Lessons and the regulator´s perspective: Mexico

Banco de México

Alejandro de los Santos
Cybersecurity Director

ACSDA - Cyber Security Workshop

Miami, FL

November, 2018

Agenda

1. Background: cyber criminals

2. Lessons

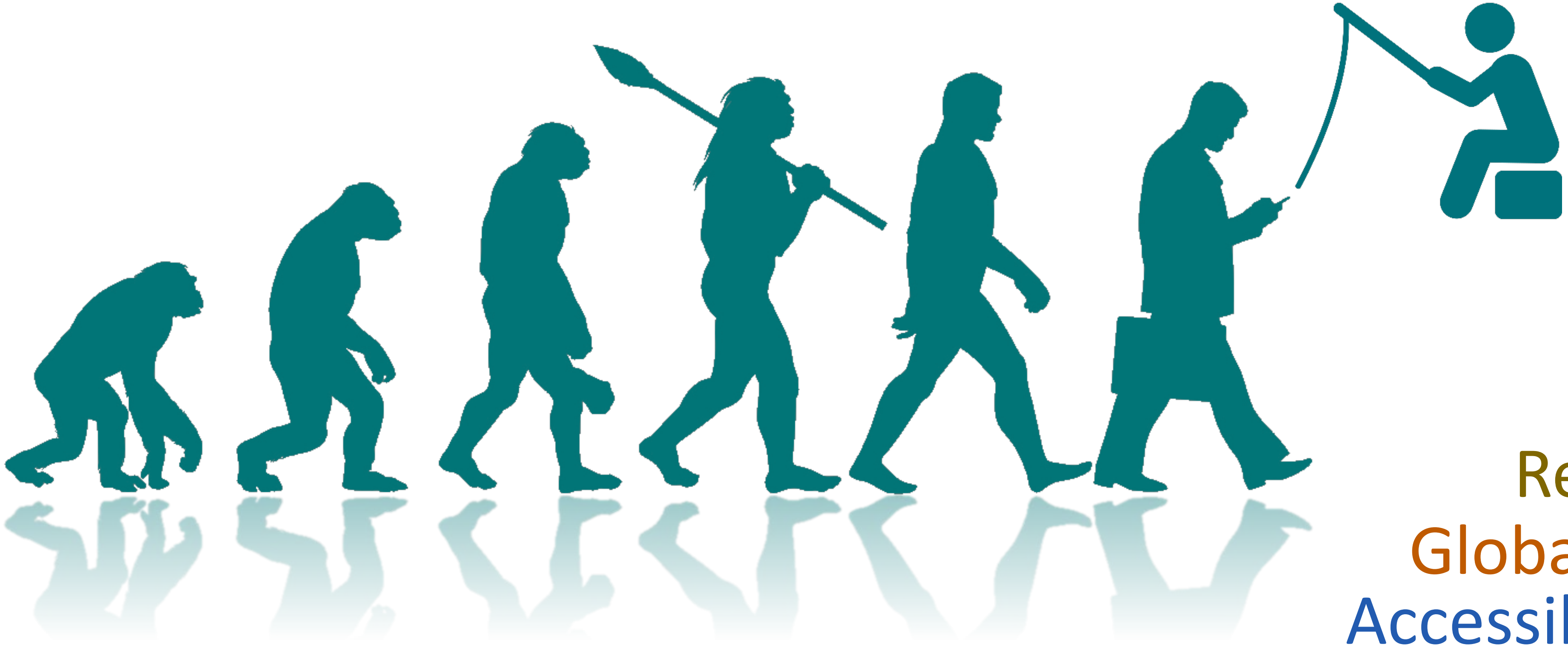
3. Change in paradigm

4. Pillars of Mexican regulation:
   - ➢ Controls
   - ➢ Corporate governance
   - ➢ Incident response

5. Final remarks

1. Background: cyber criminals

Technology evolution



Real-time

Globalization

Accessibility

Mobility

Definitions

Cyberspace

- Intangible environment, supported by Information and Communication Technologies managed by different jurisdictions, in which individuals, corporations and governments exchange information, with a global scope.

