Cyber risks in South America (with a focus on Brazil)

Mariana F. Menescal
Partner, Pellon & Associados , Sao Paulo

Cyber risks scenario in 2018

One in ten URLs are malicious.

The Web attacks increased 56%.

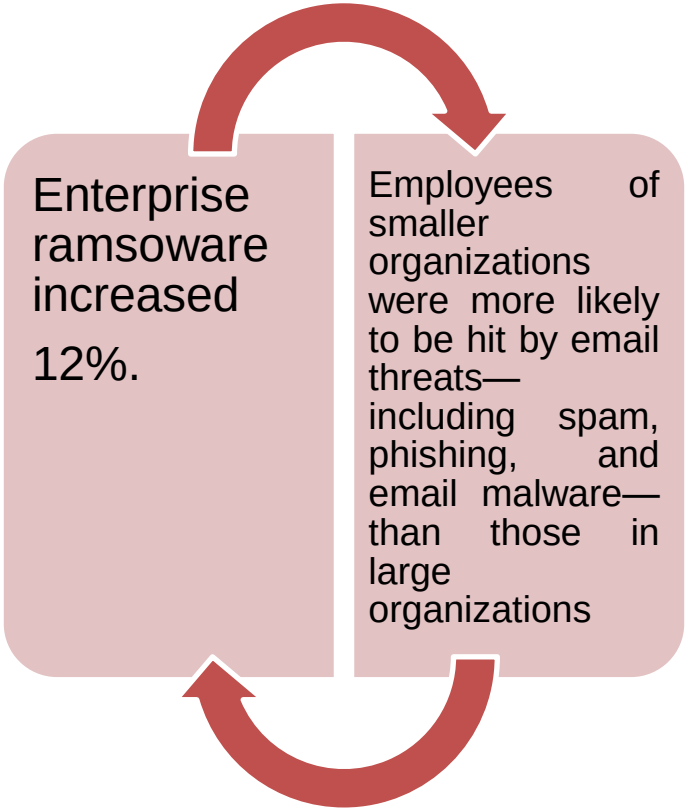
Mobile ramsoware increased 33%.

Supply chain attacks increased 78%.

Pellon & Associados ADVOCACIA

Source: Symantec Report 2019

Risks for companies



Source: Symantec Report 2019

Cyber Criminals target Payment card data

- ✓ **Formjacking**: the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of eCommerce sites.
- ✓ Incidents trended **upwards** in 2018.
- ✓ **4,818** unique websites were compromised with formjacking code **every month** in 2018.
- ✓ With data from a single credit card being sold for up to **$45** on underground markets, just 10 credit cards stolen from compromised websites could result in a yield of up to **$2.2 million** for cyber criminals each **month**.

Pellon & Associados ADVOCACIA

Source: Symantec Report 2019

Top malicious mobile app categories in 2018

Categories	Percent
Tools	39,1%
Lifestyle	14,9%
Entertainment	7,3%
Social & Communication	6,2%
Music & Audio	4,3%
Brain & Puzzle Games	4,2%
Photo & Video	4,2%

Source: Symantec Report 2019

Attacks on the Internet of Things (IoT)

- ✓ In 2018 the average of attacks per month is 5,200.
- ✓ Routers and connected cameras: 90% of all attacks.
- ✓ **Connected cameras** accounted for 15 % of attacks, up from 3.5% in 2017.

Source: Symantec Report 2019

Top source countries for IoT attacks in 2018

Country	Percent
China	24%
USA	10,1%
Brazil	9,8%
Russia	5,7%
Mexico	4%
Japan	3,7%
Vietnam	3,5%

Source: Symantec Report 2019

Top passwords used in IoT attacks in 2018

Password	Percent
123456	24,6%
[BLANK]	17%
system	4,3%
sh	4%
shell	1,9%
admin	1,3%
password	1%

Source: Symantec Report 2019

Latin America Email Attacks

Malicious Email URL Rate by Country in 2018	Email Spam Rate by country in 2018
• Brazil – 35,7% • Mexico – 29,7% • Colombia – 11%	• Brazil – 60,8% • Mexico – 58,1% • Colombia – 56,8%

Source: Symantec Report 2019

Data Protection Law in Argentina

- ✓ Argentina passed one of the first data protection laws in the Latin American region, yet it remains mostly **unchanged since 2000**. Argentina is seeking to revise the current privacy laws in order to maintain its status as a country with adequate level of protection from an EU perspective.

