

Data Breach in Latin America

Victoria E. Beckman
Frost Brown Todd

Diego Fernández
Marval, O'Farrell & Mairal

Lucía Fernández González
González Calvillo

Sergio F. Oehninger
Hunton Andrews Kurth

Victoria E. Beckman

Partner

Frost Brown Todd

Victoria is Co-chair of the Privacy & Data Security group and Chair of the Latin America Desk at Frost Brown Todd.

Victoria regularly advises clients on privacy and data security compliance as well as preparing strategies for responding to data breaches and other security incidents.

She also assists U.S. companies throughout Latin America with cross border transactions and data and technology agreements.



Diego Fernández

Partner IP, IT & Privacy
Marval, O'Farrell & Mairal
Argentina

Diego Fernández is a partner with Marval O'Farrell Mairal's Intellectual Property, Information Technology and Privacy practice group.

Currently, he is a Board Member and Chair of the Latin America Committee of the International Technology Law Association (ITechLaw), Co-Chair of the Buenos Aires KnowledgeNet Chapter of the IAPP, and member of the Technology Committee of the International Bar Association.



Lucía Fernández

Elected Counsel
González Calvillo, S.C.
Mexico

Lucía Fernández is an elected counsel (effective July 2020) and has more than 15 years of experience in commercial and corporate matters, including IT and data protection, franchising and licensing as well as regulatory matters, advising particularly in connection with consumer protection and advertisement.



Sergio F. Oehninger

Partner

Hunton Andrews Kurth LLP

Sergio counsels multinational corporations on insurance coverage and risk management issues arising across industries and borders. His advice focuses on insurance for cyber incidents, commercial general liability, directors and officers liability, property damage, and business interruption. As part of his Latin America practice, Sergio advises corporate clients on cross-border exposures in connection with transactions, projects, operations, products, and services. More recently, Sergio has been advising companies on business interruption insurance for COVID-19-related losses.



- **Purpose of Session**

To understand the different data breach notification laws and requirements throughout Latin America and compare them with U.S. requirements

- **Main Sections**

Overview of Latin American Laws
Argentina & Mexico
Cyberinsurance considerations

- **Questions**

Latin America

Overview

Country	Data Protection Law	Data Security Requirements	Breach Notification Requirement	Remedies
ARGENTINA	Data Protection Law 25,326	No Recommendations based on the principle of accountability	Recommended notification to the Data Protection Authority (DNDP), but not required	<ul style="list-style-type: none"> DNDP can impose sanctions & fines but not award damages or costs Private right of action Infringement could constitute a crime
BOLIVIA	Article 56, Title IV of Law 164 (Aug. 2011) Comprehensive (2009) law pending approval	Yes	No	<ul style="list-style-type: none"> Seek cease of breach and obtain monetary compensation for damages No cyberinsurance available
BRAZIL	Law No. 13,853/19 (LGPD)	Yes	Security incidents that present significant risk or damage to data subjects must be communicated to the Data Protection Authority (ANPD) and data subject in a <i>reasonable</i> time. Additional mitigation required depending on risk.	Private right of action to recover moral & economic damages
CHILE	No privacy laws for the private sector	No	No	Civil court action for damages
COLOMBIA	Statutory Law 1581 of 2012	Yes	Yes, to the Data Protection Authority (SIC)	<ul style="list-style-type: none"> Habeas Data (not monetary compensation) SIC can impose fines Criminal claim
COSTA RICA	Law 8968	Yes	Yes, to the Data Protection Authority (PRODHAB) and the individuals	Civil court action for damages
DOMINICAN REPUBLIC	Law No. 172-13	Yes	No	Civil court action for damages
ECUADOR	Law pending approval	Yes	No	Civil court action for damages
EL SALVADOR	No law	No	No	<ul style="list-style-type: none"> Habeas Data (not monetary compensation) No Administrative remedy
GUATEMALA	No law	No	No	None
HONDURAS	No law	No	No	None
MEXICO	LFPDPPP	Yes	No requirement to report to Data Protection Authority (INAI) Requirement to notify individuals of any breach that significantly affects their moral or patrimonial right	<ul style="list-style-type: none"> Administrative proceedings in front of INAI but no damages awarded. Civil court action for damages Criminal complaint
PANAMA	Law 81 (effective 03/29/2021)	Yes	No	<ul style="list-style-type: none"> Civil court action for damages (currently) Fines by ANTAI under Law 81
PARAGUAY	Law pending approval	No	No	<ul style="list-style-type: none"> Civil court action for damages Criminal complaint
PERU	Law N° 29733/2013 (PDPL)	Yes	No requirement to report to Data Protection Authority (APDP) Requirement to notify individuals of any breach that affects their economic or moral rights	<ul style="list-style-type: none"> Fines by APDP Civil court action for damages
URUGUAY	Law No. 18.331 (2008); Decree No. 414/009	Yes	Yes, immediately to authority and individuals	Fines by AGESIC
VENEZUELA	No law	No	No	Civil court action for damages