Cybersecurity

- Set of governance, technological, physical and administrative controls whose purpose is to protect the information in Cyberspace.

Cyberattacks evolution

80’s

Cyberattacks evolution

2000

Cyberattacks evolution

Cyberattacks evolution

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

- **October 2018.** Security researchers link the malware used to attack a petrochemical plant in Saudi Arabia to a research institute run by the Russian government.
- **October 2018.** The Security Service of Ukraine announced that a Russian group had carried out an attempted hack on the information and telecommunication systems of Ukrainian government groups.
- **September 2018**. The U.S. Department of Justice announces the indictment and extradition of a Russian hacker accused of participating in the hack of JP Morgan Chase in 2014, leading to the theft of data from over 80 million customers.
- **July 2018**. Researchers report that a hacking group linked to Iran has been active since early 2017 targeting energy, government, finance, and telecommunications entities in the Middle East.
- **July 2018**. Russian hackers were found to have targeted the Italian navy with malware designed to insert a backdoor into infected networks.
- **June 2018.** Ukraine police claim that Russian hackers have been systematically targeting Ukrainian banks, energy companies, and other organizations to establish backdoors in preparation for a wide-scale strike against the country.

https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

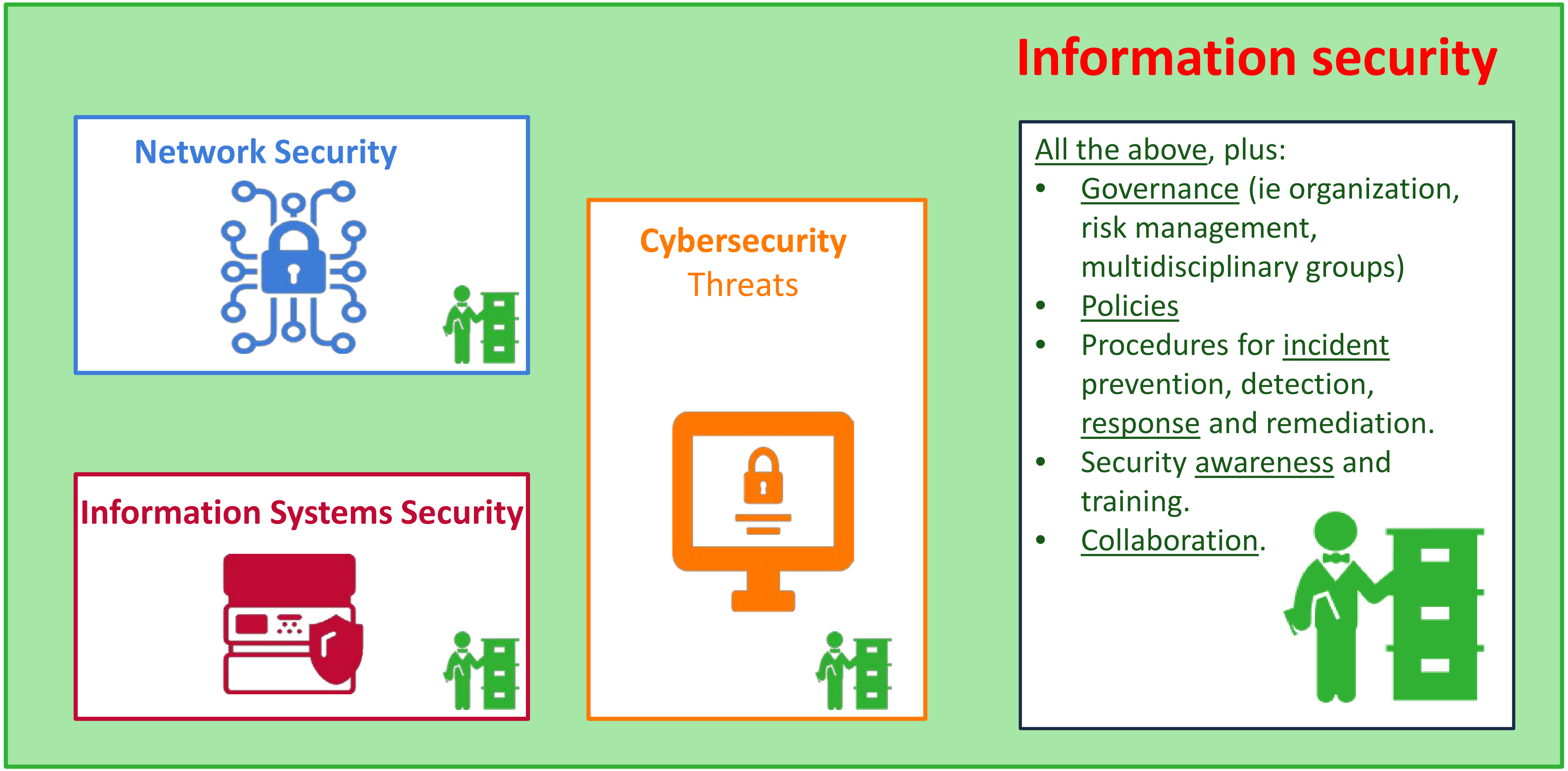
2. Lessons

Lessons

- We are all exposed. FMIs are an ideal target for cyber criminals.
- Financial organizations have similar IT architectures and procedures. A cyberattack addressed to one CSD, it is likely to work in another CSD 