- ✓ In 2018, a bill to replace Argentinian Law No. 25,326 was proposed to align with GDPR, and thus, includes similar rights and principles. These include:

  Incorporation of concepts like “genetic data”, “biometric data” and “cloud computing”;

  Limited scope referring only to natural persons, excluding legal entities;

  Obligation on governmental agencies to appoint a data protection officer if sensitive and big data are being processed; and

  Incorporation of standards for the lawfulness of data processing.

- ✓ Additional data subject rights are also addressed; the bill expressly recognizes the right to object to or restrict the processing and right of data portability.

Source: https://blogs.iadb.org/conocimiento-abierto/en/data-privacy-reform-gains-momentum-in-latin-america/

Pellon & Associados ADVOCACIA

Data Protection Law in Chile

- ✓ Personal data protection in Chile has been regulated by Law 19,628 **since 1999**. Its purpose was to establish general provisions regarding personal data processed by third parties. Although this Chilean law sets forth that **data subjects shall be informed about the purposes of the processing of their personal information** and that their consent shall be collected, it **does not establish mechanisms to supervise the proper compliance** with legal obligations on this matter.
- ✓ In light of this, Chile is seeking to amend Law No. 19,628 to **adjust it to the GDPR´s standards and provisions**. This bill will:

  Regulate protection and processing of personal data;

  Create a data protection council to enforce law and impose **fines up to $700,000 USD**; and

  Introduce biometric data to the definition of sensitive data.
- ✓ It is of great significance to mention that Chile has also agreed to **amend their constitution** to include the **right of protection of personal data**.

Source: https://blogs.iadb.org/conocimiento-abierto/en/data-privacy-reform-gains-momentum-in-latin-america/

Pellon & Associados ADVOCACIA

Data Protection Law in Colombia

- ✓ Colombia is aware of the need to incorporate relevant provisions to their current data protection laws, Law No. 1,581 and Law No. 1,266, that address contemporary technological innovations. The **GDPR includes obligations that are not regulated under existing Colombian laws**, such as the right to be forgotten and the appointment of data protection officers.
- ✓ One of the most important topics in Colombia is the **legislative bill** which pretends to endow data privacy Law No. 1,581 with the international scope of GDPR, including:

  New definitions of sensitive data, public data and privacy notice, and

  Specification of certain requirements for privacy policies.
- ✓ Colombia recently created an "adequacy" list for cross-border transfers, which contains a list of countries that comply with adequate data protection level standards under Colombian criteria.

Source: https://blogs.iadb.org/conocimiento-abierto/en/data-privacy-reform-gains-momentum-in-latin-america/

Pellon & Associados ADVOCACIA

Data Protection Law in Mexico

- ✓ The Mexican Federal Law on Protection of Personal Data Held by Private Parties, effective **since 2010**, is the foundation of a **comprehensive privacy system** which governs the **processing of personal data**, including its collection, use, transfer and storage. Under these current laws, rights such as access, rectification, cancellation or opposition to the treatment of data are granted to data subjects.
- ✓ ***The most active data protection authority in Latin America***
- ✓ **Data Subjects are increasingly more aware of these rights and actively exercise them**. Between January 2012 and June, 2017, the Mexican Data Protection Authority (known as "INAI") handled: (a) 820 Protection of ARCO Rights Procedures and; (b) 2,094 claims filed by data subjects before INAI, which have resulted in 1,520 procedures (discovery phase) and 208 Verification Procedures. Further, INAI is probably the most active data protection authority in Latin America. **Between January 2012 and June, 2017, INAI has imposed sanctions to companies operating in Mexico in 147 cases**, for a total amount of approximately **$16.7 million USD in fines**.
- ✓ While Mexican law also provides lots of room for flexibility and self-regulation, **Mexico is likely to adopt, at least to a certain degree, data protection and security provisions comparable to European regulations**.
- ✓ Important reforms to the current privacy law are expected in the short term to bring Mexican regulations **in line with GDPR**.

