Cyber risk related to the Insurance and Surety Sectors

Norma Alicia Rosas Rodríguez,
Former President of the CNSF,
Mexico

Seminario Astin AFIR
IAA, Mexico City
December 3, 2018

CONTENTS

- Cyber risk
- Attacks in the insurance sector
- Managing cyber risks and insurance products
- Cyber security regulation
- Challenges

Cyber risk

"Any risks that result from the use of electronic data and its transmission, including technological tools such as the Internet and telecommunication networks".

Cyber incidents are: physical damage, fraud caused by improper use of data, responsibility for data storage, as well as availability, integrity and confidentiality of information (individuals, industry and governments).

Cyber risk is considered one of the main risks regarding its probabilty as well as its impact. At the same time, threats materialize by directed attacks and by the deficiencies in the protection of systems.

The financial sector as a whole has been a preferred target of these attacks.

Source: Chief Risk Officers Forum, "Cyber resilience Paper"

Cyber risk

Global Overview of Risks, 2018, WEF

10 main risks

In terms of probability

1. Extreme weather events
2. Natural disasters
3. **Cyber attacks**
4. **Fraud or data theft**
5. Failures in mitigation and adaptation to climate change
6. Involuntary large-scale data migration
7. Environmental disasters caused by man
8. Terrorism
9. Illicit trade
10. Asset bubbles in a main economy

In terms of impact

1. Massive destruction weapons
2. Extreme weather events
3. Natural disasters
4. Failures in mitigation and adaptation to climate change
5. Water crisis
6. **Cyber attacks**
7. Food crisis
8. Loss of biodiversity and collapse of the ecosystem
9. Involuntary large-scale data migration
10. Propagation of infectious diseases

Cyber attacks on a large scale: cyber attacks on a large scale or malware that cause huge economic harm, geopolitical tension or general loss of trust in the Internet.
A massive occurrence of fraud/theft of data: Improper use of personal or official data that happens at a very large scale.

Source: Global Risks Report 2018, WEF[1].

Cyber risk

Threats

5 cyber security threats expected for 2018

1. Internet IT services under threat.
2. Vulnerability of the IOT.
3. Practices of cyber criminals even more harmful.
4. Silence of the investigators of cyber security.
5. Deficiencies of the IT Department.

Statistics on Cyber risk in 2017

WANNACRY

Affected 300,000 computers in more than 150 countries

EQUIFAX HACK

143 millions of social security numbers compromised in the USA

MALWARE

230,000 malware models are developed every day

RANSOMWARE

4,000 daily ransomware attacks in the world

RANSOMWARE ATTACKS

Ransomware increased up to 36%

E-MAILS

1 in every 131 emails contains a malware

"Warren Buffett defines cyber attacks as the biggest threat for humankind, even more severe than nuclear weapons"

Source: Incognito Forensic Foundation.

Cyberrisk.- How it is evolving…

4 types of cyber enemies

Cyber activists
They act on behalf of a cause

Criminal Organizations
Benefit from malicious activities

Terrorists
Aprovechan el ciberespacio para reclutar

Nacional States
Pursue their national interests

Because of these actors, cyber risk is now:

More space
The surface prone to attacks increases exponentialy

The volume and diversity of the interconnected elements, increase the complexity.

More frequent
The volume of malicious cyber activity is increasing

Low entry barriers and high rentability are an incentive for the actors.