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 depositors´ trust. The main goal should not be to comply with principles or regulations, but to keep the trust on the financial ecosystem.

3. Change in paradigm

Change in paradigm



Information security

Network Security

Information Systems Security

Cybersecurity

Threats

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

- We need to go beyond the borders of our institution, and consider the entire **ecosystem**
- Including third-party providers and end-users
- Cybersecurity should be a concern for the entire organization.
- FMIs´ information security baseline must be higher than those of other participants.
- **FMIs must be the strongest link in the chain.**
- It is required to take actions NOW. Threats DO materialize

International Actions

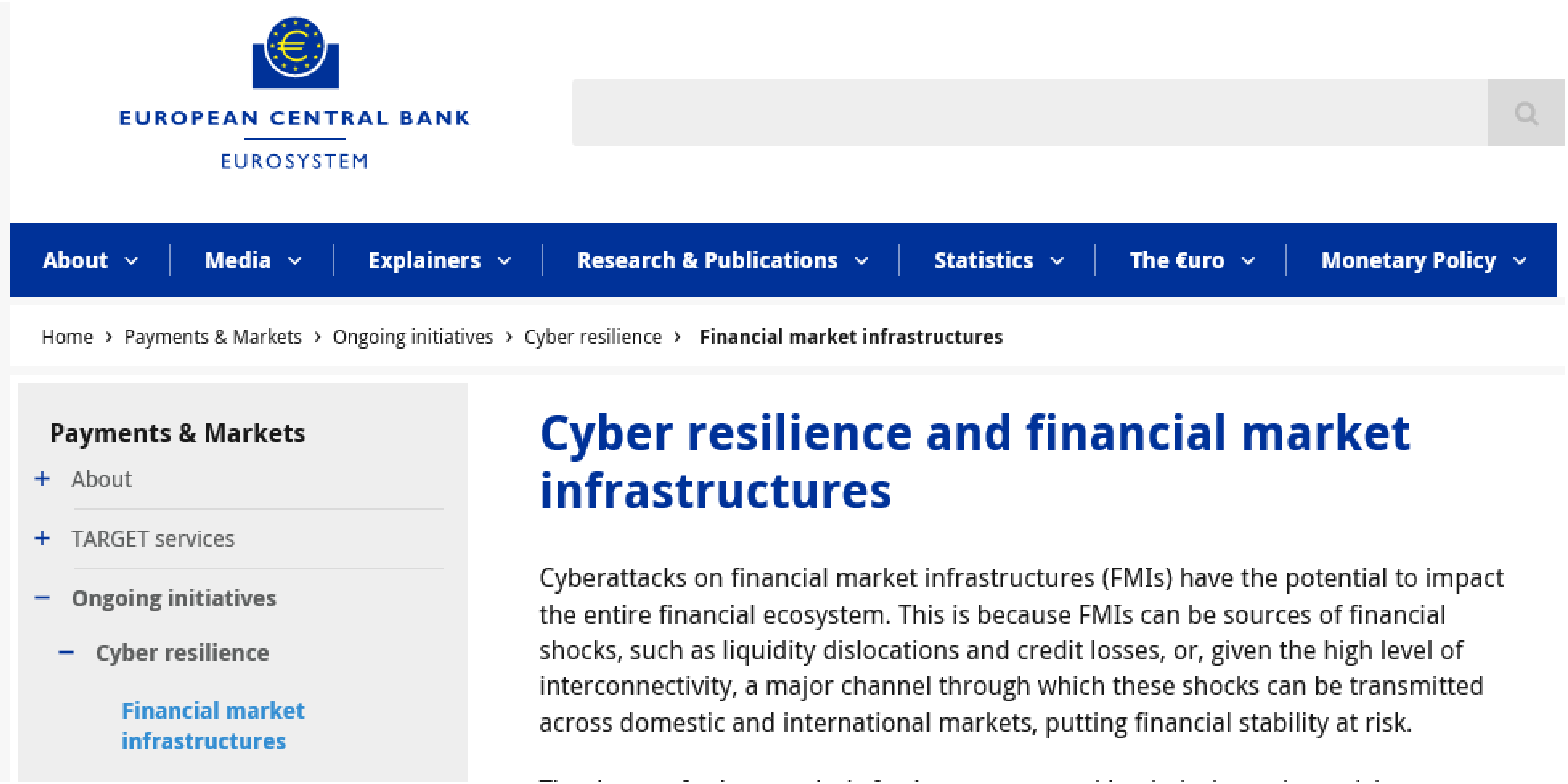
"*Guidance on cyber resilience for financial market infrastructures*" (BIS 2016)

