 minutes – an extraordinarily short window during a high-pressure situation.

Under certain circumstances, where an incident affects the continuity of client services or the security of clients' personal data, the affected institution may also be required to report the incident to its clients. Client notifications must be made in a timely manner; there is no fixed deadline.

Cross-border transfers

There are no regulations on the transfer of data within Chile or across borders.

Colombia

Key privacy and cybersecurity laws

Colombia enacted Statutory Law No. 1581, which regulates data privacy and security, in 2012.[28] The law applies to personal data processed in Colombia or where a foreign processor is subject to Colombian legislation.[29] The law establishes eight principles for interpretation and application:

- legality of data processing;
- legitimate purpose for processing;
- freedom for data subjects to control their personal data;
- accuracy of data;
- transparency in processing;
- limitation of access to those with authorisation;
- security of personal data; and
- confidentiality of personal data.[30]

The Ministry of Trade, Industry and Tourism has enacted regulations pursuant to the law.[31]

Key obligations of companies

Companies must provide notice to and obtain consent from the data subject prior to or simultaneously with the collection of his or her personal data, except where the data is publicly

28 Ley Estatutaria 1581 de 2012, available in Spanish at https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

29 Law Title I, Article 2.

30 Law Title II, Article 4.

31 Decree No. 1377/2013. English translation available at https://iapp.org/media/pdf/knowledge_center/DECRETO_1377_DEL_27_DE_JUNIO_DE_2013_ENG.pdf.

accessible.[32] Before processing, companies must develop privacy policies available to data subjects, which must inform data subjects of their rights under the law.[33] At the request of the Superintendence of Industry and Trade, companies must be able to demonstrate that they have implemented appropriate and effective measures to comply with the law.[34]

Key rights of data subjects

Data subjects have the right to access at no charge from data controllers.[35] Data subjects also have the right to request updating, rectification or suppression of personal data held by companies to ensure accuracy of the data.[36]

Breach notification

There is no obligation to notify data subjects of a breach in Colombia, but data owners and processors must notify the Data Protection Authority of security violations where there is a risk to the administration of data subjects' information.[37]

Cross-border transfers

Transfer of personal data to other jurisdictions generally is prohibited where the receiving jurisdiction does not provide an adequate level of protection. Transfer can nonetheless be made where the data subject has provided his or her express consent.[38] Further, consent is not required for the transfer of personal data from a data controller to an overseas data processor, where there is a contract in place that complies with Article 25 of Decree 1377.[39]

Mexico

Key privacy and cybersecurity laws

Mexico enacted the Federal Law on the Protection of Personal Data Held by Private Parties in 2010.[40] The government has also issued regulations pursuant to the law, which came into effect in 2011; privacy notice guidelines, which came into effect in 2013; and parameters for self-regulation, which came into effect in 2014. The law applies to all data processing in Mexico, including when processing is done outside of Mexico on behalf of a Mexican data processor.

32 Decree Chapter II, Article 5.

33 Decree Chapter III, Articles 13-15.

34 Decree Chapter III, Article 26.

35 Decree Chapter IV, Article 21.

36 Decree Chapter IV, Article 22.

37 Law Title VI, Articles 17(n) and 18(k).

38 Law Title VIII, Article 26.

39 Decree Article 25.

40 Text in Spanish: www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

Key obligations of companies

Mexican law requires that all personal data must be collected and processed fairly and lawfully.[41] Further, personal data must be collected only for specified, explicit and legitimate purposes, and the amount of data collected may not be excessive relative to the purposes for which it was collected.[42] Companies must take reasonable steps to ensure that the personal data in their databases is accurate and kept only for the time necessary to effectuate the legitimate purpose for which the data was collected.[43] Companies must also appoint a personal data officer or department[44] and establish risk-based security measures at least as robust as those used to protect the company's own data.[45]

Key rights of data subjects

Individuals in Mexico have the right to access and correct personal data, oppose the processing of personal data[46] and revoke consent to the processing of personal information.[47] Individuals also retain the right to be notified prior to consenting to the processing of personal data.[48]

Breach notification

Mexico requires breach notification to affected data subjects where the incident materially affects the property or individual rights of a subject.[49] The notification must include information regarding the nature of the breach, the personal data compromised, recommendations to the data subject to protect his or her interest, corrective actions implemented by the company and a method for data subjects to obtain further information.[50]

Cross-border transfers

Consent is generally required to transfer personal data across borders, and privacy notices in Mexico must inform data subjects when companies intend such a transfer. The transfer cannot exceed the scope of the disclosure in the privacy notice, and the receiving company must follow Mexican data privacy law.[51]

41 Law Chapter II, Article 11.
42 Law Chapter II, Article 13.
43 Law Chapter II, Article 11.
44 Law Chapter IV, Article 30.
45 Law Chapter II, Article 19.
46 Chapter III, Articles 22-27.
47 Chapter II, Article 8.
48 Regulations Chapter II, Articles 12-14.
49 Chapter II, Article 20.
50 Regulations Chapter II, Article 65.
51 Chapter V, Article 36.

Peru

Key privacy and cybersecurity laws

Data privacy and cybersecurity in Peru are regulated by the Law on the Protection of Personal Data (DPL), which was enacted in 2011.[52] Additionally, the Peruvian government issued the Security Policy on Information Managed by Databanks of Personal Data in 2013.

