Guest Speaker Speech at the European Risk Management Awards 2016

http://www.commercialriskeurope.com/awards16/

Gérald Santucci
Adviser at DG CONNECT, European Commission

Good evening Ladies and Gentlemen,

I am delighted to be with you tonight at this first – but surely not last – European Risk Management Awards presentation. I'm very grateful to FERMA for inviting me – I take it as an honour and a privilege. So, thank you so much, Mr Willaert, for your invitation, for your kind introduction, and for your own very impressive and inspirational leadership with respect to the work on Risk Management within what I consider is an awesome, fast-growing and full of promise community. I extend my thanks to *Commercial Risk Europe* for organising the Awards Ceremony and Gala Dinner.

I would like also to thank all of the competitors, finalists and of course winners who have so generously and skilfully contributed to making these awards for *Excellence in Risk Management* and for *Industry Leadership* a defining moment in the history of the Risk Management profession.

Thank you ALL for your participation in the endeavour, your stupendous work, and your commitment to finding innovative solutions for addressing the security challenge in the digital era.

I can see here the extraordinary partnership between risk managers and insurers. It's this kind of partnership that we need in Europe to keep in the forefront of our strategies in the 21st century. Also with regulators. No doubt it's a strong intellectual, cultural and economic investment, and let me tell you that in the European Commission we're proud of all of you for pulling this investment together.

The first thing that jumps out at me is that Risk Management is no longer a mere activity; it is a new profession. It's no longer a choice of opportunity made at random by an individual; it's actually a promising career path. Indeed, the acceleration of change in ICT/Internet science and technology makes it crucial to develop the insurance products and services of tomorrow, which will create the confidence critically needed by decision-makers in both the private sector and the public sector to make bold choices for keeping abreast of innovation and competition. You here – risk managers and insurers – you have recognised that in today's world, with global challenges that transcend all borders and boundaries, we must prepare businesses to think in new ways. And you're doing that every day, as you encourage and support businesses of all sizes to look beyond the horizon and to seek the development of creative solutions to the issues of the day.

Managing risk is for me not just an economic issue. It is a *civilizational* issue. It's a *social* issue. It's a *family* issue. But – perhaps more than anything – it's a *moral* issue. More specifically, as regards cyber security, it is up to all of us to use the power of technology responsibly and to use the power of insurance boldly and intelligently in order to make certain that all of our citizens and businesses in Europe share fairly in the benefits. Our common purpose demands that we put the security of our companies and families first. And it requires that we are all involved – and all of us must be asked

what we can do. Fulfilling this common purpose will require renewed resolve by everyone involved – primarily risk managers, insurers, engineers and policy-makers. It will also require a better approach and a genuine commitment to cyber security for all organisations and all individuals.

In the past two decades, we have taken important steps to provide trust and confidence to many stakeholders at a time when insurance was lacking. But incremental steps, as important as they have been, are no longer sufficient as cyber security threats undermine our *physical infrastructures* as a whole – and if I can dare say: our *societal superstructure* as well. Therefore it is time for bolder action. It is increasingly clear that the only effective and fair answer to the worsening cyber security scenarios is to embrace a broader vision and well fit strategies that represent what I called our true common purpose. In other words, we need *a new sense of community* – all stakeholders must accept to join in a continuous and constructive dialogue to co-create risk models and make quantified assessments for better understanding and mitigating risks. We need *a new willingness and commitment* to protecting critical infrastructures and preserving business continuity. We need also *a new understanding* that we are all in this together. To quote 17th century English poet John Donne, "No man is an island"… And of course we need *a new recognition* of the undeniably crucial role of partnership between risk managers and insurers.

Since the adoption of the EU Cybersecurity Strategy in 2013, the European Commission has stepped up its efforts to better protect Europeans online. We have adopted a set of legislative proposals, in particular on network and information security, and we have earmarked more than €600 million of EU investment for research and innovation in cybersecurity projects during the 2014-2020 period. In the Horizon 2020 Framework Research and Innovation Programme, there is a so-called *Societal Challenge* number 7 on 'Protecting freedom and security of Europe and its citizens'. It notably proposes work on 1) Critical Infrastructure Protection (CIP), which contains a topic cutting across physical and cyber-security, and 2) Digital Security (DS), which corresponds to a focus area covering most of cybersecurity activities of Societal Challenge 7. Let me stress that cybersecurity is today one of the key priorities of the Digital Single Market (DSM) strategy and therefore a new contractual public-private partnership has been launched in July this year to stimulate and nurture the European cybersecurity industry. At the same time, the EU has adopted the Directive on Security of Network and Information Systems – the 'NIS' Directive – whose objective is to achieve a high common level of security within the EU by means of (i) improved cybersecurity capabilities at national level, with in particular the enhanced role to be played by Computer Security Incident response Teams (CSIRTs), (ii) increased EU-level cooperation on education, training and cybersecurity exercises, and (iii) risk management and incident reporting obligations for operators of essential services and digital service providers. It is worth noting that the EU Directive covers a large range of sectors – energy, transport, banking, financial market infrastructures, health, water, and obviously the digital infrastructure.