- ***Purpose***. ... to provide guidance for FMIs to enhance their cyber resilience. Specifically, this document provides supplemental guidance to the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI), primarily in the context of governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17) and FMI links (Principle 20).

  This guidance is not intended to impose additional standards on FMIs beyond those set out in the PFMI, but instead provides supplemental detail related to the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities with the objective of limiting the escalating risks that cyber threats pose to financial stability.

https://www.bis.org/cpmi/publ/d146.pdf

International Actions

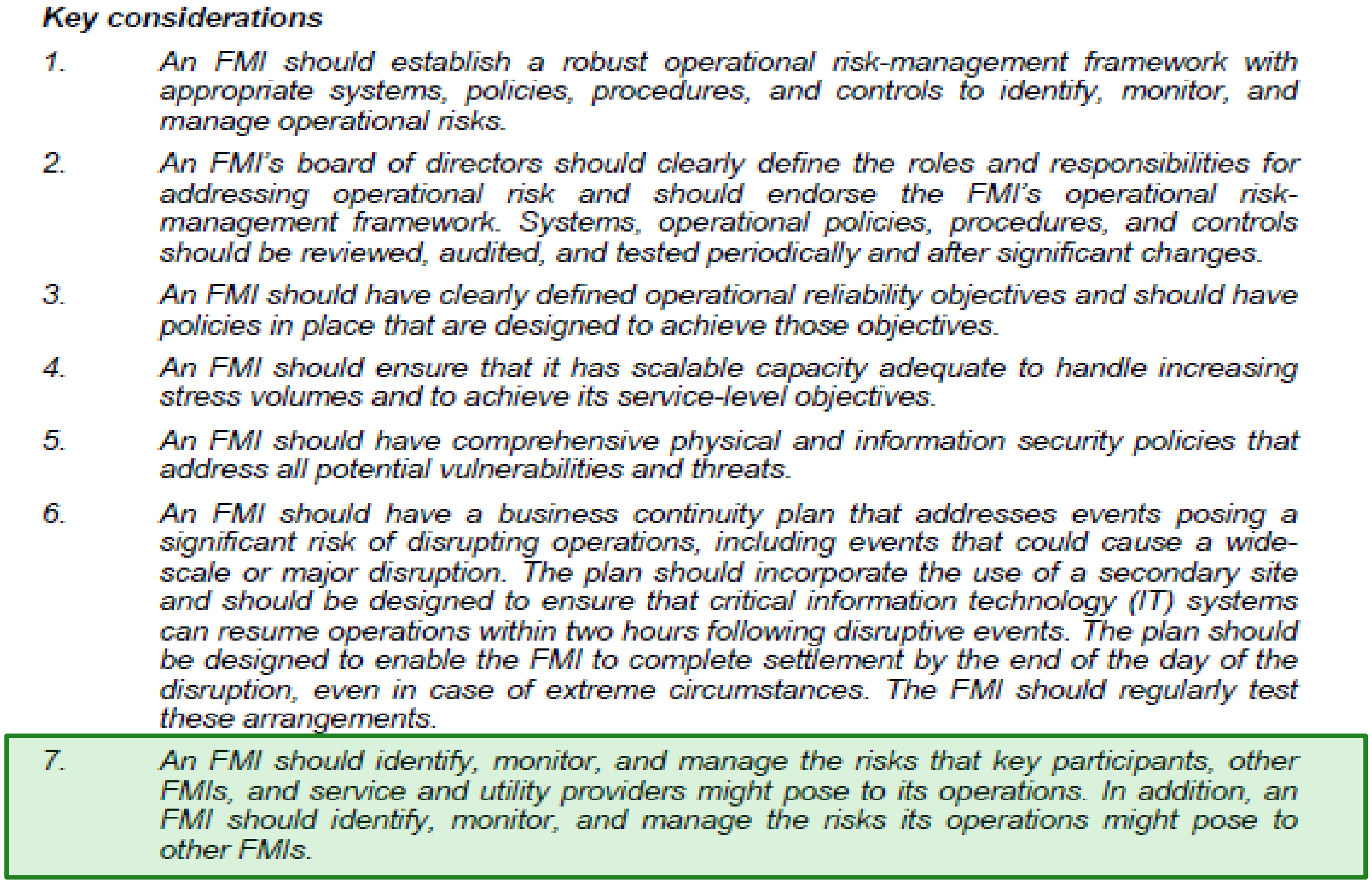


Cyber resilience and financial market infrastructures

Cyberattacks on financial market infrastructures (FMIs) have the potential to impact the entire financial ecosystem. This is because FMIs can be sources of financial shocks, such as liquidity dislocations and credit losses, or, given the high level of interconnectivity, a major channel through which these shocks can be transmitted across domestic and international markets, putting financial stability at risk.

https://www.ecb.europa.eu/paym/initiatives/cyber-resilience/fmi/html/index.en.html

Principles for FMIs



Key considerations

1. An FMI should establish a robust operational risk-management framework with appropriate systems, policies, procedures, and controls to identify, monitor, and manage operational risks.
2. An FMI's board of directors should clearly define the roles and responsibilities for addressing operational risk and should endorse the FMI's operational risk-management framework. Systems, operational policies, procedures, and controls should be reviewed, audited, and tested periodically and after significant changes.
3. An FMI should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives.
4. An FMI should ensure that it has scalable capacity adequate to handle increasing stress volumes and to achieve its service-level objectives.
5. An FMI should have comprehensive physical and information security policies that address all potential vulnerabilities and threats.
6. An FMI should have a business continuity plan that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events. The plan should be designed to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances. The FMI should regularly test these arrangements.
7. An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations. In addition, an FMI should identify, monitor, and manage the risks its operations might pose to other FMIs.