United States v. Latin America

1. Requirement to notify
2. Costs
(multiple state notification, credit monitoring and ID theft services, legal fees)
3. Attorney-client privilege
4. State laws and federal (industry specific) laws
5. Cyber Insurance

Data Breaches in Argentina

Introduction to Argentinean Law

1. Federal Legislation

- Data Protection Law 25,326
- Regulatory Decree 1558/2001
- Regulations by the Data Protection Authority

2. Data Protection Authority

Access to Public Information Agency

3. Sanctions and fines

Data Breach Regulation

1. No definition
2. No obligation in the Data Protection Law
3. Section 9 of the DPL and Regulatory Decree
4. Resolution DPA 47/2018
5. Civil and Commercial Code
6. Data Protection Bill
7. Cyber insurance
8. The market

Data Breaches in Mexico

Introduction to Mexican Law

1. Main Legislation

- Federal Law on Protection of Personal Data Held by Private Parties and secondary legislation
- General Law on Protection of Personal Data Held by Obligated Parties and secondary legislation

2. Regulatory Authority- INAI

National Institute for Transparency, Access to Information and Personal Data Protection

3. Sanctions can be relevant

Data Breach Regulation

1. Broad Data Breach Definition

2. Controller's Obligations

- Notification to data subjects, not INAI
 - if it *significantly prejudices a data subject's economic or moral rights*
 - without delay
 - must comply with minimum requirements
- Corrective Measures

Q.- What are patrimonial/economic or moral rights, what can be considered as a "significant prejudice", what is without delay?

Best Practices: INAI's Recommendation Regarding the Management of Security Incidents of Personal Data

- **Non-binding, but implementation may lower sanctions.**
- **Advice to Controllers- focuses on identifying, containing, mitigating, monitoring and documenting data breaches.**
- **Relevant legal information:**
 - Provides definition to patrimonial/economic or moral rights.
 - Provides notification timing- when breach is contained and assets no longer exposed.
 - Preference for direct notification (phone, email or personally), use more than one means if urgent.
 - Additional points in breach notification.

Cyber Insurance Considerations

Importance of Cyber Insurance Application Process

1. The Application.
2. Exclusions to Avoid.
3. Mind the Gaps.



What Does Cyber Insurance Cover?