Key obligations of companies

Companies may only collect personal data by legal methods,[53] and they only can collect and process personal data with consent from and notice to data subjects for collection and processing.[54] Data processing must be both proportional and non-excessive to the legitimate purpose of collection.[55] Companies must work to ensure the accuracy of data collected and processed,[56] and implement necessary security measures to protect personal data.[57] All personal data must be given an adequate level of protection.[58]

Key rights of data subjects

The rights granted to data subjects under the DPL include the right of access to a data subject's personal data,[59] the right to be informed of the purpose of collection and how the personal data will be processed,[60] the right to request the correction of personal data,[61] the right to oppose the processing of personal data[62] and the right to refuse providing personal data.[63] The DPL also grants data subjects the ability to pursue legal claims against companies that violate their data privacy rights.[64]

Breach notification

Companies must provide notification to data subjects of 'any incident that significantly affects their property or their moral rights'. Such notification must include a description of the incident, the personal data affected, information for the data subject on how to mitigate the potential damage and the remediation steps taken by the company.[65] The breach notification obligation was echoed in January 2020 through Emergency Decree No. 007-2020, which confirmed that public and private entities acting as digital service providers must

52 Available in Spanish at https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf.
53 DPL Articles 4, 6.
54 DPL Articles 5, 18.
55 DPL Article 7.
56 DPL Article 8.
57 DPL Article 9.
58 DPL Article 11.
59 DPL Article 19.
60 DPL Article 18.
61 DPL Article 20.
62 DPL Article 22.
63 DPL Article 21.
64 DPL Article 10.
65 Security Policy on Information Managed by Databanks of Personal Data, Section 2.3.4.2.

report to the data protection authorities when a digital security incident involving personal data occurs.[66]

Cross-border transfers

The transfer of personal data outside of Peru is generally allowed as long as the destination country provides adequate data protection measures. If the destination country does not provide adequate protection, transfer may still occur where the receiving party agrees to comply with the DPL, where the transfer is necessary pursuant to a contractual relationship with the data subject, or with the data subject's informed and express consent.

Panama

Key privacy and cybersecurity laws

In March 2019, Panama enacted Law No. 81, which will take effect in March 2021.[67] The general principle of personal data protection is enshrined in Articles 29, 42, 43 and 44 of Panama's Constitution.[68] This summary sets out the requirements to comply with Law No. 81.

Key obligations of companies

Companies must obtain consent from the data subject, who must be informed of the proposed use. Consent must be recorded in a clear and easily accessible manner so that it may be traced back to the data subject. Companies may store data in a secure database for a maximum of seven years.

Key rights of data subjects

Information may be collected only with the prior consent of the data subject. There are limited exceptions where companies may process an individual's data without their consent, including where necessary for a commercial relationship, for medical emergencies, for statistical or scientific purposes or where there is a legitimate interest pursued by the data controller. Data subjects have an ongoing right to access, modify, change or remove their personal information.

Breach notification

In the event of a data breach, companies must inform data subjects. There is no requirement for companies to register with the National Authority for Transparency and Access to Information (ANTAI), but any notification of a breach to data subjects should also be reported to ANTAI.

66 Emergency Decree No. 007-2020 (https://busquedas.elperuano.pe/normaslegales/decreto-de-urgencia-que-aprueba-el-marco-de-confianza-digita-decreto-de-urgencia-n-007-2020-1844001-2/).

67 Law No, 81 (www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf).

68 Panama's Constitution is available in Spanish here (www.antai.gob.pa/wp-content/uploads/2015/04/constituciondepanama.pdf).

Cross-border transfers

Cross-border transfers are permitted where the receiving country has comparable data protection standards to Panama and the transferring company takes all necessary steps to protect the personal data being transferred. There are a few exemptions to this: (1) where the data subject provides consent to the transfer; (2) where the transfer is required for the performance of a contract; (3) for banking or stock exchange transfers; and (4) as required by law in compliance with Panama's international treaty obligations.

Uruguay

Key privacy and cybersecurity laws

Uruguay began modernising its existing data protection legislation[69] with the approval of Law No. 19,670[70] in October 2018 and with Decree 64/2020 in February 2020.[71]

Key obligations of companies

All companies holding databases of personal information in Uruguay must register with the Uruguayan data protection authority and record:

- the categories of data;
- how the data is collected and processed;
- details of the data controller;
- the storage location;
- retention period;
- security measures;
- codes of conduct;
- International data transfers; and
- how rights to access, update and delete persona data can be exercised.

If a company processes data outside of Uruguay, the database must still be registered with the authorities where processing activities are offered in connection with goods or services targeting Uruguay or where required by contract or international law. The register should be updated every three months. Private companies that process data on a large scale (i.e., the data of 35,000 or more individuals) must appoint a data protection officer to monitor compliance.

Key rights of data subjects

Data subjects have the tight to access their own personal data and the right to rectify any inaccurate records, update and delete their data. Companies must correct, update or delete personal data on request and without charge.

69 Law No. 18.331 and Decree No. 414/009.

70 https://legislativo.parlamento.gub.uy/htmlstat/pl/leyes/Ley19670.pdf.

71 www.impo.com.uy/bases/decretos/64-2020.

Breach notification

Decree 64/2020 introduces a mandatory breach notification to the Uruguayan data protection authority within 72 hours of becoming aware of a security breach.

Cross-border transfers

International transfers of personal data are permitted where the receiving country provides an adequate level of data protection.

Bolivia

Bolivia does not currently have a specific data protection law, though there is a general right to privacy in the country's constitution. There are currently two draft data protection laws pending consideration by the Legislative Assembly that, if passed, will apply to all individuals or legal entities processing data in Bolivia.[72] The draft laws would require companies to appoint a data protection officer if the organisation carries out regular data processing. The draft laws also may require express, written consent of the data subject and that organisations to implement security measures to protect personal data, maintain its confidentiality, and allow the Agency for the Protection of Personal Data (APP) to inspect and verify data records. If the draft laws are passed, data controllers will be permitted to transfer personal data internationally where the receiving country has adequate data protection laws as required by the APP, the exporter offers sufficient guarantees that the personal data will be safeguarded, the parties have sufficient clauses in their contracts (as validated by the APP) to protect data, or where specifically authorised by the APP.

Global developments

China

China continues to be one of the most active countries in expanding data privacy and cybersecurity regulation, building on past years' efforts.

China's new E-Commerce Law came into effect on 1 January 2019. The law requires registration by e-commerce vendors operating in China. It further reiterates e-commerce operators' obligation to comply with Chinese personal data protection regulations, including providing customers with procedures allowing them to correct, erase or enquire about their personal data.

The Chinese Cybersecurity Law, which was enacted in 2017, imposes substantive requirements on 'network operators' as well as 'providers of network products and services' to ensure that they are securing their data, and have adopted appropriate incident-response plans and contingency measures in the event of a data security incident. Moreover, the Cybersecurity Law places enhanced obligations on operators of 'critical information infrastructures', including data localisation and submission to a state security review prior to the procurement of network products and services. Since the enactment of the Cybersecurity

72 http://www.diputados.bo/leyes/pl-n%C2%B0-1852019-2020; http://misdatos.internetbolivia.org/docs/anteproyecto_ley_de_proteccion_datos_personales_InternetBolivia.pdf.