BANK FOR INTERNATIONAL SETTLEMENTS

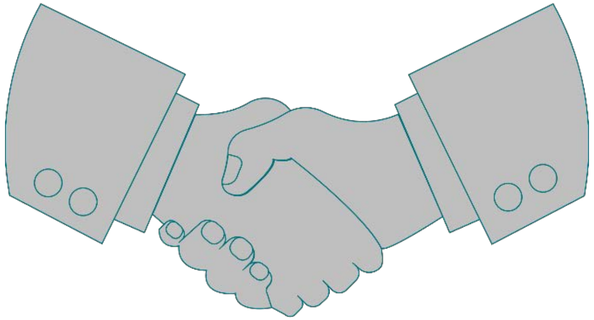
OICU-IOSCO

4. Pillars of Mexican regulation

Pillars of Mexican regulation

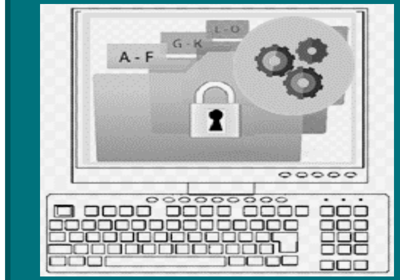
Information Security Controls

Corporate Governance



Cybersecurity Response Groups

Information Security Controls

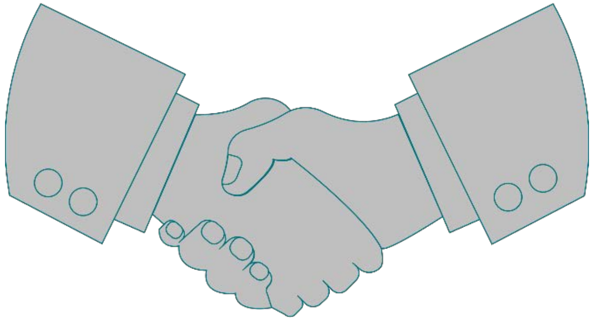


Network security

Information systems security

- ***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.***
- ***Protect personal data, as well as securities and cash records.***
- NIST SP 800-53, ISO 27001
- Financial Regulations: Banxico (SPEI, 2017-2018); CNBV (CUB, 2018)

Pillars of Mexican regulation



Information Security Controls

Corporate Governance

Cybersecurity Response Groups

Corporate Governance

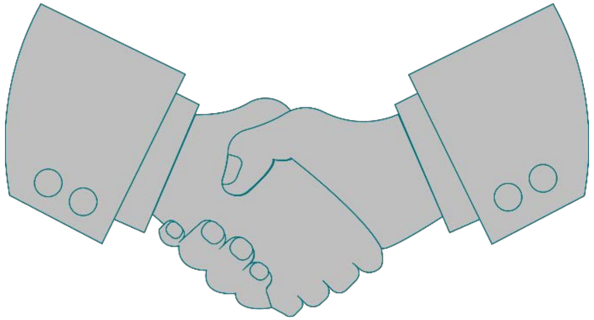
Chief Information Security Officer:

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

Pillars of Mexican regulation

Information Security Controls

Corporate Governance



Cybersecurity Response Groups

Financial sector agreements

Bases de Colaboración en Materia de Seguridad de la Información – Autoridades, Asociaciones, PGR

(24 de mayo de 2018)

1. Mejor coordinación en el sector, compartir alertas y dar respuesta a incidentes
2. Las autoridades deben determinar qué principios de seguridad de la información deben incluir en sus respectivas regulaciones
3. Además, deben dar un tratamiento homogéneo a los requisitos y prácticas que las Entidades tendrán que observar
4. Se deben definir protocolos y responsables para atender incidentes de seguridad