First Party Coverage

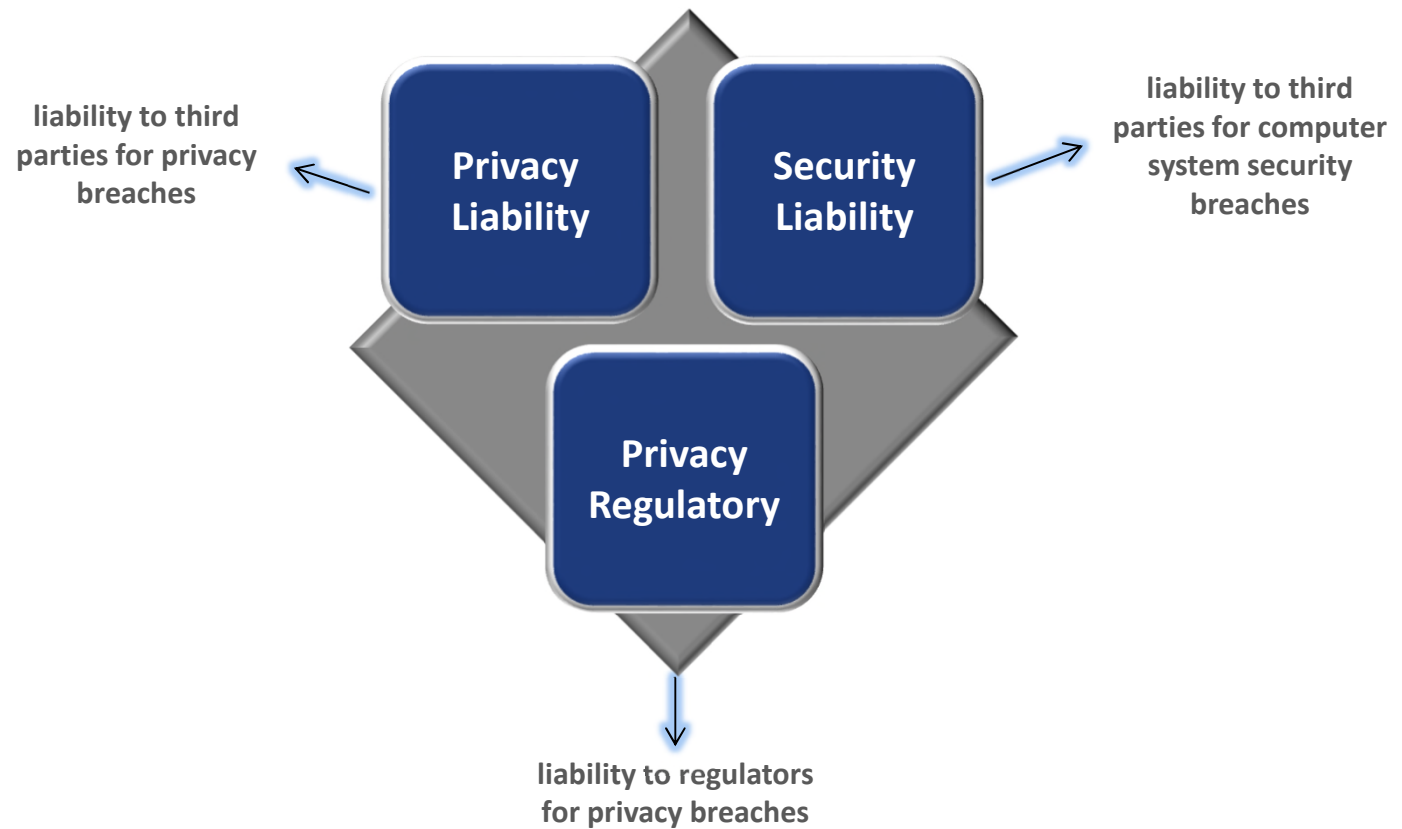
Data/Electronic
Information Loss

Business Interruption
or Network Failure
Expenses

Cyber-Extortion

Reputational Harm

What Does Cyber Insurance Cover?



**Third Party
Coverage**

Hybrid Coverage



Covered Claims

- Security Event (e.g. breach, DDOS, use of code)
- Privacy Event (involving PII or Confidential Business Information)

Covered Costs

- Forensics to determine existence, cause & scope
- Legal & PR
- Mandated (sometimes voluntary) breach notification
- Call Centers
- Credit/Identity Monitoring
- Data Restoration

Traditional Insurance

- Coverage Under Traditional Policies:
 - Property & Business Interruption
 - Commercial Crime
 - General Liability
 - D&O Liability
- Silent Cyber
- Absence of Cyber Exclusion Wording



Traditional Insurance

- Insurance Requirements Across Borders
- Structures for Multinational Corporations include:
 1. Decentralized Program
 2. Global Program
 3. Controlled Master Program



Reference Materials



Argentina:

[Data Protection Law \(Spanish\)](#)

[Regulatory Decree \(Spanish\)](#)

[Recommended Security Measures](#)

[Data Protection Bill](#)

Mexico:

[Laws and some secondary legislation \(English\)](#)

[Recommendations](#)

Cyber Insurance:

[COVID-19 Impacting Cyber-Security – Attacks on the Rise](#), Hunton Insurance Recovery Blog, March 27, 2020

[Equifax's Hefty \\$700M Bill is a Powerful Reminder to Close Cyber & D&O Coverage Gaps](#), Hunton Insurance Recovery Blog, July 24, 2019

[Are Latin America's Energy Firms Ready for Cyberthreats?](#), Energy Advisor, June 29, 2018.

[Sergio F. Oehninger, Cross-Border Insurance Coverage](#), New Appleman Insurance Law, LexisNexis Publishers, September 15, 2016

Questions + Contact



Victoria E. Beckman
Partner
Frost Brown Todd
+1 (614) 559-7285
vbeckman@fbtlaw.com



Diego Fernández
Partner
Marval, O'Farrell & Mairal
+ 54 11 4310-0100 Ext. 1303
dfer@marval.com



Lucia Fernández
Elected Counsel
González Calvillo, S.C.
+52 (55) 5202-7622
lfernandez@gcsc.com.mx



Sergio F. Oehninger
Partner
Hunton Andrews Kurth
+1 (202) 955-1854
soehninger@huntonAK.com