More dangerous
Actors are migrating towards more destructive activities

Critical infraastructure turns into the center of the attack

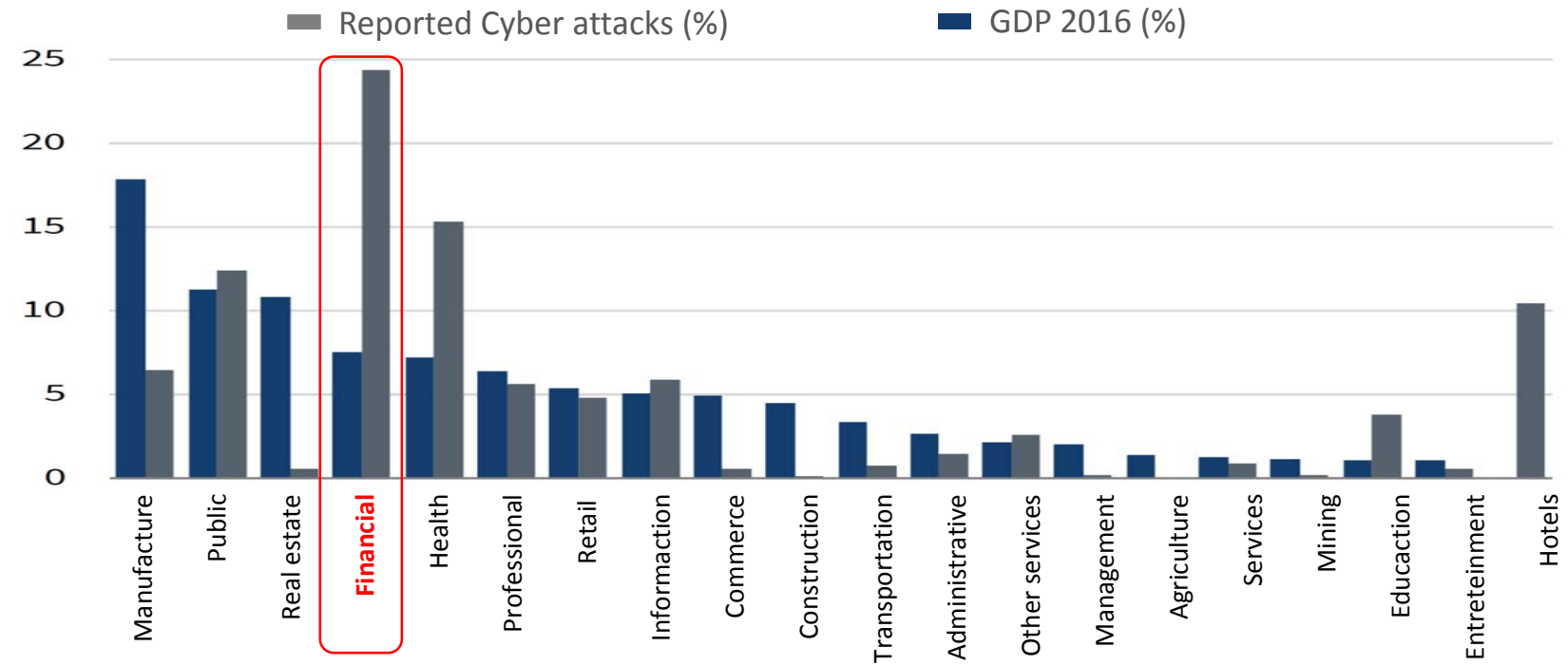
More disruptive
Potential impacts of a cyber attack are increasing

The high digital dependency increases vulnerability of society

Source: CYBER THREAT Alliance

Cyber Risk

Cyber attacks and the financial sector



Source: The Council of Economic Advisers (2018) The cost of malicious cyber activity to the U.S. economy.

Attacks to the insurance sector

- On January 27 2015, **Anthem Blue Cross Blue Shield** y **Premera Blue Cross** (USA) suffered a **data breach** (credit cards and social security data) that compromised the information of **90 millions of customers** (78.8 million of Anthem and 11 million of Premera). The **cost** for Anthem was of **USD 375 million** (260 in improvement and security and 115 in customers´demands).

- The "**DD4BC**" group has blackmailed finacial institutes (Europe, Australia, Canada and USA), with **Distributed Denial of Service (DDoS)**. The amount of the ransom varied accordingly and was to be made in bitcoins. Two German groups were attacked this way in the mids of 2015, haveing received threats of an DDoS attack to the company unless they paid 40 bitcoins. (The insureres denied the payment, becuase they evaluated that they would have only caused minor damage).