Law, the Chinese government published many draft guidelines to assist companies in compliance with the law.

In March 2020, the National Information Security Standardisation Technical Committee released an amendment to the current Personal Information Security Specification (the Specification), which came into force on 1 October 2020. The Specification is a set of voluntary best practices for businesses operating in China. The Specification is intended to set a baseline reference for regulatory bodies in China to use when evaluating how companies protect personal information. The Specification emphasises that a data subject's consent is required to collect, transfer, share and disclose data and that the data should not be retained beyond the minimum necessary period. Additionally, the Specification specifies a data subject's rights to his or her data, which are similar to the global standards (e.g., rights to access, delete or rectify data). The Specification also suggests substantive best practices for organisations, including incident-response planning (e.g., mock incident exercises), and preparations for notifying individuals in the event of a data breach. The Specification adds specific requirements for biometric data, such as facial recognition.

The 2019 Draft Security Assessment Measures for the Export of Personal Data (the 2019 Draft Measures) published by the Cyberspace Administration of China for comment apply to cross-border transfers of personal data from China. The measures extend the requirement for data localisation from critical information infrastructure operators to all network operators, and require network operators to pass on certain data protection obligations to their recipients through contracts and other binding agreements and to retain records of data transfers for five years. At present, the Cybersecurity Law does not require an overseas operator to designate local representatives to address concerns from the authorities or data subjects. If enacted, the 2019 Draft Measures could introduce an obligation on overseas institutions that collect personal information from domestic users in the course of their business activities to appoint representatives to fulfil their legal and compliance responsibilities within China.[73]

On 13 April 2020, the Cyberspace Administration of China, together with 11 other Chinese government agencies, published the Measures for the Review of Cybersecurity, detailing the procedures of operators of critical information infrastructures under the Cybersecurity Law in relation to the procurement of certain network products and services, if such procurement may affect state security. Pursuant to the Measures, operators of critical information infrastructures need to actively submit a security review, if they determine that their procurement may have state security risks. The review process may take 55-120 business days.[74]

In July 2020, the Standing Committee of the National People's Congress of China released the draft Data Security Law for public comment. The focus of the new law is to protect data that, if leaked, may directly impact China's national, economic or social security. Article 2 of the draft law states that it not only applies to data processing, use, provision and disclosure within China, but that it also applies to organisations and individuals outside of China that conduct activities that may harm China's national security or public interests. The draft law

73 www.cac.gov.cn/2019-05/28/c_1124546022.htm.

74 www.cac.gov.cn/2020-04/27/c_1589535450769077.htm.

continues to allow for regional governments to regulate and implement measures to protect important data at a local level and reiterates a variety of requirements set forth by existing regulations and draft rules, such as security review on data processing that may affect state security, export control on 'controlled data' and a blocking statute in connection with the obtaining of data by foreign enforcement agencies from China. Furthermore, the draft law creates a new licence for online data processing business. The draft law aims to centralise risk assessment, reporting, information sharing and monitoring, and creates a national response system to mitigate losses and warn the public in an emergency that threatens national security. With respect to data-related trade or investments, China has included in the draft bill the opportunity to take corresponding measures against any country that discriminates against China.[75]

Hong Kong

On 20 January 2020, the Constitutional and Mainland Affairs Bureau issued a discussion paper to propose amendments to the existing Personal Data (Privacy) Ordinance (PDPO), which was enacted in 1996 and overhauled in 2012. Recent major personal data breach incidents exposed significant gaps in the current law, including the absence of a mandatory requirement to report data breaches and inadequate penalties to deter violations. Currently, breach notifications are made on a voluntary basis, but the discussion paper proposes a mandatory breach notification to require a data user to report breaches as soon as practicable and, in any event, within five business days. The discussion paper also proposes requiring data users to formulate a retention policy, recognising the risk of a data breach increases the longer the data is held. Under the PDPO, the maximum fine for non-compliance with an enforcement notice is HK$50,000 and imprisonment for two years on first conviction. The discussion paper proposes the introduction of a fine linked to annual turnover, which will bring Hong Kong closer in line with sanctions under the EU's GDPR.

Singapore

In May 2020, Singapore's Ministry of Communications and the Personal Data Commission launched a public consultation on a new bill proposing key amendments to the existing 2012 Personal Data Protection Act. The bill was read for the first time in Singapore's parliament in October 2020 and may come into force before the end of the year.[76] The amendments aim to ensure the existing Act keeps pace with technological advances and global developments in data protection legislation. The bill proposes a mandatory data breach notification obligation for the first time in Singapore and increases the maximum penalties for violations of the Act to the greater of 10 per cent of annual gross turnover in Singapore or S$1 million. The bill also proposes to expand deemed consent as a legal basis for the collection, use and disclosure of personal data to include contractual necessity and consent by notification and proposes legitimate interests and business improvement as alternatives to

75 www.pkulaw.cn/staticfiles/fagui/20200702/09/19/5/34f52a05583e352871fa38da6c354174.pdf.

76 www.parliament.gov.sg/docs/default-source/default-document-library/personal-data-protection-(amendment)-bill-37-2020.pdf.

consent. These amendments will provide organisations with greater flexibility in how they use data. The bill also introduces the right for individuals to request that an organisation transmits a copy of their personal data to another organisation.

Europe

On 25 May 2018, the GDPR took effect across the European Union (including the nations of the European Economic Area). The GDPR imposes substantial privacy and security requirements, which apply to companies with 'establishments' in Europe. But the GDPR also applies to companies around the world – including in Latin America – that target or monitor EU citizens.

Regarding privacy, EU data subjects enjoy significant rights to receive robust notice upfront of how their personal data will be used. EU data subjects also now have the right to access, correct and even delete their personal data that is held by companies. Companies, in turn, face tough requirements to process personal data only for the limited purposes that the GDPR permits. The GDPR also limits the ability of companies to transfer personal data outside the European Union.

