European Insurance and
Occupational Pensions Authority

Keynote speech

by Gabriel Bernardino, Chairman, European Insurance and Occupational Pensions Authority (EIOPA)

at the 3rd Annual FinTech and Regulation Conference

on "Taking innovation to the next level"

on 26 February 2019 in Brussels

Cyber Security and Cyber Risk: A universal Challenge

Good afternoon to everybody,

In the conference programme, the topic of my speech reads *"Innovation in the European Insurance Industry".*

Technological innovation is disruptive in particular for the insurance industry. However, at the same time, it drives growth through new business models, which require the new skills, proper governance and oversight.

Cyber security and cyber risk both topics are very high on the agenda of any organisation and its management. Therefore, I will share my reflections how I see the situation, what EIOPA is doing and what should be done to cope with the challenge at a global level.

Cyber security and cyber risk posing significant risks to people, businesses and the insurance industry in particular.

The digital transformation of how we work, live and do business has created huge opportunities for innovation and efficiency. However, our increased dependency on digital technologies also carries information security and privacy risks.

These risks affect the insurance sector on two levels:

- First, the security of the insurance business itself, and
- Second, its role in covering and managing cyber risk.

Technology and innovation are fundamental to the development of new business models in the insurance industry. The growing use of huge volumes of personal information makes insurance companies a prime target for cyber-attacks, which according to international data, are growing rapidly, both in number and in sophistication.

A new European data privacy regulation came into force and it is the world's most advanced legislation of its kind. It sets an extremely high standard for all organisations that handle personal information, imposing substantial penalties when requirements are not met and information is compromised.

All insurance market stakeholders must therefore be aware of the additional responsibilities stemming from this regulation and must do their utmost to implement processes to ensure that the information they hold is well protected.

Appropriate insurance can make a valuable contribution to managing cyber risk currently faced by businesses and organisations. A well-developed cyber insurance market can help:

- To raise awareness of businesses to the risks and losses that can result from cyber-attacks
- To share knowledge of good cyber risk management practices
- To encourage risk reduction investment - by establishing risk-based premiums
- To facilitate responses to and recovery from cyber-attacks

Coverage of cyber risk by insurers is still in its infancy. Most of the market is concentrated in the United States. Growth in this market, however, has been significant. With current forecasts suggesting that, premiums may reach USD 20 billion in 2025.

An aspect generally regarded as essential for the further development of cyber risk insurance in the United States is mandatory notification of regulators and data subjects of incidents in which financial information or personal health data are stolen. These situations may also give rise to heavy penalties.

With the entry into force of the data protection regulation in the European Union, it is now mandatory to notify data protection supervisors where there is a risk to the rights and freedoms of the individual. It is mandatory to notify the individuals affected if the risk to them is considered as high. There is also the possibility of fines, if data breaches are deemed to be intentional or as a result of negligence.

The future demand for coverage of this kind will depend, to a large extent, on both the frequency of high profile cyber incidents and legislative developments in relation to personal data protection.

In this context, the implementation of the data protection regulation in the European Union may lead to significant growth in cyber risk insurance, with estimates suggesting that there may be parity between the EU and US markets in coming years.

An OECD study shows that the most common type of coverage is compensation for incident response costs and privacy breaches, data and software losses and business interruption.

Cyber risk insurance also normally provides policyholders with access to experts who can assist them in responding to incidents. This can include access to investigators who assess the extent of unauthorised intrusions, and the provision of legal advice on how to 'go public' about the incident and possible public relations strategies to minimise the reputational impact.

Some of the most important corporate needs, such as coverage for reputational damage or intellectual property theft, are rarely included in cyber risk insurance.

Research highlights two principal barriers to the broader development of insurance of this type:

- Firstly, the lack of consistent historic information on the frequency and severity of cyber incidents, and
- Secondly, the constant evolution of cyber attacks.

These factors hinder the development of sound actuarial risk and cost assessment techniques, leading the most prudent insurance and reinsurance companies to set exclusions and limits to control their risk exposure. In terms of supervision, this is a sound and prudent approach.