Source: https://blogs.iadb.org/conocimiento-abierto/en/data-privacy-reform-gains-momentum-in-latin-america/

Data Protection Law in Peru

- ✓ In **2011**, Peru enacted Law No. 29,733, the provisions of which seek a broad protection and grant appropriate rights to data subjects in the event that companies processing personal data fail to comply with their obligations.
- ✓ The data protection law in Peru has been **recently updated** to expand legal guidelines for data processing and to **strengthen their data protection regime**. Some relevant provisions related to data transfer have been incorporated:
- ✓ The **data controller is obliged to notify any data transfer resulting from a company´s mergers and acquisitions** and to register international data transfers in a Peruvian national registry.
- ✓ New **exemptions to obtaining consent for data processing** are also included, mainly to prevent money laundering and terrorism financing.

Source: https://blogs.iadb.org/conocimiento-abierto/en/data-privacy-reform-gains-momentum-in-latin-america/

Pellon & Associados ADVOCACIA

Data Protection Law in Brazil

- ✓ The Brazilian General Data Protection Law was enacted in August 2018.
- ✓ It will be enforceable in August 2020.
- ✓ Governs rights and obligations related to the processing of personal data, as well as good practices, and also:

  → Creates a **national data protection authority**;

  → Incorporates the **extraterritorial scope of GDPR**; it will apply to **private and public sectors** if the processing occurs in Brazil or personal data is obtained from data subjects located in Brazil, despite the location of the controller;

Data Protection Law in Brazil – cont.

→ Obliges firms and public agencies handling personal data to appoint a **data protection officer**;

→ Creates the obligation to seek the express consent to handle data (which can be revoked at any time);

→ Creates the obligation to inform if a data breach occurs; and

→ Creates the possible **imposition of sanctions, including fines** of up to 2% of a group's gross revenues in Brazil in the last fiscal year for noncompliance, **limited to R$ 50 million**.

Central Bank cyber security policy

- ✓ Enacted in April 2018.
- ✓ Object: cyber security policy and the requirements to be fullfilled in order to hire data processing and storage services and cloud computing;
- ✓ The law is applicable to **financial institutions** and other **institutions authorized by the Brazilian Central Bank**, including the **payment institutions**.
- ✓ The institutions shall comply with the law until **December 31st 2021**, upon the presentation of a **schedule of adequacy**. If they **have already hired such services**, they should have filed the **schedule of adequacy** to the Brazilian Central Bank until **November 2018**.

Civil liability of internet providers in the Brazilian Courts

Lack of responsibility regarding the acts of its users	Strict liability	Fault based liability
• TJPR, civil appeal 130075-8, Judge Des. Antônio Gomes da Silva, decided on November 19th 2002 • TJRJ, civil appeal nº. 2007.001.523346, Judge Des. Arthur Eduardo Ferreira, decided on January 1st 2008	• The decision was based upon the theory of the risk of business or defect in the services rendered (in case of a consumer relation). - AgRg no Resp 1325220/MG, decided on June 18th 2013, Judge Min. Paulo de Tarso Sanseverino	• For the non removal of the offensive content after being aware of its existence (usually by notification) - Resp 1193764/SP, decided on December 14th 2010, Judge Min. Nancy Andrighi; or • For the non compliance with a judicial decision to exclude the offensive contente from the internet – Resp 1568935/RJ, decided on April 5th 2016, Judge Min. Ricardo Villas Boas Cueva