The GDPR is best known as a privacy regulation, but it also has a significant cybersecurity component. The regulation mandates that companies maintain substantive cybersecurity protections at a level 'appropriate' to the risk of harm if the data was compromised. Companies are also required to disclose certain data breaches to data protection authorities and, in certain circumstances, to the affected individuals. Disclosure to the relevant authority is generally due within 72 hours – a short time frame that makes clear the importance of being prepared to respond to an incident.

Since the GDPR came into effect, EU supervisory authorities have demonstrated their willingness to use their newfound enforcement powers aggressively, imposing hefty fines on companies including Google and the Italian telecommunications operator TIM. The new operational cost to companies is illustrated by the fine imposed on a Swedish-headquartered data analytics firm for failing to mail privacy notices to over 6 million people, despite the fact that the cost of that mailing would have exceeded the company's turnover for the year. The most substantial fines thus far have related to companies for alleged over-collection, misuse or misconfiguration of data without any breach. The maximum administrative fine imposable is the higher of €20 million or 4 per cent of the data user's global annual turnover in the preceding year.

On 16 July 2020, in *Data Protection Commission v. Facebook Ireland* (*Schrems*, more commonly known as *Schrems II*) the Court of Justice of the European Union (CJEU) invalidated the European Commission's adequacy determination regarding the EU–US Privacy Shield, and cast substantial doubt over European Commission-approved standard contractual clauses (SCCs) for cross-border transfers of personal data.[77] In general, the GDPR allows for transfers to non-EU countries through approved channels, which, broadly speaking, ensure that EU personal data that arrives at non-EU destinations will continue to be protected by

77 http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=9714885.

privacy standards approximate to those of the GDPR. Historically, two transfer mechanisms on which companies could rely for EU-US data transfers were the Privacy Shield and SCCs that parties could include in their own contracts.

In the *Schrems II* decision, the CJEU determined that the Privacy Shield does not sufficiently safeguard EU personal data once it leaves the EU. The CJEU further found that the SSCs can constitute a lawful basis for the transfer of personal data to a jurisdiction without an adequacy decision if the recipient is in a jurisdiction that affords the data subject 'a level of protection essentially equivalent to that guaranteed within the EU'; but given the holding relating to the Privacy Shield, it seems unlikely that the US would be considered such a jurisdiction.

EU authorities will hopefully clarify their enforcement intentions soon, but in the meantime organisations that rely on the Privacy Shield alone for data transfers out of the EU generally are turning to consideration of other EU-approved mechanisms for the transfers. Companies relying on the SCCs may wish to consider whether any jurisdictions they transfer data to have local laws that could ultimately render their reliance on SCCs invalid.

The United Kingdom left the EU on 31 January 2020. The United Kingdom and the EU have until 31 December 2020 (unless extended) to negotiate their future relationship. Until this deadline, EU laws including the GDPR, continue to apply in the United Kingdom. The United Kingdom enacted its own Data Protection Act in 2018 to implement the GDPR at the national level. This means that data protection legislation in the United Kingdom will continue to be largely consistent with the GDPR, though any amendments to the GDPR after the end of the transition period will not automatically apply in the United Kingdom. Unless the United Kingdom receives an adequacy decision from the European Commission, the United Kingdom will be treated as a 'third country'. As such, after the transition period, any company wishing to transfer personal data from the EU to the United Kingdom will need to ensure they comply with the third country data transfer provisions of the GDPR.

United States

California

The California Consumer Privacy Act (CCPA), a significant new consumer privacy statute, took effect on 1 January 2020 and became enforceable on 1 July 2020. The CCPA applies to for-profit companies of all kinds and governs the collection, use and disclosure of the personal information of California residents. Most notably, the CCPA requires companies to allow consumers to opt out of the sale of their personal data. Covered companies also are required to give consumers extensive notice of how their data will be handled. Individual consumers have broad new rights to compel companies to provide access to their data, and to correct or delete it – similar to the GDPR.

California's Office of Administrative Law approved final regulations under the CCPA on 14 August 2020.[78] Among the changes in the final regulation was a broadening of the definition of 'personal information' to include IP addresses that could be linked to a consumer or

78 Department of Justice, Title 11, Division 1, Chapter 20. California Consumer Privacy Act Regulations (14 August 2020), available at www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf?.

household regardless of whether a particular business actually links or is capable of linking the IP address to a consumer. The regulation also imposes additional annual reporting requirements on any business that 'knows or reasonably should know' that it buys, receives, sells or shares, for commercial purposes, the personal information of 10 million or more consumers in a calendar year.

The new regulation also includes additional requirements for the content of a privacy policy, including that a business identify: the categories of sources from which it collects personal information, much like the GDPR's requirement that a business identify processing purposes; and the 'business or commercial purpose for collecting or selling personal information'. A business with actual knowledge that it sells the personal information of minors under the age of 16, must also describe in its privacy policy its plan for obtaining affirmative, opt-in consent for the sale of personal information.

Although the scope of the CCPA is still quite broad, several amendments limited the final rule in important ways. For example, the CCPA exempts entities subject to the federal Health Insurance Portability and Accountability Act (HIPAA)'s Privacy Rule. The amendments also exempted 'personal information collected, processed, sold or disclosed pursuant to' the California Financial Information Privacy Act and to the federal Driver's Privacy Protection Act of 1994. These exemptions are not entirely safe harbours – some of a company's uses may not fall within the exemptions. The CCPA also has important exemptions for employees' and job applicants' personal information and personal data obtained in the context of M&A due diligence, though some of these limitations will expire on 1 January 2021 unless the legislature acts again.

The CCPA is focused primarily on data privacy, but also has a security component. The CCPA grants consumers the right to sue and receive generous money damages in the event of a data breach. Over 30 such class action suits have been brought in 2020, many of them not specifying what, other than falling victim to a breach, the company did wrong. A separate, pre-existing California statute also requires companies to take 'reasonable' cybersecurity measures to protect personal data.