Europe is not alone to be aware of the big challenge which Cybersecurity represents. One week ago, the US Commission on Enhancing National Cybersecurity, which President Obama had formed in April 2016, published a 100-page report detailing a plan for protecting cyberspace. The main areas of focus are: federal governance; critical infrastructure; cybersecurity research and development; cybersecurity workforce; identity management and authentication; Internet of Things; public awareness and education; and state and local government cybersecurity.

This interesting report includes two elements which I would like to draw to your attention because they match our own line of thinking in Europe.

- The first one – **insurance** – concerns you closely. I don't need to elaborate on the fact that the discrete risks associated with insurance coverage must be measurable, quantifiable, so that insurers can have a stronger basis for making coverage decisions and standardising insurance premiums. I had the opportunity to discuss this issue with FERMA and Airbus last month.
- The second one – **Internet of Things** – is perhaps something that you are less involved in. But you are well aware that our way of life has become reliant on complex webs of interconnected infrastructure with many interdependencies. The fast-moving shift to increased connectivity is introducing an entirely new component into our economic and social spheres. Businesses and industries, many of which involving small and large companies that contribute to the supply chain that develop products, may not be fully aware of their interdependencies; likewise, elements of critical infrastructure, such as the electric grid and communications systems, are dependent on other sectors for their own operation. This hyper-connectivity is what we call the "Internet of Things". I will not discuss here its substantial potential benefits, but for our purpose tonight I just want to stress that the Internet of Things is causing massive data proliferation through devices that are capturing, aggregating, and processing data. Trust in Internet of Things enabled decisions requires confidence in such devices as well as assurance that the data have not been accidentally or maliciously altered. This trust will come from being able to identify devices that act on their own, like sensors, or devices that are associated with a person, like a mobile phone. We therefore must consider the problem of identity management from the perspective of being able to securely and efficiently identify not just people, but also individual devices and the data that come from them. Just try to imagine the difficulties risk managers and insurers will face when by 2020 security processes and coverage decisions will need to take into account a population of 50 billion connected devices, which is seven times more than the total number of human beings on Earth! This represents indeed a tremendous challenge which I'm sure your community will help us in the European Commission to meet.

So, indeed risks are growing and becoming increasingly likely, generated by private and criminal organisations but also coming from nation states, namely Russia and China. Last summer, Bruce Schneier, a top US cybersecurity expert, warned the world community that Internet-connected products and appliances were setting us up for a disaster because hackers could steal data, modify it, or prevent the owner from getting it. He said hackers could reduce the temperature on smart thermostats to freeze water pipes, crash airplanes and connected cars, and even attack connected medical devices that are necessary to keep people alive. Pessimism? '24' paranoia? Well, not at all. As you remember, on 21 October a series of Distributed Denial of Service (DDoS) attacks caused widespread disruption of legitimate Internet activity in the United States. These attacks were made possible by the large number of unsecured Internet-connected digital devices, such as home routers and surveillance cameras. These devices had been infected with malicious code to form a "botnet". Recently, we witnessed a hacker attack against Deutsche Telekom, disrupting Internet, TV and phone networks across Germany. Deutsche Telekom confirmed that around 900,000 customers had their

broadband disconnected – about 4.5 percent of its customer base! As Deutsche Telekom's head of security said, "*the naive phase of the Internet is over*"…

I do not seek to scare you. Indeed, we draw huge benefits from our network infrastructures. I have myself worked during eight years on the Internet of Things and I strongly believe that its full deployment will generate a lot of good for communities, individuals and businesses. However, we must be aware that since the invention of the microprocessor in 1971 – less than 50 years ago – and the WorldWideWeb in 1989 – less than 30 years ago – our world has profoundly changed, and the nature, scope and impact of the threats as well. In order to meet the unprecedented challenge which I have just sketched in for you tonight, we must first of all get the right people in the right roles at the right time in order to raise the profile and augment the effectiveness of Risk Management. Fortunately, we already have that in Europe! It is called FERMA, our essential organisation of the Risk Management profession.

I look forward to an open, transparent and inclusive debate on Risk Management, and to defining cooperatively the package of customised solutions which, on one hand will acknowledge the global, complex and unpredictable nature of today's risks and, on the other hand, will meet the requirements for risk transfer, management, prevention and claims handling. Europe's citizens and organisations deserve no less.

Thank you.