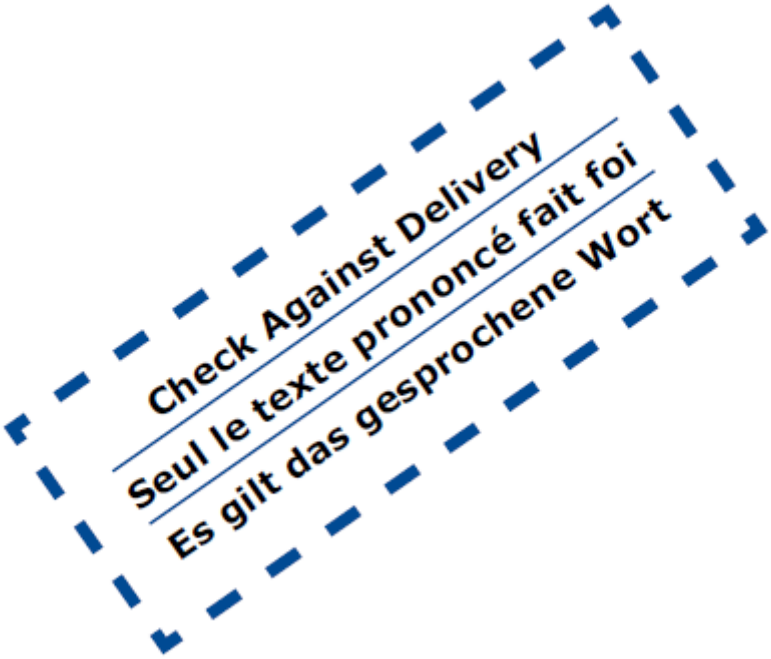
Fausto Parente
Executive Director

CYBER UNDERWRITING: MANAGING THE RISKS OF DIGITAL FINANCE



AFORE 4th Annual FinTech and Regulation Conference
Brussels, 3 March 2020

Ladies and gentlemen

Thank you for inviting me to today's conference. It's always so interesting to hear about the different aspects of FinTech and the pace of innovation. I'm also pleased to be here with the Chairs from my fellow supervisory authorities. Digital finance and FinTech are areas that we all follow closely.

We've heard a lot today about the vast potential of FinTech and how it is changing the lives of business and people.

The digitalisation of finance is dependent on many things, but the core drivers are technology and data. Data is valuable, especially the type of data held by financial institutions. And technology is vulnerable.

And that leaves companies and people open to the risks of cyber crime.

Earlier this morning we heard about the need for operational resilience and the importance of cyber security. The threat of cyber attacks are a serious risk to business. Ask any CEO what keeps him up at night, and cyber attacks and data theft are likely to be high on the list of answers.

So today, I would like to talk to you about two things: the importance of respecting data, and the importance of protecting the people through cyber insurance.

Data is power

Let me start with a few words on the importance of how we treat data.

In the old days, they used to say 'knowledge is power'. Today, it's more likely to be 'data is power'.

In the world of insurance for example, products, policies and pricing are all powered by data.

This is what makes it so valuable: with data an insurance company is able to offer the consumer just what they need and hopefully at just the right price. It should be a win-win for provider and policyholder.

And more choice and lower costs are what makes consumers so ready to share their data.

But what happens when data is not used ethically? When people find themselves excluded from insurance? Or when the holders of the data do not act responsibly?

At EIOPA, we believe that data needs to be respected. It must be used fairly and organisations holding data must act responsibly.

Because of this, last year we set up a consultative expert group on digital ethics in insurance to help us develop principles of digital responsibility in insurance.

We want these principles to have European values at their core while at the same time recognising the important role that insurance plays in our economy and also in our society.

So we are not reinventing the wheel. Nor are we ignoring the work on artificial intelligence being done by the European Commission and other bodies. Instead we want to operationalise best practice for the insurance sector.

In particular we are paying attention to:

- **Fairness and non-discrimination** – including data biases and the fairness around the use of price optimisation practices;
- **Transparency and explainability** – being clear on how data is used and any trade-offs with accuracy;
- **Governance** – touching on accountability, security and resilience.

Security of data is perhaps the most important thing here.