In November 2020, California voters approved the California Privacy Rights Act (CPRA). The CPRA defines a new category of 'Sensitive Personal Information'. This category includes data elements such as Social Security number, ethnic origin and religious beliefs. Consumers now have the right to 'limit the use of [their] sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services'. That appears to mean, among other things, no use of sensitive personal information for marketing or analytics. The CPRA explicitly broadens the CCPA's regulations to include companies 'sharing' - not just 'selling' - personal data. The CPRA becomes enforceable on 1 January 2023, giving companies a little over two years to prepare for compliance. Consumers' data requests, though, will relate back one year. This means a request made after the CPRA's effective date may require searching for, disclosing, correcting or deleting data going back as far as 1 January 2022.

New York

In mid-2019, the US state of New York enacted the Stop Hacks and Improve Electronic Data Security Act (the SHIELD Act), which created new substantive requirements of 'reasonable' cybersecurity. The SHIELD Act also expanded the definition of personal information in New York's data breach notification requirements.

The SHIELD Act requires any person or business that owns or licences the computerised personal information of any New York resident to 'develop, implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information including, but not limited to, disposal of data'. The law does not precisely define 'reasonable' security, but offers some guidance on minimum expectations. It appears this is intended to be an evolving standard, which will likely become more stringent over time, as the collective definition of an objectively appropriate cybersecurity programme evolves to match developing threats.

An entity is deemed compliant with New York's new 'reasonableness' standard if it is subject to, and compliant with, certain other cybersecurity regimes: the federal Gramm–Leach–Bliley Act; the federal healthcare standards; the New York Department of Financial Services (DFS)'s Cybersecurity Regulation (DFS Part 500); or any other data security rules and regulations promulgated by the federal or New York state government.

In July 2020, DFS brought its first enforcement action for alleged violations of DFS Part 500, imposed stringent new cybersecurity regulations on financial institutions beginning in 2017. In its statement of charges, DFS asserted that the subject company had failed to perform an adequate risk assessment; failed to maintain proper access controls; failed to provide adequate security training for cybersecurity employees; and failed to encrypt certain non-public information.[79] The company in question also allegedly failed to remediate a vulnerability that exposed the sensitive personal information of thousands of individuals, despite identifying the issue during penetration testing. The violations carry potential penalties of up to US$1,000 each. In its press release, the DFS asserts that each instance of non-public information that was accessed by an unauthorised person constitutes a separate violation.

Both the SHIELD Act and DFS Part 500 have national and global implications, including in Latin America, because financial institutions from around the US and the world do business in New York under licence from the DFS and own and licence New York residents' information.

Other states and the federal government

All 50 US states now have breach notification laws, many of which have recently been strengthened. For example, the state of Washington shortened the time companies have to notify impacted individuals to 30 days and expanded its definition of personal information.[80]

79 *In Re First American Title Insurance Co.*, No. 2020-0030-C (21 July 2020) www.dfs.ny.gov/system/files/documents/2020/07/ea20200721_first_american_notice_charges.pdf.

80 WA ST § 19.255.005 et esq.

Texas amended its data breach law to require, among other things, that a company to offer free credit monitoring for breaches that involve Social Security numbers.[81]

There is still no general breach notification requirement at the federal level in the United States. Notice of certain breaches involving healthcare data is required under the federal HIPAA statute. Financial institutions regulated under the federal Gramm-Leach-Bliley Act are subject to regulatory agency guidance instructing them that they should give notice of breaches.

Best practices for risk reduction and crisis management

This section focuses on how companies may seek to prevent and ultimately respond to data breaches in a way that both meets any legal disclosure obligations and preserves trust with their stakeholders. While the guidance here is focused on security breaches, it also applies in large measure to privacy breaches that are unrelated to security issues.

Substantive cybersecurity measures

As noted, the emerging global law of cybersecurity typically states that a company's security programmes must be 'appropriate' to the risk (e.g., GDPR), 'reasonable' (e.g., California law and HIPAA) or uses similar terminology. Notably, both the GDPR and the LGPD require both 'technical and organisational' measures – meaning that the cybersecurity programme must include a combination of policies and procedures, such as a well-tested incident-response plan (discussed below), alongside strong technical protections (e.g., encryption of sensitive data).

Collectively, this means that cybersecurity is not simply the domain of technical experts. The required level of protection is risk-based and should contemplate the sensitivity of the data in question, the risk of harm if a given data set were compromised, whether best practices as recognised by the technical community are in place and whether the cybersecurity programme is regularly evaluated and improved based on the evolving threat profile.

Certain measures have already been so widely embraced by the security community that they would be part of almost any 'appropriate' or 'reasonable' cybersecurity programme. As noted, encryption of data, both at rest and in transit, is required by New York's DFS cybersecurity regulation. So is the use of multifactor authentication – that is, the use of both a password and a second entry credential, such as a short-term code transmitted to the user by text message, to access an account.

Threat vectors and best practices are constantly evolving, as is the technical community's understanding of what are 'reasonable' or 'appropriate' security measures – as well as the law's understanding. Companies should thus encourage strong communication among their information security, legal and compliance teams. This will help companies recognise and respond to new technical standards as they begin to shape into legal standards.

81 TX BUS & COM § 521.001 et seq.

The incident-response plan

Good preparation begins with having a written incident-response plan (IRP). Strong IRPs have a number of recognised elements.

The IRP should identify all the key teams within a company that are essential to cross-functional incident response. Typically, the IRP will assign primary leadership roles to the information security team and the legal team. Other teams with key roles include the C-suite, communications (including media relations and social media), risk, human resources and government relations. The privacy team and the information technology team – to the extent these are separate from information security – generally should be included as well.

The IRP should identify the specific personnel members who will form the company's incident response team (IRT). Each business unit should have both a primary and backup person designated. Contact details for each person should be listed, including business contact information, personal email addresses and mobile phone numbers that can be used if corporate systems are compromised.

The IRP also should identify key external resources that may be engaged in an incident. The list of key external resources should typically include:

- external counsel;
- at least one external forensic vendor;
- law enforcement;
- relevant regulatory agencies;
- the company's insurance broker and carriers;
- key members of the company's external board of directors; and
- a crisis communications consultant or vendor who can handle large-scale mailings to affected customers or shareholders.

Once again, both work and non-work contact details should be included. Many of these stakeholders should not just be listed in the IRP but should be engaged in its preparation and testing, so that they are aware of the role they would play in a breach.