Cyber attacks and civil liability

New data protection law creates the obligation to inform in case of a security breach - notification should attend the legal requirements setforth in the law

USA: nowadays almost all of the states have laws that creates an obligation on public and private companies to notify people whose data have been compromised

Very difficult to estimate the damages

The company can also be a victim

Solution:

Identify the risks, adopt the adequate security measures and create a program to prevent and respond to cyber threats

Civil liability of directors and officers in case of a cyber attack

"The director must employ, in the exercise of its duties, the care and diligence that all active men usually employs in the administration of its own business" – Companies Act and Civil Code

Corporate governance and cyber risks

The directors and officers must adopt the security and prevention measures necessary to avoid a cyber attack – the prevention begins at the top of the corporation

USA: shareholders litigation against directors and officers for failure on cyber security – the fall on the price of a stock after a breach has been revealed for example

The SEC has been demanding more detailed information about cyber security and breaches on its forms

Cyber attacks in Brazil

XP

- Data leak of 29 thousand clients accounts between 2013 and 2014.
- A file containing sensitive information from clientes such as name, social security, e-mail and phone number was sent to the victims by e-mail, in order to request money.
- The company only revealed the breach in January 2017 and said that was investigationg the facts.
- Security measure: sped up the use of tokens to acess the accounts.

Wannacry

- Encrypts user data and requires payment of a value for recovery of compromised data (ransomware).
- A security breach from Microsoft allowed the attack on many countries (over 150).
- More than 300 Thousand computers were infected and the payments made were around USD 130 mil.
- Many companies and governamental bodies were infected, including hospitals, Telefonica, Petrobrás and Courts.

Whatsapp attacks

- Mcdonald´s: The message requested to share a malicious link with 10 users in order to receive a cupom worth R$ 70,00.
- Kopenhagen: a malicious link with a research was sent and also requested that the user shared it with 10 people to get a free Easter Egg.
- Boticário: the user received a fake R$ 500,00 cupom and by clicking on the link was directioned to malicious sites.

Cyber attacks in Brazil – cont.

Banco Inter

- Data leak of clients and employees information, including passwords, revealed in May 2018.
- MPDFT filed a class action for collective moral damages against Banco Inter, asking for the payment of R$ 10 millions of indemnification, due to the fact that it didn´t take the necessary measures to assure the safety of personal data of clients and non clients. They settled for R$ 1,5 million in December.
- CVM notified the bank asking for clarifications on the matter.

Uber

- In November 2017 admitted that there was a cyber attack in 2016.
- The attack resulted on the theft of data from 57 million users and drivers all over the world, affecting 196 thousand people in Brazil.
- The company alleges to have adopted more strict measures to protect the data collected.
- MPDFT forced the company to notify all users of the breach.

Netshoes

- In 2018 it was revealed the leak of banking and personal information of approximately 2 million users.
- The company made an agreement with MPDFT to make the personal communication, through telefone to all the clients whose data was leaked on the internet.

Cyber insurance in Brazil - Coverages

- ✓ Insured and Third- Parties: civil liability for the violation of data privacy
- ✓ Costs of notifications
- ✓ Crisis management
- ✓ Cyber Extorsion
- ✓ Business Interruption of the insured
- ✓ Forensic experts
- ✓ Investigation costs
- ✓ Costs of data loss
- ✓ Lawyers fees

Cyber insurance in Brazil - Exclusions

- ✓ Intentional or malicious acts
- ✓ Negligence in the security of the computer system
- ✓ Material Damages
- ✓ Complaints due to unsolicited electronic mail (spam)
- ✓ Assets under the Insured´s custody
- ✓ Terrorism
- ✓ Contractual obligation (may be excepted in case of breach of data privacy)
- ✓ Intellectual property (there may be coverage depending on the product)
- ✓ Among others...