An additional concern for the supervisory authorities relates to the potential for accumulated losses arising from an incident that affects a significant number of policyholders. Examples generally cited are the exploitation of weaknesses in mass-use software and an attack on one of the leading cloud computing services.

Cyber attacks against financial institutions have increased in frequency, complexity and sophistication, with potentially systemic impact. The motivation for such attacks, which have tended to focus on financial gain, is moving towards critical infrastructure disruption, which can undermine confidence in the financial system and financial stability itself.

Given the ongoing geopolitical turbulence, coupled with rapidly changing technological innovation, many observers believe that a large-scale cyber-attack is just a matter of time.

Expert opinion in this regard is that the attack with the greatest systemic potential will involve critical data manipulation. There are three reasons for this, all relating to difficulties:

- In detection: One cyber security enterprise estimates that it takes an average of 146 days for a company to detect an intrusion
- In response, particularly in highly interconnected systems such as payment processes
- In recovery, since analyses and diagnoses of data manipulation situations can be extremely complicated and lengthy

Therefore, this is a potential systemic risk, requiring thorough assessment and mitigation.

In my opinion, the nature and scope of cyber risk suggests that a global strategy must be developed to prevent and manage these risks. Such a strategy must consider the important role the insurance sector can play in risk management.

One of the major challenges concerns the definition of a consistent, harmonised taxonomy that enables information on cyber incidents and the associated losses to be compiled. This challenge can only be met through the joint efforts of public and private organisations, preferably at global level.

Let me now explain **EIOPA's activities** in this field.

EIOPA has been monitoring developments in the cyber insurance market for some time.

Last year, we published a report called 'Understanding cyber insurance' based on a structured dialogue with insurance companies across Europe.

Through this dialogue, we identified a number of issues relevant to the cyber insurance market in Europe such as:

- There is a **clear need for a deeper understanding of cyber risk**, on both the supply and demand side, for the European cyber insurance industry to develop further. This relates not only to the assessment and treatment of risks in new cyber insurance propositions, but also to an understanding of a client's own needs.
- In terms of products and services, **coverage is mainly focused on commercial business**. However, interest in cyber insurance for individuals is growing as digital technology becomes more and more part of people's lives.
- The cyber insurance industry **expects a gradual increase in demand for insurance, mainly driven by new regulation, the increase in cyber risk related incidents**, increased awareness of risks and the increased frequency and severity of cyber attacks.
- Qualitative models are used more frequently than quantitative models to estimate pricing, risk exposure and risk accumulation. **A lack of data is a significant obstacle** and this limitation might not always allow for the proper estimation and pricing of risks.
- **Non-affirmative exposures are a key concern** regarding the proper estimation of accumulation of risks.
- **The lack of specialised underwriters, data and quantitative tools are key obstacles** to the development of the industry and the provision of proper coverage to the economy.
- **Regulation may be welcomed by the industry in a moderate fashion,** as it could help to address some of the identified challenges.

We have taken our work and these findings into account in the development of our supervisory convergence plan for 2018 – 2019. In this plan, cyber risk is identified as a priority under the **supervision of emerging risks**. As part of our activities in this field, EIOPA will develop guidelines regarding Information & Communication Technologies (ICT), security and governance, including cyber resilience and will further

develop supervisory practices that seek to assess information system resilience, cyber risk vulnerability and the insurance industry's use of big data.

EIOPA will also look into an efficient way of carrying out stress tests on the resilience of the insurance sector to cyber-attacks.

It is clear that cyber insurance affects countries across the world, not just in Europe. Issues related to cyber security and cyber risk are, therefore, one of the three priorities of the European Union – United States Insurance Project, in which EIOPA plays a leading role.

To conclude, cyber security and cyber risk are at the forefront of the concerns of economic operators and public authorities.

The insurance sector has an important role to play in establishing good risk management practices and the associated coverage.

The innovation and efficiency brought with the use of new technologies and high volumes of information will only become a reality if we find collective solutions to deal appropriately with cyber risk.

As cyber-insurance markets mature, we should start to discuss if cyber insurance should also be mandatory. This would provide a further level of security for companies and consumers in the digital world.

This is a universal challenge! Everyone has to contribute to meet this challenge!

Thank you very much for your attention

I stand ready to answer your questions.