- Another important insurance company anounced a **violation of the data of their IT systems de los datos de sus sistemas** in 2015, that affected **1.1 millions of members**. The insurer notified each one of the affected memebers of the violation and offered a free credit control and protection against theft.

- In 2015, **penetration testing** (realized by an internal audit team in a French insurance company) discovered that here had been **an unauthorized access to the accounting tools**.

Source: IAIS, KPMG y EY

Attacks to the insurance sector

- In the Netherlands, an insurer suffered a "***hack CEO***", a specific form of *"phishing"*, where the CEO of an important and well known client was impersonated and the criminals tried to **persuade the employees to transfer money to a certain account**. They had apparently researched certain operational details of the insurer.

- A health insurance in the USA suffered a cyber attack in July 2016 that compromised two separate data systems and exposed **confidential information of 3.7 million** of customers and medical care providers (social security numbers, claims, payment data – name, number and dates). At least, **a collective lawsuit** has been made after this data breach.

- In 2017, Anthem informed that **data of 18,500 clients** had been compromised.

- On that same year, BUPA suffered a **filtration of information** that affected **500,000 clients** of their international insurance plan.

Source: IAIS, EY e Insuranceblog Accenture

Cyber risks management and insurance products

Cyber security framework

1 Identify

Diagnostic: Profil of threats, risk exposure and expected losses.

2 Protect

Increase of internal security and of 3rd parties.
Intern patches and to 3rd parties to guarantee security and functionality of the environments.

3 Detect

Evaluation of the security performance.
Periodical scanning of **vulnerability.**
Cautious **evaluation** of the digital infrastructure and defence of the organization.

4 Respond

Capacity of responce to incidents in scenaries of threat.
Dynamic **Simulation** of a threat to evaluate the preparation and efficiency of the response to the incident.

5 Recuperate

Beginning of **plans of action and movilization** of resources to amend a cyber incident

Source: CPMI-IOSCO

Cyber risks management and insurance products

Cyber Insurance

Insurance role

It works as a point of contact for an organization to evaluate its cybernetic practices and coordinate its response plan to cyber incidents.

Reimburse a company's costs for responding to a cyber incident.

Cover fees and damages in response to litigation for a cyber incident.

Reimburse income or expenses for interruption, related to a cyber incident.

Types of Coverages

- Confidenciality
- Security
- Costs by response to incidents
- Digital Responsability
- Cyber Blackmail
- Loss of Data
- Business interruption