External counsel and the external forensic consultant should be brought together with other key IRT members ahead of any breach so that they can all become familiar with the company's relevant systems, policies, procedures and personnel. As the saying goes, 'do not meet your team for the first time on the day of the game'. External counsel have a key role to play in ensuring that legal requirements are met and that the legal privilege applicable to the work of the IRT is protected to the maximum extent possible under local law.

The IRP should spell out a process for classifying incidents according to their severity and the degree of certainty regarding the facts. There is usually an early period during which an incident is suspected but not yet confirmed. It is usually best that a smaller 'core team' take charge of evaluating potential incidents and responding to less severe incidents. The broader cross-functional team should be engaged to help respond to larger incidents once the facts are confirmed or if there is an extended period of uncertainty.

The IRP should provide a process for responding to confirmed incidents. There should be clear pre-defined roles for each IRT member. Someone should be designated to chair the IRT and to keep a record of its work. Key documents that are likely to be needed as part of a

breach response – such as notices to regulators, to affected data subjects and to the press – should be drafted in advance and appended to the IRP, with blanks left for the facts specific to a given incident.

The IRP should be as short and clear as possible. The goal is to have IRT members actually rely on and utilise the IRP in the event of a crisis. The longer and more complicated the IRP is, the greater the chance that people will simply disregard it.

Testing the incident-response plan

A well-written IRP and a well-defined IRT are essential to strong incident response, but they can be ineffective if they are not also well tested. Incident-response simulation drills, known informally as 'tabletop' exercises, have become an important part of many corporate cybersecurity programmes.

The best tabletops are prepared with an eye towards the specific facts and circumstances of the company. Certain personnel (often external counsel or forensic consultants) are designated to prepare the tabletop scenario, in isolation from the participants in the tabletop. This ensures that participants are responding during the drill without prior knowledge of the 'facts'.

On the day of the drill, the members of the IRT (or whatever business units are part of the drill) gather in a room, or via teleconference or video link. The person responsible for guiding the drill then announces the 'facts', revealing additional facts periodically as the drill proceeds. Tabletops can last anywhere from a couple of hours to a whole day.

Over the course of the tabletop, the moderator announces a series of new factual revelations according to a stated timeline: 'it is Tuesday at 10am, and the hacker just did X; now we assume it is Thursday at 2pm, and law enforcement just announced Y' and so on. With each factual revelation, different participants are called on to state what they would do, and how and with whom they would communicate. There is active discussion between all participants throughout.

The results of the tabletop are often processed in two stages. Before people leave the room at the close of the drill, they step out of the role-playing format and have an immediate discussion about the lessons learnt from the drill. Afterward, thoughts are collected from participants in a more systematic manner, and the lessons learnt are incorporated in the form of revisions to the IRP.

Responding to an actual incident

With a well-tested IRP in place, a company is prepared to respond to an actual incident:

- the IRP is activated and the IRT is periodically brought together at a set time and place. As the facts are confirmed, necessary notifications begin to go out – to civil regulators, data subjects, the press, the board, employees and other stakeholders;
- technical measures are implemented to protect the company's systems, for example, by cleansing malware from infected computers, or backup systems are activated to circumvent a ransomware attack that has disabled main systems;
- a careful record is kept of all key incident response steps, with one or more IRT members specifically designated to act as the secretary or archivist of the process;

- if criminal activity is suspected, the company makes a decision as to whether and how to engage with law enforcement;
- evidence that may be needed to document the events is carefully retained. For example, any cleansing of infected computers is conducted by the information security team or outside forensic experts in consultation with counsel and law enforcement, so that evidence necessary for subsequent investigations and legal proceedings is preserved; and
- all participants in the breach response process are carefully cautioned to communicate in a careful manner. Secure communication channels should be used until it is certain that intruders are not present on company systems.

As the days and weeks go by, the crisis atmosphere will begin to recede. Immediate forensic and communications measures are completed. The company can then begin to engage in a 'lessons learned' exercise. This involves going beyond the purging of infected computers to consider and address any more systemic weaknesses identified by the breach. Longer-term remedial measures in a large company can easily take months or even years to complete. A 'lessons learned' exercise specific to the work of the IRT is often useful as well, and can lead to positive improvements to the IRP.

The importance of communications in minimising legal and reputational harm cannot be overstated. The guidance here is simple: companies survive breaches best when they communicate early, clearly, accurately and tersely. There is an understandable wish to deny or minimise a cybersecurity problem, rather than admit embarrassing facts. At the other extreme, there can be a temptation to state the details with great precision, to encourage the impression that the company is fully in command of the situation. But cybersecurity incidents often do not lend themselves to either approach. Cyber forensics take time, and the facts are rarely clear at first.

Accordingly, an early statement along the lines of 'we are aware of suspicious activity, we are investigating and we will post updates as we know more' will often be most consistent with the facts. A company that denies the problem, or that prematurely states uncertain facts as if they were definitive, may then have to issue corrective statements as the facts change. This can create the impression that the company is not candid or competent. That, in turn, tends to create reputational damage and increases the chances of tough legal scrutiny from regulators and courts. As legal requirements for prompt breach disclosure grow, clear and careful early communication becomes ever more important.

Impact of covid-19 on data breaches

In countries impacted by covid-19, the introduction of lockdown measures, the use of new virtual communication platforms and the increased numbers of employees working from home have multiplied many companies' risk of cyber threats. In particular, companies around the world are seeing a dramatic rise in phishing attempts and resulting security incidents, including the deployment of ransomware and the exfiltration of sensitive data.

Cybersecurity and protection of personal data should remain a priority for companies even during these challenging times. Companies should ensure that employees are provided with encrypted devices and do not use their personal emails for professional purposes and

companies should review, update and distribute their confidentiality, cyber hygiene and IT policies. To minimise the threat posed by phishing attacks, companies should regularly train employees on how to spot a potential phishing email, ensure that they use consistent formatting in emails, bolster their anti-virus software and firewalls, and protect their networks from ransomware attacks.

As companies begin to reopen their physical spaces, it is also becoming common to collect significant new amounts of personal information from employees and visitors. New procedures include temperature checks, health questionnaires, and the use of various apps and devices to track health and location. It is prudent to check these new practices against the standards of the privacy laws of the countries where the practices are used. Privacy law, for example, may call for additional disclosure of data collection and processing, while security law may call for additional measures to protect the data.