Because cyber attacks and data thefts cost.

They leave companies liable for fines of millions of euro. On top of that, there is the cost to a company's reputation, which is harder to quantify and very difficult – sometimes impossible – to earn back.

So cyber resilience is essential for any organisation and an effective cyber insurance market is a core component of a sound cyber resilience framework.

The cyber insurance market today

A sound cyber insurance market is an enabler of the digital economy.

From raising awareness of the risks and losses that can result from cyber attacks to facilitating responses and recovery, a well-developed cyber insurance market can play a valuable role in risk management.

And the European cyber insurance market is growing rapidly.

This is in part due to the overall increase in written contracts offered by insurers, and also because of the growing number of insurers providing cyber insurance.

And we expect the market to continue to grow.

The increasing frequency of cyber attacks, coupled with stricter regulation regarding cyber security as well as continued technological developments are all expected to increase demand for cyber insurance in the near future.

It's also likely that as businesses make their own investigations and investment into cyber security, they will become more aware of the growing need for insurance cover against cyber attacks.

Cyber underwriting to build European resilience

We need to work together to strengthen cyber resilience and create a strong cyber insurance market.

At EIOPA we have been studying the evolution of cyber insurance in Europe for some years now, including regular dialogue with insurance companies, and we have just published our cyber underwriting strategy.

Our strategy outlines the areas that we see need strengthening and sets out our approach and proposed actions.

First and foremost, we have seen that a **lack of data** is one of the biggest obstacles to a detailed understanding of the fundamental aspects of cyber risk and the provision of proper coverage.

It's understandable of course that companies are reluctant to share information on their security measures and their history of cyber incidents. The information is extremely sensitive but it is also incredibly valuable to underwriters.

And this lack of quantitative information on incidents makes it difficult for insurers to properly price risk and estimate the liability of exposures. It also hampers cyber risk measurement and management for insurers.

Therefore, we believe that we need to develop at European level a standardised cyber incident reporting framework that enables the sharing of aggregated data, anonymised to protect sensitive information, so that insurers and reinsurers can develop adequate pricing and risk management models.

To do this, we will engage with different bodies, including national authorities, the EBA and ESMA, as well as ENISA to explore and promote the development of a harmonised cyber incident reporting taxonomy so that we can put the data to work to underpin cyber underwriting modelling.

We also believe that there needs to be **a common understanding of contractual definitions**. Policyholders and insurers must share the same understanding of contract terms. Clear and transparent cyber coverage is essential from a consumer protection perspective. This is just as important for big companies as it is for individuals.

At European level, EIOPA will work other EU institutions can help to accelerate and promote engagement between industry and consumer associations which, in the long run, will help to maintain consumer confidence and avoid the potential for disputes.

As a supervisor, we are also working closely with national supervisors to ensure that appropriate **underwriting standards** are in place and that national supervisors have the capacity to supervise these. Technology changes, the nature of cyber attacks change, supervisors must be able to keep pace with these changes.

Continuing European cooperation

Cyber attacks are complex. They are dangerous. And they are ever more sophisticated.

Because of this, cyber risk is seen as a potentially systemic risk for the financial system and the real economy.

So we need a common approach to mitigate this risk.

And this involves continuing to work together to find shared solutions. Because a shared approach will mean a more effective approach.

And so in addition to working with national supervisors to foster a common approach to supervision, we will also continue our very valuable dialogue with

industry, consumer associations and other stakeholders to raise awareness of cyber security and insurance issues.

And at European level, we will continue our close cooperation, not only with the EBA and ESMA, but also with other EU bodies, so that we can strengthen Europe's over all resilience to cyber attacks.

In conclusion

Let me say in conclusion that it is no surprise that cyber security and cyber risks are a top concern not only for the financial sector, but for all industry and, indeed, for all people.

The digital era, and digital finance in particular, has brought us many benefits. But if too many people suffer because they are not better protected, we will quickly lose faith not only in the company that caused the suffering but also in technology itself.

This should not happen.

Let's work together to make sure that the risks resulting from digitalisation are considered and managed appropriately, including through an appropriate cyber insurance framework, so that digital finance continues to work for the people.

Ladies and gentlemen, thank you very much.