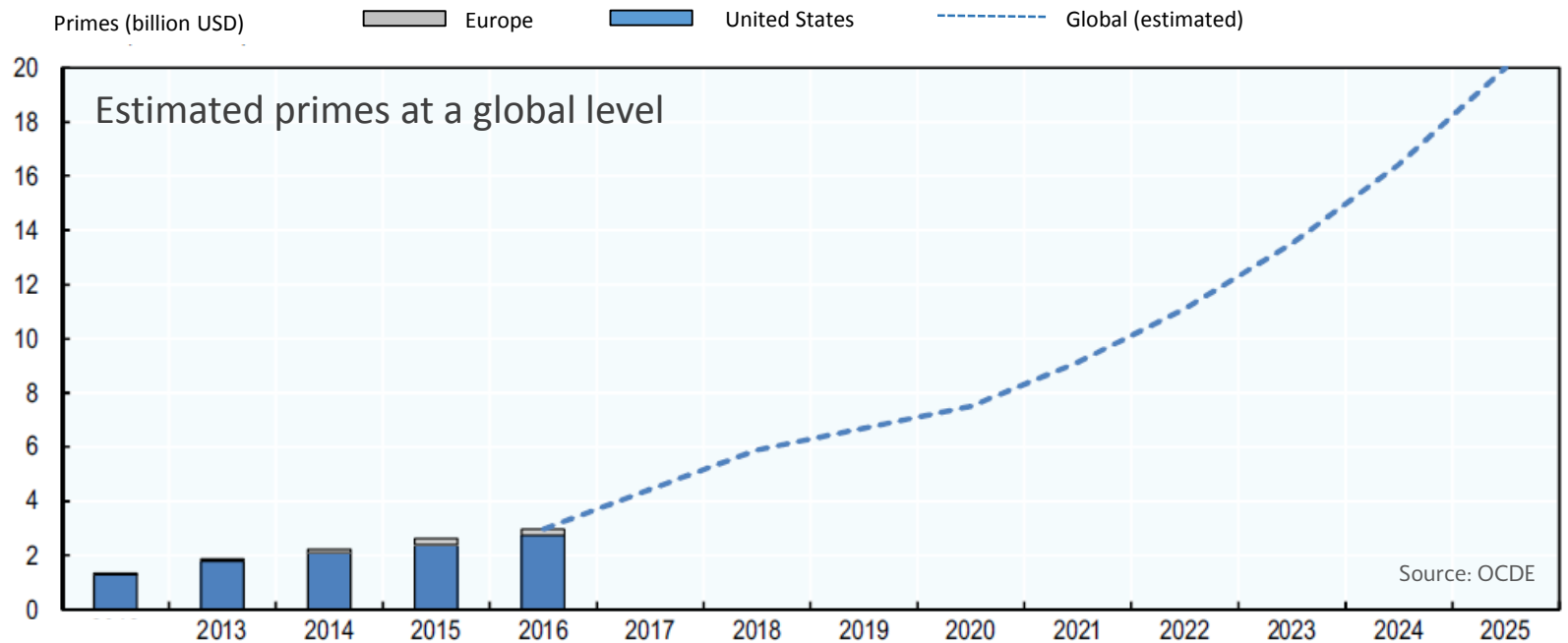
- •Defense expenses
- •Legal responsibility
- •Defense expenses related to regulation
- •Confidentiality about fines / sanctions

- •Malicious acts
- •Malware
- •Hacking
- •Unauthorized access
- •Programming error
- •Human error
- •Power failure

Cyber risk management and insurance products

At an international level, the insurance market against cyber risks is still young:

- In 2016, the estimated market was between USD 3 y 3.5 billion.
- The USA have 85%-90% (dominated by 20 insurers) and Europe has 5-9%.
- It is expected that for 2025 the market will reach USD 20 billion.
- This number is small if compared to other branches (Fire in OCDE countries was of USD 277 billion in 2015).



Cyber risks management and insurance products

- In Mexico, 8 insurance companies offer products related to cyber risk, either as ad-hoc products or with additional coverages to other products.

Insurance Institution	Name of the insurance product	Coverages
Grupo Nacional Provincial, S.A.B	GNP Cyber Safe	Insurance Data Coverage Coverage of Loss due to Interruption of Activities.
Zurich, Compañía de Seguros, S.A.	Data protection insurance and computer security (Data Protect)	Civil Liability related to personal and corporate data, expenses for security breaches, defense and sanctions, loss of income, replacement or replacement costs of digital activities, civil liability derived from content on the Web page and reputational costs of the insured business.
Chubb Seguros México, S.A	Cyber Personal Protection package	Misuse of bank cards by theft, assault, loss; falsification and / or physical adulteration of the card; fraudulent cyber shopping or by phone.