Increased adoption of artificial intelligence technologies

The global market for artificial intelligence (AI) is poised to skyrocket over the next decade. Companies are increasingly embedding AI technology in their products and services to automate complex tasks, solve problems and learn from new data at scale. AI also can improve efficiencies of both human and physical capital, such as by reducing worker fatigue or predicting which machinery will need maintenance before problems occur.

AI adoption in both the public and private sectors is proceeding rapidly in Latin America, as in the rest of the world. According to Accenture, AI has the potential to add up to one percentage point in annual economic growth to the economies of Argentina, Brazil, Chile, Colombia and Peru through 2035.[82] AI is already deployed across key sectors – from chat-bots in banking and retail to sentiment recognition in hiring and autonomous drills in mining. Latin America's AI adoption has been fuelled not only by the digitisation of sectors such as healthcare, but also by regulatory changes that make it easier to collect and share data. For example, in the fintech space, open banking reforms have encouraged portability of customer data and transaction histories, driving the ability of start-ups to innovate and compete with established banks.[83]

Attempts to regulate AI in Latin America are still in the early stages and have focused largely on the adoption of national AI strategies or ethical frameworks. In 2018, Mexico became the first country in Latin America – and among the first 10 countries worldwide – to publish a national AI strategy, which included a focus on developing adequate governance frameworks.[84] Mexico also published a set of principles and a 'risk assessment tool' to

82 See Armen Ovanessoff and Eduardo Plastino, 'How Artificial Intelligence Can Drive South America's Growth', Accenture Research (2017), available at www.accenture.com/_acnmedia/pdf-48/accenture-ai-south-america.pdfla=es-la.

83 See PYMNTS.com, 'All Eyes Are on LATAM Open Banking' (24 July 2020), available at www.pymnts.com/bank-regulation/2020/all-eyes-are-on-latam-open-banking/.

84 Enrique Zapata, Estrategia de Inteligencia Artificial MX 2018, México Digital Blog (22 March 2018), available at www.gob.mx/mexicodigital/articulos/estrategia-de-inteligencia-artificial-mx-2018.

facilitate the ethical and responsible use of autonomous systems in its federal government.[85] More recently, Brazil, Argentina, Chile and Uruguay likewise have embarked on the process of developing their own national AI strategies and frameworks.[86] Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico and Peru also adhere to the OECD's Principles on Artificial Intelligence, which aim to 'promote AI that is innovative and trustworthy and that respects human rights and democratic values'.[87]

In the absence of binding laws and regulations, the burgeoning growth of AI in Latin America has been effectively left to be regulated by data protection or consumer protection laws. Many countries are currently looking to the European Commission, which has announced its intention to develop a comprehensive regulatory framework for AI. In February 2020, the European Commission published a white paper outlining a series of possible oversight mechanisms for certain 'high-risk' AI applications or sectors, such as transportation, healthcare and energy.[88] If the European Union ultimately adopts a sweeping approach to AI regulation similar to the GDPR, this could serve as a template for other jurisdictions in the future.

Conclusion

Legal requirements concerning cybersecurity and data privacy are continuing to multiply in the Americas and around the globe. As they do, global standards are emerging for what a corporate cybersecurity and data privacy programme should look like in the ordinary course and for how to respond when things go wrong.

History and the law provide this simple message: companies that prepare for the worst will respond the best. The key is to have a robust suite of cybersecurity and data privacy measures designed to reduce the chances of a crisis, accompanied by a robust plan for incident response when a crisis inevitably hits. That plan should be practical, business-friendly, cross-functional, written clearly and compactly, and well tested. Above all, response plans should be designed to preserve and build trust, through clear, prompt and careful communication and action followed by effective long-term remediation.

85 See Innova MX, 'Guía de análisis de impacto para el desarrollo y uso de sistemas basadas en inteligencia artificial en la APF' (28 November 2018), available at www.gob.mx/innovamx/articulos/guia-de-analisis-de-impacto-para-el-desarrollo-y-uso-de-sistemas-basadas-en-inteligencia-artificial-en-la-apf.

86 See OECD.AI Policy Observatory Dashboard, Brazil Formal Consultations for a National Artificial Intelligence Strategy, available at https://oecd.ai/dashboards/policy-initiatives/2019-data-policyInitiatives-25303; OECD.AI Policy Observatory Dashboard, Argentina Artificial Intelligence National Plan, available at https://oecd.ai/dashboards/policy-initiatives/2019-data-policyInitiatives-24309; OECD.AI Policy Observatory Dashboard, Chile Artificial Intelligence Working Plan, available at https://oecd.ai/dashboards/policy-initiatives/2019-data-policyInitiatives-24840; OECD.AI Policy Observatory Dashboard, Uruguay Data Science and Machine Learning Roadmap, available at https://oecd.ai/dashboards/policy-initiatives/2019-data-policyInitiatives-26480.

87 See OECD Press Release, 'Forty-two countries adopt new OECD Principles on Artificial Intelligence' (22 May 2019), available at www.oecd.org/going-digital/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm.

88 See European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust (19 February 2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

Appendix 1

About the Authors

Jeremy Feigelson
Debevoise & Plimpton LLP

Jeremy Feigelson, a litigation partner, is co-chair of the firm's global data strategy and security practice and is a member of the firm's intellectual property and media group. He frequently represents clients in litigation and government investigations that involve the internet and new technologies. His practice includes litigation and counselling on cybersecurity, data privacy, trademark, right of publicity, false advertising, copyright and defamation matters. Mr Feigelson is recognised by *The Legal 500: United States* (2020). In 2018, *American Lawyer* named him 'Litigator of the Week' based on the right of publicity victories of Debevoise client Take-Two Interactive in *Lohan v. Take-Two* and *Gravano v. Take-Two* at the New York Court of Appeals. Other recognitions include designation as a 'Privacy MVP' by *Law360*, a cybersecurity and data privacy 'Trailblazer' by *The National Law Journal* and 'IP Star' by *Managing Intellectual Property*.