Principios de reforzamiento de la seguridad de la información – CESF

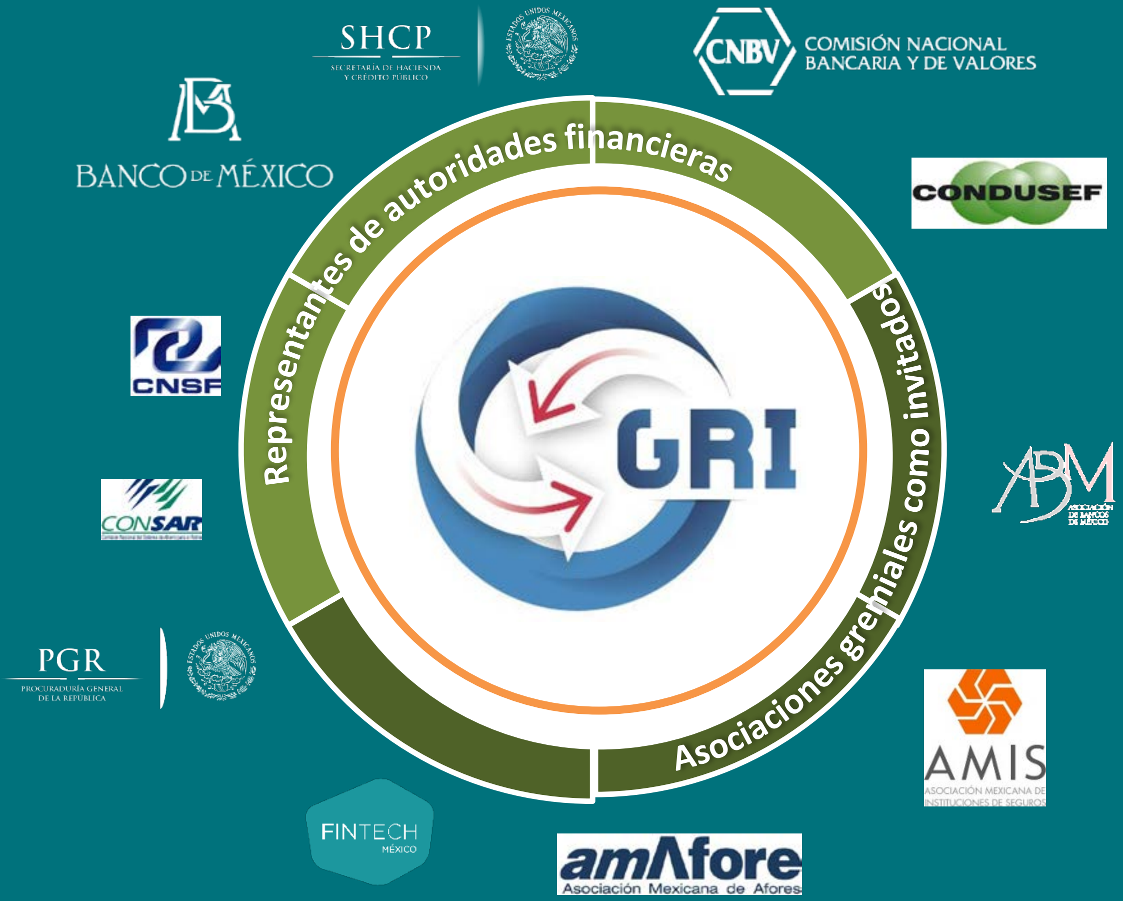
(14 de junio de 2018)

1. Gobierno corporativo en el que la seguridad informática ocupe un
2. Esquemas de protección de datos robustos
3. Administración de riesgos de seguridad de la información
4. Controles de seguridad en los puntos de acceso
5. Protocolos de respuesta a incidentes
6. Identificación de exposición a riesgos por parte de terceros
7. Políticas de protección a la infraestructura
8. Políticas de protección a los sistemas
9. Programa de capacitación y de fomento de una cultura de la
10. Programas de educación y fomento de una cultura de seguridad uso que hacen los clientes de los servicios financieros

Financial Authorities´ GRI

Financial Authorities´ Incident Response Group (GRI)

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


SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO
CNBV
COMISIÓN NACIONAL BANCARIA Y DE VALORES
BANCO DE MÉXICO
CONDUSEF
Representantes de autoridades financieras
CNSF
GRI
CONSAR
Asociaciones gremiales como invitados
ABM
ASOCIACIÓN DE BANCOS DE MÉXICO
PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA
AMIS
ASOCIACIÓN MEXICANA DE INSTITUCIONES DE SEGUROS
FINTECH
MÉXICO
amafore
Asociación Mexicana de Afores

5. Final remarks

Final remarks

- Cybersecurity is not just an IT issue. It should be everyone´s concern within the organization.
- We need a new paradigm that puts information in the center: *information security*
- The protection strategy should not be constructed just to comply with standards and regulation.
- FMIs cannot afford being the example of a successful cyberattack. The economy and stability of the country would be in jeopardy.

Final remarks

- FMIs are the pillars of the financial system, its services must be strong and resilient to cyberattacks.
- A hit on a CSD is a hit on the heart of the financial ecosystem. Cybersecurity should not be seen as a regulatory issue.
- Cybersecurity for FMIs is not optional. It should be on the top of the CSD´s priorities keeping the ecosystem safe!

asantos@banxico.org.mx

BANCO DE MÉXICO