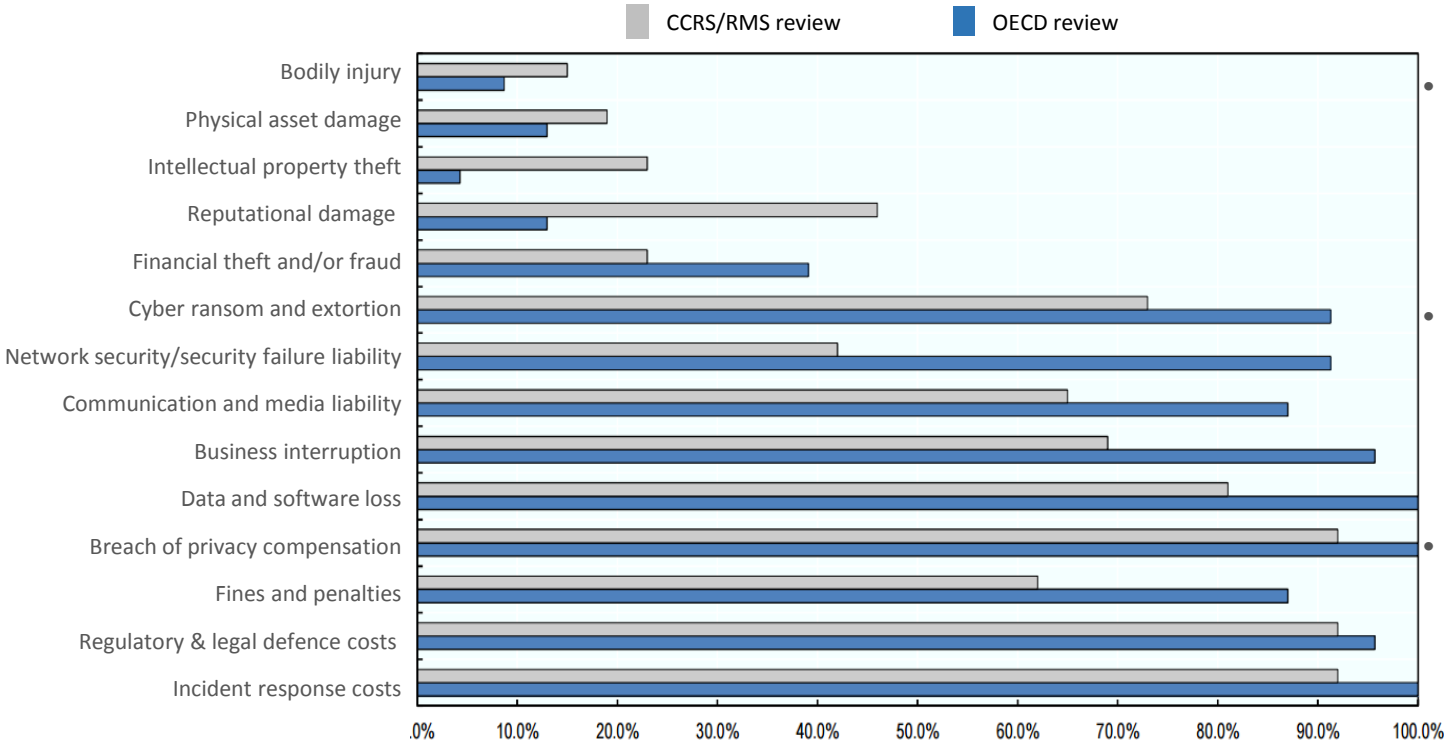
Cyber risks management and insurance products

Insurance Institution	Name of the insurance product	Coverages
Zurich Santander Seguros México, S.A.	Super Shield with Identity Theft	Coverage for fraud, theft or credit or debit card loss.
QBE de México Compañía de Seguros, S.A. de C.V.	Financial Protection Insurance	Identity theft Coverage against phishing
XL Seguros México, S.A. de C.V.	Professional Civil Liability	Sanctions on data protection
AIG Seguros México, S.A. de C.V.	Data Protection Insurance	Personal data liability Corporate data liability Data security liability Outsourcing company liability
Ace Seguros, S.A., actualmente, Chubb Seguros México	Cyber Risk Management Policy	Privacy liability Network security liability Electronic content liability Loss of digital assets Business interruption

Cyber risks management and insurance products

- There are important gaps between coverage and the risks to be covered (physical and reputational damage, liability, fraud, etc.)

Costs commonly covered in special policies



- Coverages vary between each insurer (CR vs. third parties, own damages).
- The policies are "customized" according to the needs of the insured (business majority).
- There are "gaps" between the coverages and the risks to cover.