Mr Feigelson received his BA in public and international affairs *magna cum laude* from Princeton University's School of Public and International Affairs in 1984. He received his JD *cum laude* from the University of Chicago Law School in 1991, where he was admitted to the Order of the Coif and served as articles editor of the *The University of Chicago Law Review*.

Andrew M Levine
Debevoise & Plimpton LLP

Andrew Levine is a litigation partner at Debevoise and devotes a significant portion of his practice to investigative and compliance matters in Latin America. He is well recognised in the region for defending companies and individuals in criminal, civil and regulatory enforcement matters, and for conducting internal investigations. Mr Levine serves as a trusted adviser to numerous leading global companies and represents many clients on

corruption-related matters in Latin America, including the *Lava Jato*, *Zelotes*, *Carne Fraca* and *FIFA* scandals. In addition, Mr Levine frequently advises clients on a broad array of compliance matters, including conducting risk assessments, enhancing compliance programs and mitigating risks presented by potential corporate transactions.

In 2020, *Latin Lawyer* named Mr Levine as 'International Lawyer of the Year'. He is ranked as a leading lawyer for corporate crime and investigations in Latin America by *Chambers Latin America* and as a leading lawyer for FCPA by *Chambers USA*. Since 2013, Mr Levine has co-chaired the annual *Latin Lawyer - GIR* 'Anti-Corruption & Investigations' conference in São Paulo, Brazil and, in June 2019, co-chaired the inaugural edition of this conference in Mexico City, Mexico.

Before joining Debevoise, Mr Levine served as deputy counsel to the Independent Inquiry Committee into the United Nations Oil-for-Food Programme. He received his JD from Yale Law School and his BA *summa cum laude* and Phi Beta Kappa from Yale College.

Christopher Ford

Debevoise & Plimpton LLP

Christopher S Ford is an associate in the litigation department and a member of the firm's intellectual property litigation group and data strategy and security practice. His practice includes advising clients on incident preparation and response, as well as related criminal and civil litigation and regulatory investigations. His recent matters include managing responses to corporate data breaches, business email compromises, ransomware incidents and other data security issues, as well as advising a wide range of the firm's clients on managing their cybersecurity and business continuity risks. Mr Ford joined Debevoise in 2012. From 2015 to 2017, he clerked for the Hon Laura Taylor Swain of the United States District Court for the Southern District of New York. Mr Ford received a JD from Duke University School of Law, *cum laude*, in 2012, where he served as an articles editor on the *Duke Law Journal*. He received a BA, with high honours, from Swarthmore College in 2007.

Anna R Gressel

Debevoise & Plimpton LLP

Anna R Gressel is an associate in the litigation department and a member of the firm's data strategy and security practice and commercial litigation group. Ms Gressel represents clients in a wide range of complex commercial litigation, including M&A litigation and securities class actions. Ms Gressel also actively advises clients on the legal and regulatory implications of artificial intelligence and other emerging technologies. Her practice includes representing companies in regulatory inquiries and supervisory examinations, as well as assisting companies in developing AI compliance and governance mechanisms. Ms Gressel also regularly speaks on issues concerning AI regulatory and litigation trends. She is a member of the Law Committee of the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, and she also participates in industry efforts to establish best practices in the areas of AI explainability, risk assessments and governance. Ms Gressel joined Debevoise in 2014. Ms Gressel received a JD from Harvard Law School in 2014. Prior to law school, she was awarded a Fulbright Research Fellowship to Morocco. Ms Gressel received a

BA in neuroscience from Pomona College in 2006, where she was awarded the senior prize in neuroscience.

Stephanie Cipolla

Debevoise & Plimpton LLP

Stephanie Cipolla is an associate in the litigation department and a member of the firm's data strategy and security practice. Her practice focuses on cybersecurity and data privacy issues, including incident preparation and response. Her recent matters include assisting clients in the finance, tech and critical infrastructure sectors in responding to data security incidents, including nation-state attacks, insider threats, email compromises and ransomware attacks. Ms Cipolla also assists clients in developing tailored incident response plans, testing their plans through customised simulated breach drills and advising on regulatory issues, including compliance with the new NYS Department of Financial Services cybersecurity regulation. Ms Cipolla joined Debevoise in 2016. She received her JD *cum laude* from St John's University School of Law in 2016, where she was an editor of the *St John's Law Review*. She received a BA *cum laude* from the University of Pennsylvania in 2012.

Hilary Davidson

Debevoise & Plimpton LLP

Hilary Davidson is a corporate associate and a member of the firm's mergers and acquisitions and data strategy and security groups. Ms Davidson's practice focuses on private M&A, with particular experience advising private equity clients. This has included advising on joint ventures, cross-border mergers and acquisitions, and secondary and co-invest transactions. Ms Davidson joined Debevoise in 2015 and completed her training in the London and Hong Kong offices. She received a BA (Hons) in Law from Pembroke College, University of Cambridge in 2014 and completed the LPC at BPP Law School in 2015. Ms Davidson was admitted as a solicitor of the Senior Courts of England and Wales in 2017.

Debevoise & Plimpton LLP

919 Third Avenue
New York, NY 10022
United States
Tel: +1 212 909 6000
Fax: +1 212 909 6836
jfeigelson@debevoise.com
amlevine@debevoise.com
csford@debevoise.com
argressel@debevoise.com
smcipolla@debevoise.com
hdavidson@debevoise.com
www.debevoise.com

Corruption investigations, expropriation, industrial accidents, pandemics: corporate crises take many forms, but each can be equally dangerous for companies in Latin America.

Published by *Latin Lawyer*, edited by Sergio J Galvis, Robert J Giuffra Jr and Werner F Ahlers of Sullivan & Cromwell LLP, *The Guide to Managing a Corporate Crisis* is designed to assist key corporate decision-makers and their advisers in effectively planning for and managing corporate crises in the region. Fifty leading practitioners from a variety of disciplines have contributed their knowledge and insights from their experience.

Covering the impact of political instability, the role of communications in crisis response, approaches to bribery investigations and game plans in response to financial stress, this book provides guidance that will benefit all practitioners when an unexpected crisis hits.

Visit latinlawyer.com
Follow @Latin_Lawyer on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-429-3