

# Mexico's strategy to foster cybersecurity

## Banco de México

Alejandro de los Santos  
Cybersecurity Director

Cemla  
Mexico City  
January, 2019

# 1. Today's cybersecurity environment

# Cyberattacks evolution

Today



# Lessons from recent attacks



- We are all exposed and all financial organizations and payment processors are ideal target for cybercriminals.
- Financial organizations have similar IT architectures and procedures. A cyberattack addressed to one platform is likely to work in another platform as well. It is easy and cheap to adjust a cyberattack.
- Cybersecurity should be a business concern; not just a technological issue. Besides IT tools, we need to have procedures and multidisciplinary teams to protect and react.
- The cybersecurity strategy should aim to protect final users' trust. The main goal should not be to comply with principles or regulations, but to maintain trust in the financial ecosystem.

## 2. Change in paradigm

# Change in paradigm

## Network Security



## Cybersecurity Threats



## Information Systems Security



## Information security

All the above, plus:

- Governance (ie organization, risk management, multidisciplinary groups)
- Policies
- Procedures for incident prevention, detection, response and remediation.
- Security awareness and training.
- Collaboration.





## Change in paradigm

- It is required to take actions NOW. Threats DO materialize
- We need to go beyond the borders of our institution, and consider the entire **ecosystem**, including **third-party** providers and end-users
- **Payment processors and messaging networks must be the strongest link in the chain.** In general, the FMI's information security baseline must be higher than those of other participants.

### 3. Pillars of Mexican regulation



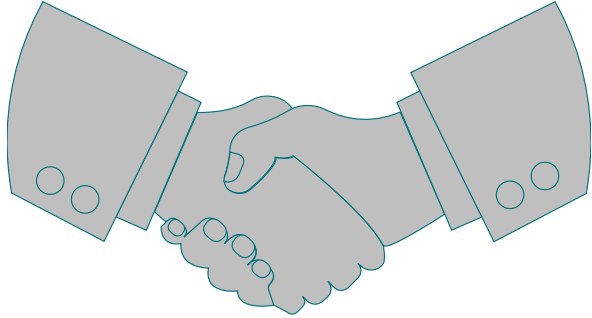
# Pillars of Mexican regulation



**Information Security Controls**



**Corporate Governance**



**Cybersecurity Response Groups**

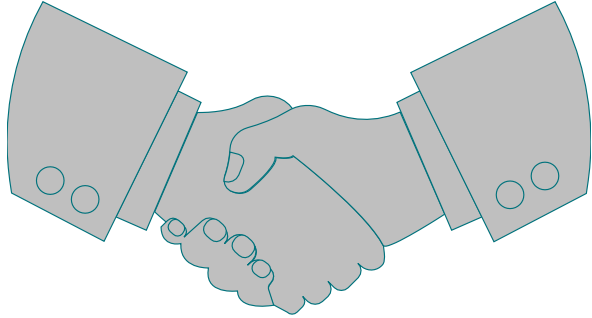
# Pillars of Mexican regulation



**Information Security Controls**

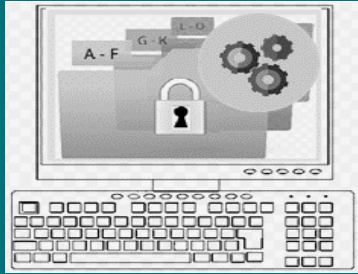


**Corporate Governance**



**Cybersecurity Response Groups**

# Information Security Controls



- *Set up and improve basic security controls in all information systems and infrastructure. Cyber hygiene.*
- *Implement practices and processes to protect the information, not the systems. Monitor transactions.*

Network  
security



- NIST SP 800-53, ISO 27001
- Financial Regulations: Banxico (SPEI, 2017-2018); CNBV (CUB, 2018)

Information  
systems security



# Pillars of Mexican regulation



Information Security Controls



Corporate Governance



Cybersecurity Response Groups

# Corporate Governance



¿.....?

## **Chief Information Security Officer:**

- **Executive officer with influence throughout the organization**
- **Responsible for the institutional strategy and protection**
- **Balance between operation and security controls**

# Pillars of Mexican regulation



Information Security  
Controls



Corporate Governance



**Cybersecurity Response  
Groups**

# Financial Authorities' GRI



## Financial Authorities' Incident Response Group (GRI)

- Alerts
- Incident communication
- Response coordination
- Recommendations to protect and contain





BANCO DE MÉXICO



## 4. Actions within the Central Bank

## Background

- In 2017, the Central Bank of Mexico hired one of the most prestigious consultants in cybersecurity issues to assess its strategy on such matter.
- The main opportunities identified to mature and improve our strategy were:
  - To expand the scope of cybersecurity to "Information Security"; making it an issue beyond the IT department.
  - To create a high-level unit in charge of coordinating Banco de México's strategical efforts to strenght Information Security. These efforts should be made aimed to the internal controls but also focus on the financial ecosystem.
- A three-year program was designed with specific task and deliverables. The new cybersecurity unit should lead the efforts.

# Cibersecurity Directorate - responsibilities

- Inside Banco de Mexico
  - Define, communicate and promote the Bank's information security strategy.
  - Create policy and regulations regarding information security.
  - Periodically evaluate the information security strategy and adjust it when necessary.
  - Coordinate the different administrative units of the Bank around the defined strategy and propose the institutional position of information security
- Outside Banco de Mexico
  - Foster information security in the financial ecosystem, considering Banco de Mexico's faculties.
  - Participate in the design and, where appropriate, issuance of regulation on information security policies applicable to Mexican financial entities.
  - Represent Banco de México on Cybersecurity issues in different forums: i) the Mexican financial system, ii) Mexican financial authorities and iii) foreign entities (financial authorities, central banks, private or public entities, etc).