Source: OCDE

CNSF cyber risk management

- In order to preserve the confidentiality, integrity and availability of the information handled by the CNSF, an Information Security Management System (SGSI) certified under the international standard ISO / IEC 27001: 2013 has been implemented.

Source: OCDE

Cyber risk regulation

International Overview

In October 2017, the "FSB summary report on financial sector cybersecurity regulations and supervisory practices" concluded that:

- The **regulatory iniciatives** are mainly oriented to an evaluation of risks, reports to the regulator, the role of the administrative counsel, servicies with 3rd parties, systems to control the access to information, recovery actions after incidents and testing of protection systems.

- **Supervision iniciatives** are oriented to the review of documentation (i.e. the procedure of risk management), to the review monitoring programs, testing and audit, review of response mechanisms to incidentes, etc.

The IAIS in 2016 published the "Issues Paper on Cyber Risk to the Insurance Sector" that explores the challenges related to regulation and supervision of cyber risk in the insurance companies. In addition, it is preparing a document, that will be out for public consultation this year, and it will provide the guidelines to develop supervision frameworks for cyber risks.

Cyber risk regulation

National Overview

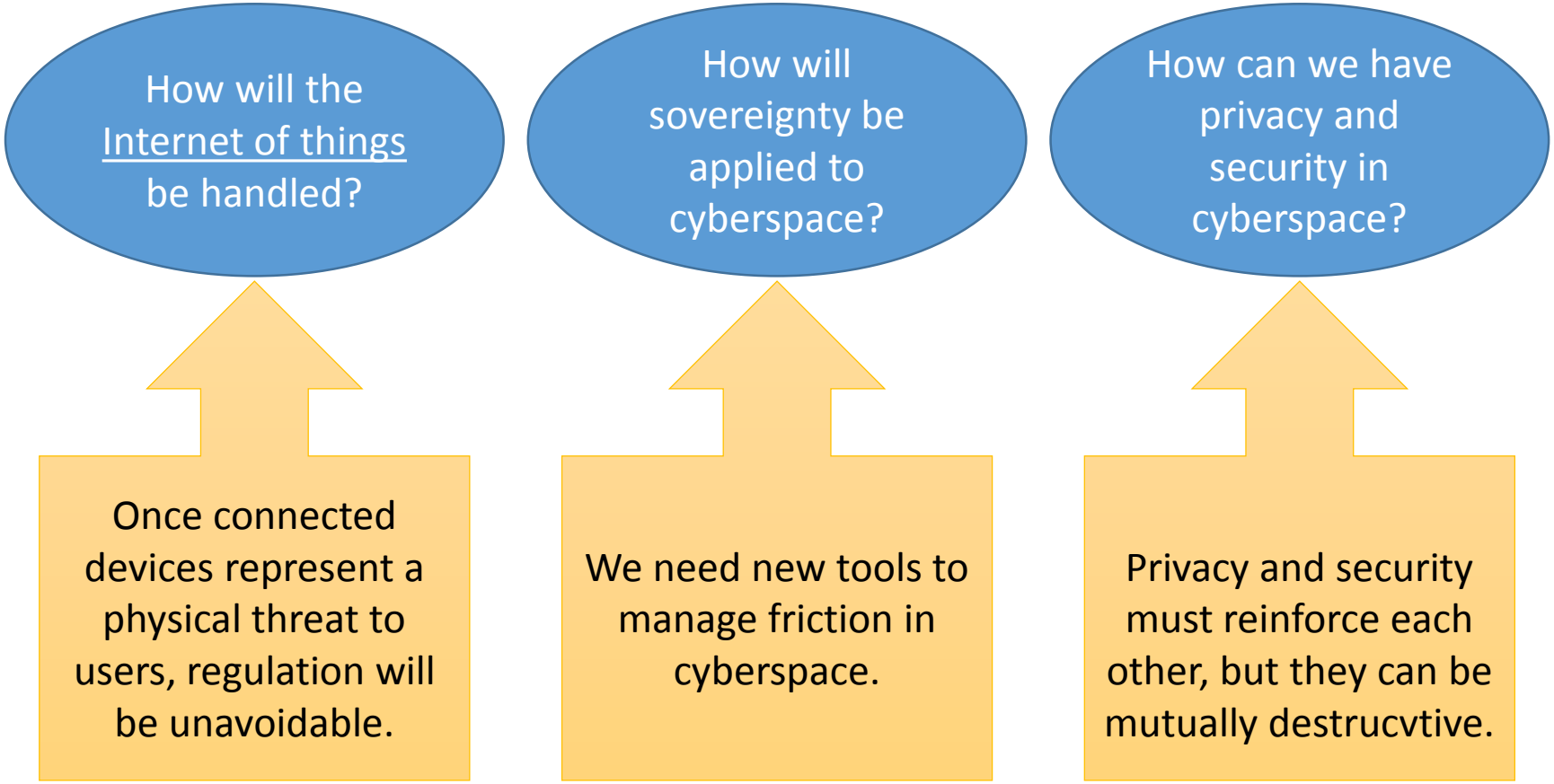
- In December 2013 the LISF (Law of Institutions of Insurance and Surety) was promulgated and it came into effect on April 4, 2015. It proposes a new model of solvency based on a better identification, measurement, mitigation, control and prevention of all different risks to which insurance institutions are exposed, **being one of them cyber risk.** (art. 235).
- On the other hand, article 69 of the LISF, points out that institutions have to establish a **system of corporate governance** that should define an integral management system considering:
  - Politics and procedures for risks management, setting specific methodologies for its measurement, auto evaluation of risks and institutional solvency (ARSI) evaluating the levels of exposure to the different types of risks and the contingency plans. The CNSF over the last two years has been focusing on supervision tasks **to verify the correct setting up** of this system. Especially:
  - **Verifying** that the institutions **count on an efficient and permanent system** of corporate governance that considers an adequate risk management; that they **perform the ARSI periodically,** (detecting risks and generating contingency plans), verifying in certification and authorization visits **the adequate functioning of the security systems and their security.**

Cyber risk regulation

- Insurance and Surety companies in their operations are **prone to cyber risk because**:
  - **Main accounts** with credit institutions to collect primes and to pay losses, **investment and keeper managament** for their investments, **operations with counterparties** (loans, reinsurance, etc.), **confidential data bases** (information of customers and users, doctors, financiers, etc.).
  - **Operations with clients thorugh electronic ways** → Respecting this, Chapter 4.10 of the CUSF points out the authentification mechanisms of clients and Art. 4.10.16 states that : "The institutions and mutual societies that use electronic ways to carry on operations and services, ***should implement security mechanisms for the transmission, storage and information processing*** to avoid revealing the information to third parties."
- The results of having signed the **Bases of Coordination in Security of the Information are**:
  - **Strenghthen the law** to set requirements for reporting in **Security of the Information**.
  - Establish the coordination within the **organizations for an integral strategy** in Cyber security.
  - Generate the **regulatory framework** for the correct **implementation of the bases**.

The future of the Cyber security regulation…

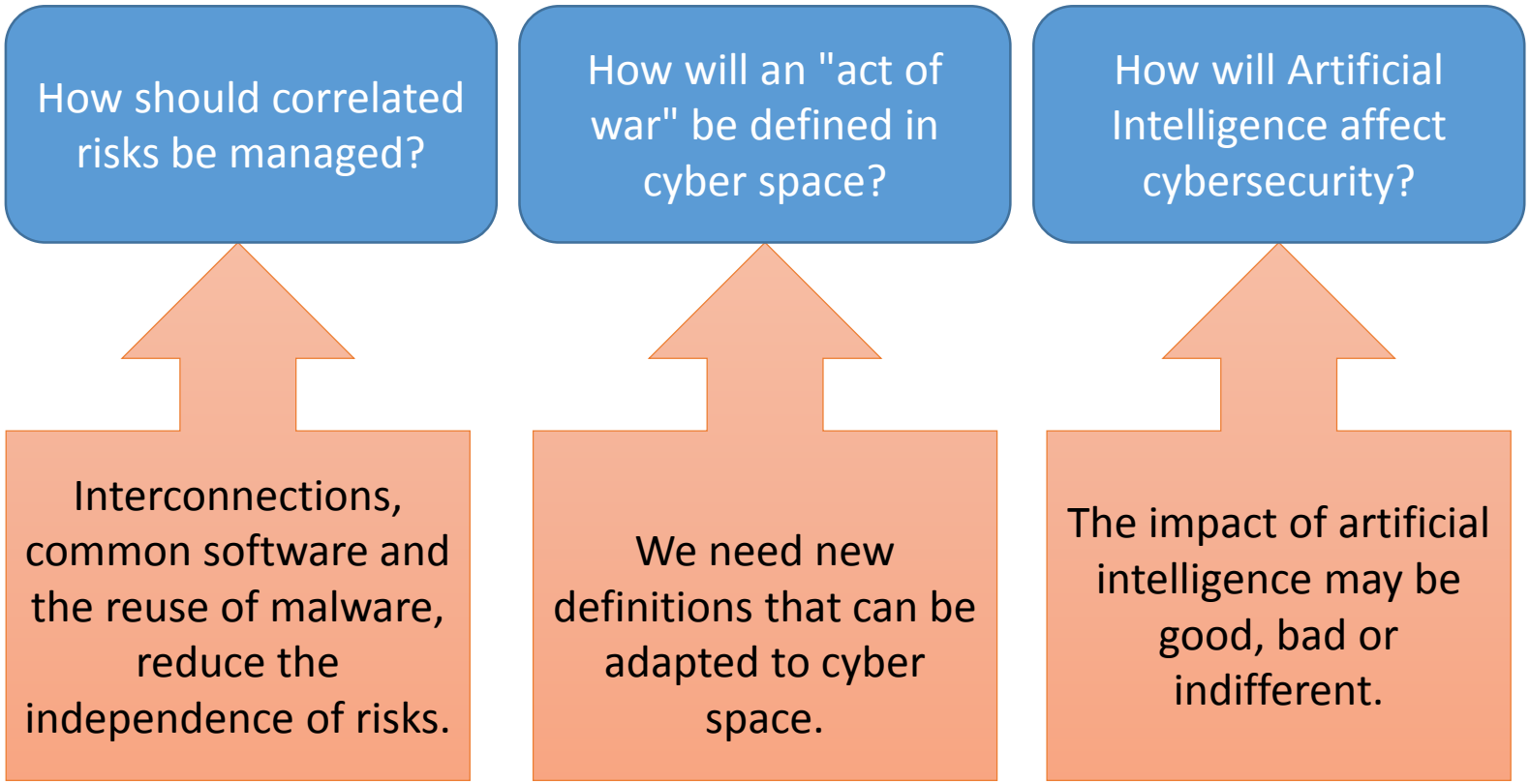
Elements that will drive public policies regarding cyber security…



Fuente: CYBER THREAT Alliance

The future of the Cyber security regulation …

Elements that will drive public policies regarding cyber security…



Fuente: CYBER THREAT Alliance

Challenges

- Implement a regulation-supervision cyber security framework for the financial sector.
- Design specific supervisory practices to identify, measure and possibly calculate the capital requirement necessary to face cyber risks (at the international level, cybersecurity is already talking about cyber stress testing). Also, to establish specific areas of supervision.
- Separate cyber risk from operational risk, for better management and supervision.
- Include the report of cyber incidents as part of the systematic regulatory reports, both for the protection of the financial sector and for future risk modeling.
- Promote the exchange of information between financial sector authorities both nationally and internationally.

Cyber risk related to the Insurance and Surety Sectors

Norma Alicia Rosas Rodríguez,
Former President of the CNSF,
Mexico

Seminario Astin AFIR
IAA, Mexico City
December 3, 2018